ANTEPRIMA DELLA DOMANDA NON VALIDA PER LA PRESENTAZIONE. SI RICORDA A TUTTI I COMPILATORI CHE LA CONSEGNA FORMALE DELLE DOMANDE DI CONTRIBUTO E' RAPPRESENTATA ESCLUSIVAMENTE DALLA CONCLUSIONE DELL'OPERAZIONE DI CARICAMENTO DEL PDF FIRMATO DIGITALMENTE SU PIATTAFORMA SECONDO LE MODALITA' INDICATE NELLE LINEE GUIDA ALLA COMPILAZIONE PIATTAFORMA SVILUPPO TOSCANA. TALE OPERAZIONE DOVRA' ESSERE COMPIUTA ENTRO LE ORE 17:00 DEL GIORNO 15/03/2012 PENA LA NON AMMISSIBILITA' DELLA DOMANDA.

Regione Toscana
POR CReO 2007 - 2013
LINEA DI INTERVENTO 1.5.a - 1.6
BANDO UNICO R&S ANNO 2012

Alla Regione Toscana
Direzione Generale Competitività del sistema regionale e sviluppo delle competenze
Area di Coordinamento Industria, Artigianato, Innovazione tecnologica
Settore Ricerca industriale, Innovazione e Trasferimento tecnologico
Via Luca Giordano, 13
50132 Firenze

SCHEDA TECNICA DI PROGETTO

Il/la sottoscritto/a *Giuseppe Sajeva* nato/a a *Palermo* (*PA*) il 24/05/1971 sesso *M* residente in *Palermo* prov *PA* via *Viale Regina Margherita, 9* CAP *90138* in qualita' di legale rappresentante del(della/dell') Impresa *Engineering Ingegneria Informatica S.p.A.* con sede legale nel comune di *Roma* Provincia *RM* Via e N. Civico *Via San Martino della Battaglia, 56* CAP *00185* CF *00967720285* P.IVA *05724831002* Forma Giuridica *S.P.A.* Matricola INPS *7044662393* Posizione INAL *3733953* ATECO 2007 *J62.01.00* telefono *081 6103497* fax *081 6103200* E-mail legale rappresentante del(della/dell') Impresa *giuseppe.sajeva@eng.it*

SEZIONE 1: ANAGRAFICA DEL PROGETTO

Titolo: *Secure!*

Acronimo: *Secure!*

DATE DI INIZIO E FINE PROGETTO

Data prevista per l'avvio: 01/01/2013

Data di conclusione prevista: 31/08/2014

Durata in mesi: 24

LINEA DI AZIONE DEL BANDO

Indicare la Linea di Azione del Bando e l'eventuale appartenenza ad una delle aree tematiche/ tecnologiche riferite ai PIS e/o ai settori high-tech elencati nel Bando

- ○ **Linea A**

  Indicare se il progetto è riferibile ad una delle seguenti ambiti indicati dal par 6.1 del Bando

  - ○ Sistemi e distretti produttivi tipici
  - ○ Distretti tecnologici regionali
  - ○ Altri cluster industriali regionali

  In Caso positivo indicare quale:

- ◉ **Linea B**

Indicare se il progetto è riferibile ad una delle seguenti ambiti indicati dal par 6.2 del Bando

(●) Distretti tecnologici regionali

( ) Settori hi-tech
In Caso positivo indicare quale: *ICT e tecnologie delle telecomunicazioni*

( ) **Linea C**

Indicare se il progetto è riferibile ad una delle seguenti ambiti indicati dal par 6.2 del Bando

( ) Distretti tecnologici regionali

( ) Settori hi-tech
In Caso positivo indicare quale:

Nel caso di appartenenza ad una delle aree tematiche/tecnologiche riferite ai precedenti PIS e/o ai precedenti settori high-tech che conferiscono priorità, motivare l'appartenenza del progetto alla specifica area/settore, facendo riferimento ai documenti programmatici/definitori di seguito riportati:

CATEGORIA	DOCUMENTO DI RIFERIMENTO
Sistemi e distretti produttivi tipici	Programma regionale di sviluppo 2011-2015, pagg 95 e ss.
Distretti tecnologici regionali	Programma regionale di sviluppo 2011-2015, pagg 107 e ss.
Altri cluster industriali regionali	Programma regionale di sviluppo 2011-2015, pagg 121 e ss.
Settori hi-tech	1) Per "Nanotecnologie" e " Fotonica e optoelettronica": Comunicazione della Commissione "Preparare il nostro futuro: elaborare una strategia comune per le tecnologie abilitanti fondamentali nell'UE" COM (2009) 512. 2) Per ""Meccanica avanzata, robotica e robo-meccatronica": Programma nazionale per la ricerca 2005-2007, pagg. 61 e ss., richiamato dal Programma Nazionale della Ricerca (PNR) 2011-2013.

Secondo il Programma regionale di sviluppo 2011-2015, nelle pagine richiamate, il Distretto Tecnologico per l'ICT e le telecomunicazioni è il tentativo di mettere a sistema le eccellenze territoriali massimizzando partnership e collaborazioni tra i vari attori dell'innovazione e del trasferimento tecnologico.
Questa attenzione è declinata in maniera specifica su 3 ambiti da valorizzare in ottica trasversale e multidisciplinare: ICT per il sistema produttivo, ICT per la funzione pubblica, ICT per le grandi infrastrutture tecnologiche.
E' evidente che Secure! focalizza proprio questi ambiti per la sua valenza in termini di sicurezza in ciascuno di essi.
Inoltre nelle stesse pagine del Programma si sottolinea come negli ultimi anni sia avvenuta una convergenza tra varie aree disciplinari, dove domini scientifici, inizialmente distinti, hanno iniziato ad integrarsi fortemente (Complexity Science), con l'ICT che diventano strumento di dialogo.
Secondo il Programma in particolare le infrastrutture tecnologiche complesse giocano un ruolo ormai vitale nella vita delle nazioni e sono quindi ormai elementi nevralgici la cui vulnerabilità può avere ripercussioni gravi. Per questo accanto all'uso di paradigmi conoscitivi e strumenti tecnologici convenzionali, si rendono necessari nuovi modelli di "Sistemi Complessi" e nuovi approcci.
Secure! propone appunto un approccio innovativo al problema, centrato sulle potenzialità dell'intelligenza diffusa e cooperativa.

Nel caso in cui il progetto non afferisca alle aree tematiche/tecnologiche riferite ai precedenti PIS e/o ai precedenti settori high-tech, illustrare la coerenza del progetto rispetto alla programmazione regionale.

INFORMAZIONI PROGETTO

Categoria del progetto di ricerca:	ricerca informatica
% Ricerca Industriale:	90.27
% Sviluppo Sperimentale:	9.73

Pareole-Chiave del Progetto
Sicurezza, affidabilità, fiducia e privacy, Social Networking, Cooperative Intelligence, crowdsensing, crowdsourcing, decision making, sicurezza e protezione territorio, web, crowds, sensors, situation awareness, gestione delle crisi/emergenze, Early Warning Systems (EWS, Informazioni geospaziali, crowdmapping, real time analysis,Data Analitics, social data, social media, information extraction, security system.

Sintesi del Progetto.
Secure! realizzerà un innovativo sistema di supporto alle decisioni in tema di sicurezza pubblica e privata e di protezione civile (prima, durante e dopo), mettendo in sinergia elementi di crowdsensing e crowdsourcing ed il coordinamento delle attività di monitoraggio ed intervento sul territorio.
Con la diffusione dei social media, l'obiettivo generale del progetto Secure! è studiare l'applicabilità e le modalità di applicazione di meccanismi, modelli, tecniche, tecnologie e strumenti di crowdsourcing per la prevenzione (quando possibile), l'anticipazione e la gestione di eventi e situazioni di emergenza relativi alla sicurezza pubblica ed alla protezione civile. In pratica si vogliono definire e realizzare strumenti e servizi che complimentino ed integrino gli attuali sistemi di gestione delle suddette situazioni, sfruttando le potenzialità offerte dall'enorme mole di informazioni presenti sui social media e la disponibilità di "sensori umani" coinvolgibili in processi di crowdsensing.
Il progetto studierà, definirà ed implementerà tecniche e componenti innovative per l'acquisizione e la raccolta di dati da sorgenti multiple (social media, applicazioni di crowdsensing, reti di sensori, sistemi informativi esistenti). Saranno studiate e realizzate tecniche e componenti innovative per l'estrazione, l'analisi e l'integrazione di informazioni (spesso non strutturate, come testo, immagini, ecc.) dalle suddette sorgenti. Inoltre verranno studiati e definiti servizi di supporto decisionale che integrano meccanismi di gestione della conoscenza per la determinazione della situation awareness e di ragionamento pratico (orientato all'azione) per la gestione dei piani operativi di intervento. Inoltre, si studieranno meccanismi e tecniche di sicurezza, trust, privacy ed affidabilità delle informazioni raccolte e gestite e dei servizi della piattaforma.
I risultati saranno integrati in un'infrastruttura abilitante orientata ai servizi (il Secure! Framework) per la costruzione di servizi di gestione della sicurezza pubblica e delle infrastrutture e di protezione civile basati sui meccanismi del crowdsourcing.
Il framework sarà applicato a due scenari dimostrativi (la protezione e la gestione del patrimonio artistico-culturale, la protezione di infrastrutture critiche).

AFFIDABILITÀ ECONOMICO FINANZIARIA

Dare dimostrazione dell'affidabilità economico finanziaria dell'impresa proponente ai sensi dell'art. 5 del bando attraverso il seguente rapporto:

CN/(CP-I):	106,66

Dove
CN = capitale netto quale risulta dall'ultimo bilancio approvato alla data della domanda.
Per le imprese di nuova costituzione si considera il valore del CN risultante dall'atto costitutivo, qualora alla data del bando non sia ancora avvenuta l'approvazione del bilancio relativo al primo esercizio;
CP = somma dei costi complessivi del progetto indicato in domanda;
I = importo del contributo richiesto.
Ad incremento di CN potranno essere considerati:

a. un aumento di capitale, rispetto a quello risultante dall'ultimo bilancio approvato, che risulti comunque deliberato, ai sensi del Codice Civile, alla data di presentazione della domanda, ovvero

b. l'eventuale quota di capitale sociale riportata nell'ultimo bilancio approvato e non ancora versata, risultante dalla voce "crediti verso soci per versamenti ancora dovuti" di cui alla voce a) dell'attivo dello stato patrimoniale, ovvero

c. eventuali versamenti in conto capitale deliberati dai soci successivamente alla data di riferimento dell'ultimo bilancio approvato.

SEZIONE 2: PARTECIPANTI AL PROGETTO

Partecipante N°1

Denominazione:	Engineering Ingegneria Informatica S.p.A.
Dimensione:	Grande
Ateco 2007:	J62.01.00

Indirizzo della sede legale.

Via e n. *Via San Martino della Battaglia, 56* Comune *Roma* Cap *00185* Telefono *081 6103497* Fax *081 6103200* Email *giuseppe.sajeva@eng.it*

Indirizzo a cui inviare le comunicazioni ufficiali se diversa dalla sede legale:

Via e n. *Via E. Gianturco, 15* Comune *Napoli* Cap *80142* Telefono *081 6103497* Fax *081 6103200* Email *luca.bevilacqua@eng.it*

Sede di svolgimento del progetto se diversa dalla sede legale:

Via e n. *Via del Pian dei Carpini 1 e via Panciatichi, 40* Comune *Firenze* Cap *50127* Telefono *055 5303110* Fax *055 5303110* Email *segreteria.fi@eng.it* codice Ateco *J62.01.00* Matricola INPS *7044662393* Posizione INAIL *3733953* Nr. Iscrizione registro Imprese *531128* Presso la C.C.I.A. di *Roma* Settore economico di appartenenza *Industria e servizi*

Referente scientifico per il progetto dell'impresa

Nome:	Silvia
Cognome:	Boi
Telefono:	3408100593
Cellulare:	3408100593
Fax:	
Email:	silvia.boi@eng.it

Direttore tecnico (eventuale)

Nome:	
Cognome:	
Tel:	
Fax:	
E-mail:	
Luogo di nascita:	
Data di nascita:	

Partecipante N°2

Denominazione:	Crowd srl
Dimensione:	Micro
Ateco 2007:	62.01.00

Indirizzo della sede legale.

Via e n. *Via Livorno, 3* Comune *Catania* Cap *95127* Telefono *05044076* Fax *05044076* Email *gio@crowd.it*

Indirizzo a cui inviare le comunicazioni ufficiali se diversa dalla sede legale:

Via e n. *Via Nino Bixio, 18* Comune *Pisa* Cap *56125* Telefono *05044076* Fax *05044076* Email *info@crowdengineering.com*

Sede di svolgimento del progetto se diversa dalla sede legale:

Via e n. *Via Nino Bixio, 18* Comune *Pisa* Cap *56125* Telefono *05044076* Fax *05044076* Email *info@crowdengineering.com* codice Ateco *62.01.00* Matricola INPS *2110311375* Posizione INAIL *18441665/79* Nr. Iscrizione registro Imprese *164483* Presso la C.C.I.A. di *Pisa* Settore economico di appartenenza *Sviluppo Software*

Referente scientifico per il progetto dell'impresa

Nome:	Massimo
Cognome:	Piccioni
Telefono:	05044076
Cellulare:	
Fax:	05044076
Email:	massimo@crowdengineering.com

Direttore tecnico (eventuale)

Nome:	
Cognome:	
Tel:	
Fax:	
E-mail:	
Luogo di nascita:	
Data di nascita:	

Partecipante N°3

Denominazione:	RESILTECH SOCIETA' A RESPONSABILITA' LIMITATA
Dimensione:	Piccola
Ateco 2007:	62.01

Indirizzo della sede legale.

Via e n. *Via B. Gigli 27* Comune *LATIGNANO - CASCINA* Cap *56021* Telefono *3481696574* Fax *0587829995* Email *info@resiltech.com*

Indirizzo a cui inviare le comunicazioni ufficiali se diversa dalla sede legale:

Via e n. *Piazza Nilde Iotti, 25* Comune *PONTEDERA (PI)* Cap *56025* Telefono *3473636595* Fax *0587829995* Email *INFO@RESILTECH.COM*

Sede di svolgimento del progetto se diversa dalla sede legale:

Via e n. *Piazza Nilde Iotti, 25* Comune *PONTEDERA (PI)* Cap *56025* Telefono *3473636595* Fax *0587829995* Email *INFO@RESILTECH.COM* codice Ateco *62.01* Matricola INPS *6205543849* Posizione INAIL *14602937* Nr. Iscrizione registro Imprese *PI - 159748* Presso la C.C.I.A. di *PISA* Settore economico di appartenenza *Servizi avanzati di consulenza in informatica, ricerca e sviluppo, analisi e collaudi*

Referente scientifico per il progetto dell'impresa

Nome:	Lorenzo
Cognome:	Falai
Telefono:	0587466695
Cellulare:	3473636595
Fax:	0587829995
Email:	lorenzo.falai@resiltech.com

Direttore tecnico (eventuale)

Nome:	
Cognome:	
Tel:	
Fax:	
E-mail:	
Luogo di nascita:	
Data di nascita:	

ORGANISMI DI RICERCA PARTECIPANTI AL PROGETO

Partecipante N°2

Denominazione: Istituto di Informatica e Telematica (IIT-CNR)

Indirizzo della sede legale.

Via e n. *Piazzale Aldo Moro, 7* Comune *Roma* Cap *00185* Telefono *0503152123* Fax *0503152113* Email *domenico.laforenza@iit.cnr.it*

Indirizzo a cui inviare le comunicazioni ufficiali se diversa dalla sede legale:

Via e n. Comune Cap Telefono Fax Email

Sede di svolgimento del progetto se diversa dalla sede legale:

Via e n. *Via Giuseppe Moruzzi 1* Comune *Pisa* Cap *56124* Telefono Fax Email codice Ateco Matricola INPS Posizione INAIL Nr. Iscrizione registro Imprese Presso la C.C.I.A. di Settore economico di appartenenza

Referente scientifico per il progetto dell'impresa

Nome:	Fabio
Cognome:	Martinelli
Telefono:	+39 050 315 3425
Cellulare:	348 8260772
Fax:	+39 050 315 2113
Email:	fabio.martinelli@iit.cnr.it

Direttore tecnico (eventuale)

Nome:

Cognome:

Tel:

Fax:

E-mail:

Luogo di nascita:

Data di nascita:

Partecipante N°3

Denominazione: Dipartimento di Sistemi e Informatica - Università degli Studi di Firenze

Indirizzo della sede legale.

Via e n. *Piazza S. Marco 4* Comune *Firenze* Cap *50121* Telefono *055 2757211* Fax *055 2757429* Email *andrea.bondavalli@unifi.it*

Indirizzo a cui inviare le comunicazioni ufficiali se diversa dalla sede legale:

Via e n. *Viale Morgagni 65* Comune *Firenze* Cap *50134* Telefono *0554237457* Fax *0554237436* Email *bondavalli@unifi.it*

Sede di svolgimento del progetto se diversa dalla sede legale:

Via e n. *Viale Morgagni 65* Comune *Firenze* Cap *50134* Telefono *0554237457* Fax *0554237436* Email *bondavalli@unifi.it* codice Ateco Matricola INPS Posizione INAIL Nr. Iscrizione registro Imprese Presso la C.C.I.A. di Settore economico di appartenenza

Referente scientifico per il progetto dell'impresa

Nome: Andrea

Cognome: Bondavalli

Telefono: 0554237457

Cellulare: 3294309838

Fax: 0554237436

Email: bondavalli@unifi.it

Direttore tecnico (eventuale)

Nome:

Cognome:

Tel:

Fax:

E-mail:

Luogo di nascita:

Data di nascita:

Partecipante N°4

Denominazione: MICC Media Integration and Communication Center - Università degli Studi di Firenze

Indirizzo della sede legale.

Via e n. *P.zza San Marco, 4* Comune *Firenze* Cap *50121* Telefono *055 4237401* Fax *055 4237400* Email *delbimbo@dsi.unifi.it*

Indirizzo a cui inviare le comunicazioni ufficiali se diversa dalla sede legale:

Via e n. Comune Cap Telefono Fax Email

Sede di svolgimento del progetto se diversa dalla sede legale:

Via e n. *Viale Morgagni, 65* Comune *Firenze* Cap *50134* Telefono *055 4237404* Fax *055 4237400* Email *roberto.caldelli@unifi.it* codice Ateco Matricola INPS Posizione INAIL Nr. Iscrizione registro Imprese Presso la C.C.I.A. di Settore economico di appartenenza

Referente scientifico per il progetto dell'impresa

Nome:	Alberto
Cognome:	Del Bimbo
Telefono:	0554237401
Cellulare:	3392000104
Fax:	05542374000
Email:	delbimbo@dsi.unifi.it

Direttore tecnico (eventuale)

Nome:	Roberto
Cognome:	Caldelli
Tel:	0554237404
Fax:	0554237400
E-mail:	roberto.caldelli@unifi.it
Luogo di nascita:	Figline Valdarno (FI)
Data di nascita:	21/04/1970

SEZIONE 3: ORGANISMI DI RICERCA (OR) SUBCONTRAENTI NELL'AMBITO DEL PROGETTO

Indicare i seguenti dati per organismo di ricerca 1
Denominazione Soggetto/i del/i quale/i l'OR è subcontraente Indirizzo della sede legale o unità locale Referente scientifico del progetto (indicare nome cognome e riferimenti) Direttore tecnico (eventuale, indicare nome cognome e riferimenti.)

SEZIONE 4: DESCRIZIONE DEL PROGETTO

Titolo:	*Secure!*
Acronimo:	*Secure!*

Idea alla base del progetto
L'avvento dei social media e la sempre crescente disponibilità di dispositivi mobili personali, sempre più frequentemente e facilmente connessi alla rete, offrono l'opportunità di una nuova e crescente sorgente di informazioni in tempo reale, fornite da comunità di utenti che continuamente esprimono e spesso condividono idee, commenti, suggerimenti, notizie aggiornate, esperienze, sentimenti, lamentele, segnalazioni, ecc.
Oggi i social media rappresentano il più importante mezzo di comunicazione, grazie alla possibilità di

legare agevolmente persone, fatti, eventi e luoghi (Bruns, A., & Bahnisch, M. "Social Media: Tools for User-Generated Content Social Drivers behind Growing Consumer Participation in User-Led Content Generation". July 20, 2009; Huberman, Bernardo, Romero, Daniel, and Wu, Fang. "Social networks that matter: Twitter under the microscope" First Monday, Volume 14 Number 1, 20 December 2008), attraverso una grande quantità di dati in "tempo reale", aperti, geo-referenziati e interconnessi: gli utenti sono oggi i veri detentori della cosiddetta "living information" ed i primi veri fornitori di informazioni aggiornate su fenomeni sociali, eventi pericolosi, ed accadimenti di ogni natura; gli utenti dei social media possono essere considerati come veri e propri "sensori umani", che forniscono informazioni qualitative e qualche volta anche quantitative.
Come conseguenza della diffusione dei social media e del social networking, principi e meccanismi di crowd-sourcing possono quindi essere applicati anche ad attività e processi critici, come la gestione di crisi di larga scala o di singole emergenze (come è già avvenuto ad esempio nel caso della crisi in Egitto ed in Libia).
Tali meccanismi ci offrono l'opportunità di sfruttare le suddette informazioni per "prevenire" o "anticipare" alcune situazioni di pericolo, di crisi, di emergenza. Ma sono applicabili anche a situazioni e scenari come
(i) la gestione della sicurezza pubblica di una città (come la piccola criminalità, si veda ad esempio "Man tracks stolen laptop hundreds of miles away, calls thief", http://storify.com/btballenger/man-tracks-stolen-laptop-thousands-of-miles-away),
(ii) la gestione di emergenze legate a fenomeni naturali (es. alluvioni, forti nevicate, crolli, frane, ecc.),
(iii) la gestione delle emergenze relative agli incidenti stradali,
(iv) la protezione del patrimonio culturale,
(v) la protezione di infrastrutture critiche (es. aeroporti, stazioni, fabbriche, data center, ecc.),
(vi) la gestione e la prevenzione delle emergenze di traffico e dei trasporti locali in genere (integrando anche informazioni provenienti da sorgenti istituzionali o da infrastrutture).
Anche la gestione degli eventi sociali sta assumendo nei tempi recenti una sempre maggiore rilevanza, soprattutto dal punto di vista della tutela dell'ordine pubblico e del patrimonio, in quanto è sempre più frequente l'occorrenza di eventi di aggregazione spontanea che, facilitati da internet e dall'uso dei social network, arrivano a manifestarsi pressoché all'improvviso, impedendone una gestione adeguata da parte della forza pubblica e degli enti interessati.
Un esempio è l'organizzazione e la mobilitazione di gruppi violenti, "London Riots: Twitter That Caused Them?", http://www.huffingtonpost.co.uk/2011/08/08/london-riots-twitter-that_n_920791.html.
È evidente come tali situazioni, soprattutto (ma non esclusivamente) quando non organizzate, possano facilmente degenerare in emergenze, con potenziali impatti sull'integrità del patrimonio pubblico e privato, sulla sicurezza dei cittadini e sui servizi.
In tutte queste situazioni, la possibilità di raccogliere informazioni dalla folla (la cosiddetta "crowd"), direttamente sul campo, può portare alla prevenzione (nel caso migliore), all'anticipazione (early warning), alla valutazione e alla riduzione dell'entità e dell'impatto della crisi/emergenza e a una migliore gestione della stessa, grazie alla possibilità di raggiungere le persone ed eventualmente anche aiutare da loro.
In pratica si possono sfruttare anche i meccanismi che governano le community: un insieme di persone che forniscono informazioni su un evento costituisce una comunità virtuale, anche se inconsapevolmente, che, anche per un tempo definito, condivide qualcosa, un interesse, un'intenzione, un'emozione, ecc.; le informazioni inserite vengono anche validate dagli altri membri, generando la cosiddetta "saggezza della folla" (wisdom of the crowd).
Si pone quindi una problematica di raccolta, monitoraggio e analisi di tali informazioni, al fine di prevenire o intercettare tempestivamente eventuali derive illecite e/o violente e di intervenire con successo nella tutela della persona e del patrimonio privato e pubblico (incluso quello artistico/culturale), cui tali manifestazioni dovessero venire a contatto.
Molte informazioni sono già oggi raccolte da infrastrutture di sensori dispiegati sul territorio, nelle città, nei luoghi potenzialmente a rischio o da monitorare; altre informazioni sono raccolte e gestite da sistemi informativi esistenti (a volte istituzionali). Molte altre informazioni sono volontariamente inserite dalle persone sui social network (tra tutti Twitter e Facebook) o più in generale sul Web (blog, forum, ecc.) anche mediante dispositivi mobili (smartphone, tablets).
In questo contesto, la sfida scientifica e tecnologica è raccogliere, esaminare e sfruttare informazioni "realistiche" e "credibili" immesse nel Web dagli utenti presenti sul campo, "integrandole opportunamente" con dati e informazioni provenienti dai canali tradizionali di segnalazione, dai sistemi esistenti e dalle infrastrutture di sensori dispiegate sul territorio, e al contempo coordinare gli interventi attraverso un meccanismo di moltiplicazione delle forze basato sul crowdsourcing.
L'opportuna esplorazione e integrazione di queste risorse può permettere di migliorare l'efficienza della gestione operativa di scenari di crisi così o di singole situazioni di emergenza, in termini di prevenzione, rapida individuazione e intervento, per diversi livelli di gravità in termini di urgenza e numero di persone coinvolte (ad esempio, si va dalla gestione di scenari di crisi su larga scala come terremoti, alla prevenzione di potenziali suicidi, al rapido intervento di manutenzione stradale o per il

recupero di opere d'arte).
Il progetto Secure! mira a fornire strumenti ICT e servizi di supporto per la gestione di scenari di sicurezza pubblica e privata e di protezione civile (prima, durante e dopo), sfruttando i social media e mettendo in sinergia elementi di crowdsensing e crowdsourcing e il coordinamento delle seguenti attività di monitoraggio e intervento sul territorio:
- rilevazione di eventi imprevisti o non pianificati, attraverso il monitoraggio, l'estrazione e l'analisi di informazioni presenti su siti di informazione collaborativa e sui social network: infatti, le persone tendono a utilizzare strumenti come Twitter in maniera molto intensa anche nelle situazioni di crisi, di pericolo, di emergenza o semplicemente per fare delle segnalazioni (si veda quanto successo in Egitto recentemente, "How Egyptians Used Twitter During the January Crisis", http://mashable.com/2011/02/01/egypt-twitter-infographic/);
- raccolta spontanea (push) di informazioni sensibili da parte delle workforce coinvolte sul territorio (es. persone dotate di smartphone con applicazioni interoperabili con l'infrastruttura di Secure!);
- raccolta periodica (pull) e analisi di informazioni da parte delle reti integrate di sensori dislocati sul territorio (es. telecamere fisse o robotizzate, sensori di rilevazione di parametri ambientali, ecc.);
- analisi, integrazione e correlazione di tutte le suddette informazioni raccolte, al fine di individuare prontamente situazioni di pre-allerta che richiedano ulteriori verifiche o approfondimenti;
- quadro della situazione (situational awareness), sulla base delle informazioni raccolte ed elaborare nel modo suddetto, anche in quegli scenari in cui i canali tradizionali potrebbero non essere attivi o fornire informazioni parziali o non aggiornate. Alcuni casi eclatanti riguardano il recente tsunami in Giappone ("Twitter Users React To Massive Quake, Tsunami In Japan", http://mashable.com/2011/03/11/japan-tsunami) ed il terremoto di Haiti ("In Haiti earthquake coverage, social media gives victim a voice", http://www.guardian.co.uk/media/pda/2010/jan/14/socialnetworking-haiti) in cui le informazioni raccolte dai vari canali sono risultate frammentarie e parziali. Ma anche la semplice determinazione dell'entità di un evento meno catastrofico (il danno a un monumento, il numero di persone coinvolte in un determinato evento, incidente o aggressione, la gravità di un incidente stradale, ecc.) sono esempi di informazioni che contribuiscono a costruire la "consapevolezza della situazione da gestire";
- comunicazione dell'emergenza e/o di avvertimenti preventivi e/o di campagne informative orientate alla prevenzione o all'educazione dei cittadini, attraverso i social media o altri strumenti dedicati;
- utilizzo delle squadre operative coinvolte sul territorio per sopralluoghi nelle aree interessate, tesi a verificare e approfondire effettive situazioni a rischio;
- segnalazione della necessità di intervento di enti preposti alla sicurezza, per la risoluzione definitiva o la mitigazione dell'emergenza;
- analisi post-evento al fine di migliorare le performance del sistema di risposta e la gestione nel caso di future emergenze, sulla base dell'aggregazione di grandi moli di informazioni storiche, di estrazione di nuove informazioni, dell'identificazione di pattern ricorrenti, ecc.
Il progetto Secure! mira a sperimentare e validare i suddetti strumenti e servizi in almeno due casi reali: la protezione del patrimonio artistico-culturale e la protezione di infrastrutture critiche. Tali scenari sono descritti nel seguito.
Qui a titolo di esempio, per chiarire l'idea che sta alla base del progetto, si vuole descrivere uno scenario tipico.
Si consideri il caso di un'aggregazione non autorizzata di persone, organizzata spontaneamente e in maniera repentina (flashmob), mediante social network (es. Twitter), in una località di interesse storico-culturale come il centro storico di una città.
La gestione di questa situazione avverrà tramite una serie di iterazioni del ciclo osservazioni/analisi/decisioni/azioni ripetute varie volte per gestire in maniera appropriata l'evento.
(Fase di osservazione/analisi). Adeguati strumenti di crawling, così come una workforce di utenti che frequentano Twitter (potrebbero essere anche utenti civetta), potrebbero rilevare e segnalare tempestivamente alcune informazioni che caratterizzano l'evento alla piattaforma. In prima istanza la piattaforma filtrerebbe le segnalazioni, valutandone l'attendibilità e analizzando le eventuali correlazioni, per individuare effettive condizioni degne di attenzione e scartare invece segnalazioni isolate o comunque poco attendibili.
Successivamente la piattaforma potrebbe coinvolgere una workforce esperta, che sarebbe chiamata a confermare o meno le segnalazioni accedendo alla pagina di Twitter, verificandone l'effettivo contenuto e aggiungendo o correggendo eventuali informazioni utili (es. livello di criticità, tempistiche, location).
(Fase di decisione/azione.) Nel caso in cui la segnalazione fosse confermata, la piattaforma potrebbe pre-allertare gli organi istituzionali e coinvolgere la workforce dislocata sul territorio (nei luoghi e negli orari confermati) per effettuare una serie di sopralluoghi di verifica. La piattaforma potrebbe anche informare i cittadini dell'evento proponendo soluzioni alternative per fruire certi servizi (e.g. accesso al centro storico).
(Fase osservazione/analisi.) Qualora la workforce presente in loco osservasse effettivamente situazioni anomale, quali disordini o illeciti di varia natura, potrebbe contribuire ad arricchire la segnalazione fornendo informazioni aggiuntive, dettagliando la situazione e stabilizzando o innalzando il livello di

criticità.
(Fase decisione/azione.) A questo punto, eventualmente dopo un ulteriore passaggio di analisi, la piattaforma potrebbe essere indotta a segnalare l'emergenza immediata a una workforce "dedicata" (le forze dell'ordine) che potrebbe intervenire per ripristinare l'ordine pubblico o mitigare il rischio di involuzioni violente, danni al patrimonio o pericolo per l'incolumità delle persone.
Da notare che nel progetto, per sua natura, la workforce è un concetto logico: chiunque può rappresentare in linea di principio una fonte di informazione e allo stesso tempo fruire delle informazioni fornite da altri (prosumers: produttori e consumatori di informazioni). In tale modello chiunque può essere attore e spettatore. È la pervasività del concetto di crowd che rende il modello potente ed efficace.
Ovviamente, al fine di rendere il suddetto modello realmente realizzabile ed utilizzabile, vi sono delle problematiche da affrontare e che il progetto studierà approfonditamente. Alcune problematiche sono le seguenti:
- la diversità dei vari social media che possono fornire informazioni rilevanti alle varie applicazioni di gestione delle emergenze e di eventi potenzialmente pericolosi o rischiosi: la diversità si manifesta negli approcci (es. gli amici di Facebook, i follower di Twitter, ecc.), i contenuti (es. testo, immagini, video, ecc.), i modelli di interoperabilità (forniscono informazioni, offrono delle APIs, ecc.);
- la grande mole di informazioni potenzialmente disponibili e quindi la capacità di selezionare e filtrare quelle rilevanti (la rilevanza è da intendere come una proprietà dinamica: una stessa informazione potrebbero essere rilevante o meno in momenti diversi, in funzione delle esigenze e del contesto nei vari momenti);
- la capacità di estrarre informazioni utili da dati non strutturati (es. i tweet, i blog, i post su un forum, tutti scritti in linguaggio naturale; anche le immagini rientrano in questa categoria);
- la capacità del sistema di integrare e correlare la grande mole di dati ed estrarne informazioni che caratterizzano e descrivono l'evento da monitorare, prevenire, gestire e mitigare e che determinano il quadro complessivo della "situazione";
- la capacità del sistema di determinare ed organizzare gli interventi, supportando i decisori umani in tutte le fasi della gestione dell'emergenza;
- la verifica e la valutazione della veridicità e dell'attendibilità delle informazioni fornite dagli utenti o presenti sui social media, in relazione ai dati ed alle informazioni fornite dai sensori o da sorgenti istituzionali;
- la selezione di informazioni realmente utili e rilevanti tra tutte quelle ricevute dalla folla o inserite nei social media, soprattutto in presenza di grandi moli di segnalazioni e sensori umani per lo stesso evento/fenomeno;
- la valutazione della dimensione "tempo" in relazione alle informazioni ricevute, oltre alla ovvia georeferenziazione: questo aspetto riveste un importanza assoluta nel caso di gestione di eventi anche potenzialmente pericolosi per la società e da gestire in maniera tempestiva;
- la "motivazione" delle persone (i sensori umani) nel fornire informazioni utili dal campo, dalla strada, dal luogo di accadimento di un certo evento: perché dovrebbero farlo ?
- Queste ed altre problematiche sono meglio descritte nella successiva sezione "stato dell'arte".

Stato dell'arte
Il progetto Secure! mira a studiare modelli, meccanismi, tecnologie e strumenti per gestire eventi e situazioni di emergenza, di crisi e di pericolo sfruttando prevalentemente le potenzialità del crowd, caratterizzato da un'enorme quantità di dati multimodali presenti nei social media (crowdsourcing) e dalla disponibilità dei cosiddetti "sensori umani" (crowdsensing).
Un elenco delle soluzioni state-of-the-art per la gestione degli eventi critici/emergenze, principalmente prodotti di imprese, è presentato di seguito:
■ N4C E-TEAM: è un sistema multi-utente basato su un browser web per la gestione delle informazioni relative a eventi. Permette un rapido aggiornamento dello stato, delle risorse e delle situazioni, e permette il tracciamento delle azioni degli utenti in base al loro ruolo.
■ OpsCenter: è un'applicazione internet per la gestione di eventi critici e eventi speciali, come ad esempio eventi che vedono la partecipazione o il coinvolgimento di un alto numero di persone. Permette il controllo di numerosi eventi, anche per mezzo di una tecnologia multi-screen; permette inoltre la creazione di report, per gli utenti accreditati che accedano al sistema.
■ SoftRisk: software di gestione delle emergenze e eventi critici che permette di aggregare informazioni di svariati tipi. È improntato alla possibilità di gestire un levato numero di tipi di file, compresi formati CAD. sono presenti funzioni di mappatura e di reportistica.
■ WebEOC: improntato alla pianificazione e gestione delle informazioni in tempo reale di eventi critici o emergenze. È stato ideato sulle caratteristiche di un centro operativo e permette di visualizzare stati, mappe, collegamenti a link esterni, mappe tattiche per agenti specifici, come polizia, vigili del fuoco, ...
■ S.A.F.E.R.: è una soluzione multi agente per la gestione della crisi, che permette di coprire le varie fasi dell'emergenza (attenuazione, stato di allerta, risposta, recupero dalla crisi) attraverso

sottosistemi che coinvolgono le comunicazioni con un call center, la gestione delle risorse a disposizione, il tracking delle risorse in gioco, pianificazione di scenari, rischi maturali, rilevazioni meteo e di sensoristica, in modo da rispondere in maniera efficace alla crisi stessa.
■ EOC System: gestionale basato su Microsoft Word e Excel che fornisce template form per la redazioni di manuali operativi. Fornisce un diagramma completo su come creare un centro operativo, su come creare e distribuire informazioni e un piano di risposta operativa per 13 differenti scenari.
Alcuni prodotti di impresa per la diffusione delle informazioni e dettagli in caso di emergenza sono i seguenti:
■ InterGraph Public Safety: è una soluzione che fornisce agli operatori uno strumento in grado di creare e aggiornare dettagli degli eventi, gestire risorse critiche attraverso l'interazione real time di dati cruciali. È possibile combinare queste informazioni con dati storici e ricerche locali, in modo da ottenere tutte le informazioni possibili per prendere le opportune decisioni urgenti. Include interfacce radio e di comunicazione in generale per una distribuzione dati veloce ed efficiente.
■ Mission Mode: applicazione web che permette di trasmette allerta a migliaia di persone e di tracciare le risposte in tempo reale. Le trasmissioni web sono criptate per incrementare la sicurezza di comunicazione, ed è presente un sistema di ricezione e verifica delle risposte automatico, e molto altro. Gli allerta sono inviati sia attraverso la linea telefonica tradizionale, cellulare, SMS, e-mails.
■ N4C: E-SPONDER: permette la condivisione di informazioni critiche durante le collaborazioni per attività quotidiane, eventi particolari e emergenze. È altamente personalizzabile e in grado di gestire i bisogni tipicamente presenti in caso di emergenze, che possono superare le caratteristiche di gestionali quotidiani.
Alcuni progetti rilevanti per Secure! sono i seguenti:
Ambito comunicazioni
■ SECRICOM: (Seamless communication for crisis management): mira alla definizione di una piattaforma di riferimento per le operazioni di gestione delle emergenze a livello Europeo, con essenzialmente due scopi: (A) mitigare i problemi delle attuali infrastrutture di comunicazione (Tetra, GSM, Citizen Band, IP) come la bassa interoperabilità, vulnerabilità allo spionaggio e al cattivo uso, problemi nel recupero da guasti, ecc, e (B) aggiungere nuove funzioni ai servizi esistenti per rendere le comunicazioni più efficaci e utili per gli utenti. Il progetto prende in considerazione sensori chimici e fisici e la loro integrazione, al fine di sviluppare una piattaforma ICT aperta per la mobilità e per i requisiti tempo-critici delle operazioni di USaR.
■ IDIRA: (Interoperability of data, systems, tools and equipment): l'obiettivo principale è di creare una infrastruttura architetturale e una implementazione esemplificativa di una struttura di Comando e Controllo Integrata Mobile, in grado di supportare la gestione di disastri su larga scala. L'idea è di prendere in considerazione tutte le idee esistenti, le tecnologie e gli standard e di completarle con nuovi componenti eventualmente necessari.
Ambito sensoristica
■ DITSEF (Digital and innovative technologies for security and efficiency of first responders operation): mira a incrementare l'efficienza e la sicurezza del personale in azione attraverso la raccolta e la distribuzione di informazioni ottima con i loro supervisori. L'obiettivo è di fornire una comunicazione robusta anche dove le infrastrutture presenti siano compromesse, posizionamento anche in ambienti indoor, sensoristica che metta in allerta da situazioni di potenziale rischio (esplosivi, chemici, fuoco, ecc.).
■ ESS (Emergency support system): mira al miglioramento di tecnologie per la raccolta dati (radioattività, bio-chimici, audio-video, etc.) installati sia su piattaforme mobile che fisse, in modo da fornire una copertura completa delle aree di interesse, dati che poi saranno fusi e analizzati per fornire un supporto in real time.
■ WICOSMO (Wireless Cognitive Sensors Network per Monitoraggio ambientale): affronta lo studio di una rete di sensori capace di prendere decisioni con grande affidabilità. Questa rete è composta da sensori relativamente semplici, e quindi poco costosi, che rendono possibile un'economia di scala. Il fattore principale di innovazione risiede nel meccanismo che rende possibile un processo di decisione distribuito. La strategia proposta non richiede, necessariamente, la presenza di un nodo centralizzato cui tutti i sensori debbano far pervenire le loro decisioni parziali, per poter ottenere la decisione finale. Ciò elimina, a priori, i problemi di congestione tipici delle reti di sensori attuali. La tecnica proposta è di vasta applicabilità e costituisce uno strumento di cui possono beneficiare sia centri industriali presenti nella Regione Toscana, al fine di ridurre i costi di monitoraggio di strutture meccaniche complesse, sia enti civili preposti al monitoraggio ambientale. Un ulteriore punto qualificante del progetto è lo studio di una rete di comunicazione geografica in grado di assicurare la comunicazione dati e voce (e più in generale multimediale) in completa sicurezza sull'area monitorata e tra essa e il centro di gestione dei dati raccolti.
Utilizzo di sensori "umani" e integrazione di vari ambiti
■ RATIONAL: il progetto si propone di sfruttare i dispositivi mobili che la maggioranza delle persone ha a disposizione (smart phones, PDA) in grado di effettuare una connessione continua tra di loro, per esempio attraverso una connessione blue-tooth o wi-fi. Questa cosiddetta mobile network of

individuals si pensa che sia in grado di diventare una importante tecnologia della società futura. I messaggi e la comunicazione possono fluire agevolmente tra i vari nodi della rete e quindi tra le varie persone, e anche in caso di eventi critici o emergenze questa infrastruttura di rete può essere determinante nella diffusione di informazioni utili, e nel coadiuvare le operazioni di soccorso e recupero. Il fatto di essere una rete completamente aperta e a disposizione di tutti pone però anche dei limiti di sicurezza e affidabilità; scopo del progetto è quindi lo studio e la costruzione di meccanismi per costruire un sistema sicuro e distribuito basato su reti mobili di individui.
■ INFRA (Innovative and novel first responders applications): l'obiettivo del progetto è la ricerca e lo sviluppo di tecnologie innovative per sistemi di supporto digitali, come parte di un sistema di gestione dell'emergenza in aiuto alle forze di soccorso. Mira a creare da un lato un sistema interoperabile che garantisca una comunicazione efficiente tra tutti i gruppi operativi, il comando e il centro operativo, e dall'altro di fornire nuove e utili applicazioni, come sistemi di navigazione indoor, applicazioni di imaging termico, sensoristica a fibra ottica, ...
I prodotti presenti in commercio sono essenzialmente dei gestionali che permettono di raggruppare messaggistica, reportistica e tracking del personale di soccorso presente sul luogo dell'evento. In nessuna delle soluzioni e dei progetti summenzionati si parla di prevenzione: questi progetti intendono la gestione dell'emergenza come gestione una volta che l'emergenza è già avvenuta. Il progetto Secure! presenta diverse direzioni di avanzamento dello stato dell'arte legate principalmente all'utilizzo di nuove tecnologie, capaci di portare un nuovo contributo e una nuova efficienza alla gestione stessa, e a un uso sinergico dei risultati di diverse aree tematiche scientifico-tecnologico. In particolare, i punti di forza della proposta Secure! sono correlati alle seguenti direzioni:

1. il crowdsourcing e il crowdsensing, sia come tematiche generali emergenti che stanno diventando sempre più diffuse, che come applicazione per la prevenzione, anticipazione e gestione di situazioni di emergenza/crisi, di sicurezza pubblica e di protezione civile;

2. l'acquisizione e la raccolta di dati da sorgenti multiple;

3. l'integrazione e l'analisi di informazioni, soprattutto raccolte dai social media;

4. situation awareness, early warning system (EWS) e supporto decisionale che rivestono un ruolo fondamentale per il modello di sistema che il progetto vuole proporre.

5. infine, le problematiche di sicurezza, trust, privacy ed affidabilità delle informazioni raccolte e gestite sono anch'esse studiate ed analizzate nel contesto del progetto Secure!.
Tutte le suddette aree sono discusse nel seguito, analizzandone brevemente lo stato dell'arte ed evidenziandone l'avanzamento proposto dal progetto.

1. Crowd-sensing/crowd-sourcing applicato alla prevenzione, anticipazione e gestione di situazioni di emergenza/crisi, di sicurezza pubblica e di protezione civile
Il termine "crowdsourcing" in genere si riferisce alla capacità di ottenere informazioni e/o contributi su un particolare progetto e/o compito, servendosi delle competenze di un certo numero di persone, sia pagate che non, tipicamente via Internet (Oxford Dictionary). Neologismo (da crowd, gente comune, e outsourcing, esternalizzare una parte delle proprie attività) coniato per la prima volta nel 2006 da Jeff Howe sulla rivista Wired [How06].Il Crowdsourcing è, quindi, un modello di business in cui una azienda o una istituzione individua una o più attività, tradizionalmente eseguite da dipendenti incaricati, e le assegna in outsourcing ad un gruppo di persone, generalmente molto vasto e non definito a priori (il crowd), secondo un modello ad open call.
Storicamente, le tipologie di attività che meglio si prestano a questo modello sono in generale quelle legate al problem solving ed alla generazione di conoscenza e/o contenuti. Inizialmente tale modello era stato pensato per sfruttare una parte della potenza di calcolo dei PC delle persone comuni, al fine di velocizzare le ricerche. Il primo e più famoso esempio è SETI@home (http://setiathome.berkeley.edu/), un progetto di calcolo distribuito volontario creato all'Università di Berkeley per analizzare i dati provenienti dallo spazio profondo, captati dai radiotelescopi.
La vera rivoluzione è avvenuta quando si è passati dallo sfruttamento della potenza di calcolo dei computer all'utilizzo dell'intelligenza e dell'intuito degli internauti.
La forza del crowd sta nella molteplicità delle risorse a disposizione e quindi nella possibilità di scelta fra tutti i vari contributi che arrivano da professionalità e talenti diversi.
Le caratteristiche peculiari del crowdsourcing possono essere così sintetizzate:
- le interazioni con il crowd avvengono attraverso il web (internet),
- il processo viene iniziato da una azienda o una organizzazione che necessita di eseguire alcune attività oppure deve risolvere un problema,
- l'esecuzione delle attività richieste è affidata al crowd (un vasto gruppo di utenti sconosciuti) e non ad altre aziende/organizzazioni, nè a singoli individui,

- generalmente il coinvolgimento del crowd avviene in forma di open call.
Le iniziative di Crowdsourcing possono essere classificate in funzione della tipologia delle attività che devono essere eseguite, secondo le tre seguenti macro categorie principali:
- idea game: consiste essenzialmente in una chiamata di massa per la discussione e/o lo sviluppo di idee esistenti o nuove; si tratta di un Crowdsourcing selettivo, in cui l'azienda iniziatrice deve poi verificare tutti i contributi ricevuti e selezionare il subset delle soluzioni migliori e premiare i vincitori,
- problem solving: questo è lo scenario in cui un utente ha un problema da risolvere e lo sottomette ad un vasto insieme di potenziali risolutori (il crowd); si tratta di un Crowdsourcing integrativo, in cui una soluzione completa viene costruita integrando i molteplici contributi ricevuti,
- prediction market: il crowd viene coinvolto in simulazioni di scenari futuri e i vari responsi vengono utilizzati per generare delle previsioni, ad esempio su come i mercati potrebbero rispondere all'ingresso di nuovi prodotti.
Non esiste un criterio preciso per stabilire quali attività possano essere abilitate con successo al Crowdsourcing, ma in generale non è da ritenersi adeguato ad attività produttive, vista la distribuzione sconosciuta delle risorse.
La tendenza è di valutare l'opportunità di realizzare in Crowdsourcing una determinata attività in funzione delle competenze necessarie per la sua esecuzione da parte degli individui del crowd, individuando quindi tre tipologie di attività:
- attività semplici: rientrano in questa classe le attività che possono essere descritte facilmente e non richiedono sforzo elevato o esperienza rilevante per essere comprese dagli individui del crowd, inoltre possono essere portate a termine con un coinvolgimento relativamente contenuto; il valore aggiunto per questa tipologia di attività non consiste tanto nelle abilità di chi le porta a termine, quanto nel loro basso costo: questo è in caso di contributi volontari, piccoli incentivi o anche la soddisfazione personale nel contribuire ad obiettivi e benefici pubblici,
- attività complesse: sono in generale caratterizzate dalla possibilità di avere soluzioni e percorsi di soluzione non univoci, oltre alla presenza di incertezza sul risultato; la loro comprensione ed esecuzione richiedono competenze specifiche, capacità di problem solving e sforzo cognitivo: questo tipo di attività richiede schemi di incentivazione e remunerazione più articolati,
- attività creative: sono quelle in cui la creatività e l'originalità hanno la maggiore rilevanza: l'obiettivo più importante in questi casi consiste nell'accesso alla potenza creativa offerta dal crowd, ovvero un vasto gruppo variegato e interdisciplinare di individui; in questo caso il modello di incentivazione e remunerazione si colloca in una posizione intermedia rispetto alle altre tipologie di attività.
Vari studi su casi reali mostrano come, a partire da queste tre macro tipologie di attività, sia possibile ricondurre al Crowdsourcing molte attività in ambito economico/industriale, nel campo dei servizi e perfino in ambito scientifico.
L'esecuzione di attività secondo il modello del Crowdsourcing può essere schematizzata attraverso un processo sequenziale che attraversa le seguenti fasi consecutive:
- preparazione: viene identificata l'attività che deve essere eseguita in Crowdsourcing; fattore critico di successo in questa fase è la corretta definizione del perimetro dell'attività,
- inizializzazione: vengono espletate tutte le attività di preparazione, quali ad esempio la definizione del problema o dell'obiettivo, la stesura della sua descrizione, la definizione dei criteri di valutazione, il setup delle piattaforme tecnologiche necessarie e la preparazione della pubblicazione della attività; fattore critico di successo in questa fase è l'individuazione della piattaforma adeguata a supporto dell'attività
- esecuzione: l'attività viene pubblicata e il crowd fornisce le proprie risposte, interagendo eventualmente con il committente per avere chiarimenti; fattori critici di successo in questa fase sono la stabilità della piattaforma e l'applicazione di un adeguato controllo della qualità,
- valutazione: tutti i contributi ricevuti vengono esaminati e valutati secondo i criteri prestabiliti; fattore critico di successo in questa fase è la disponibilità di sufficienti risorse per la revisione di tutto il materiale,
- finalizzazione: in questa fase il committente traduce le soluzioni ricevute (e selezionate) in prodotti, servizi e funzionalità che devono confluire in un ulteriore processo di innovazione e/o sviluppo.
I fattori di successo del Crowdsourcing in generale possono essere così riassunti:
- individuazione accurata delle attività da eseguire,
- definizione chiara dell'obiettivo desiderato,
- acquisizione del crowd, in termini di massa critica, interdisciplinarietà e competenza degli individui,
- definizione delle strategie di incentivazione e remunerazione,
- mentalità aperta e innovatrice del committente.
Da uno dei fattori di successo, deriva probabilmente il maggiore limite del Crowdsourcing, ovvero il fatto che venga applicato ad un problema ben individuato e definito dallo stesso committente, secondo la propria visione e/o percezione al momento della preparazione, quindi con un certo grado di influenza sul risultato. Questo chiaramente pone dei limiti alla libertà di azione del crowd, e manifesta maggiormente i propri effetti sulle attività di tipo creativo, che più dovrebbero poter contare sulla massima libertà all'espressione degli individui.

Due sono le principali direzioni in cui si sta muovendo il Crowdsourcing: evoluzione delle piattaforme esistenti e esplorazione di nuovi fenomeni.
Per quanto riguarda l'evoluzione delle piattaforme esistenti, si considerano i seguenti aspetti:
- miglioramento dei supporto per la definizione e la descrizione di attività complesse,
- miglioramento del supporto per i controlli di qualità e l'assurance delle procedure,
- introduzione di meccanismi semi-automatici per la valutazione delle soluzioni e/o dei contributi,
- rafforzare l'integrazione fra Crowdsourcing e processi aziendali.
Per quanto riguarda, invece, l'esplorazione di nuovi fenomeni, si prendono in considerazione scenari in cui ad iniziare il processo non sia una azienda o una organizzazione, ma gli utenti stessi (ad esempio la proposta di nuove idee/prodotti/servizi non regolata o invocata dall'azienda, ma su spontanea iniziativa degli utenti), oppure l'analisi dei comportamenti e/o delle discussioni degli utenti all'interno di Social Network e siti di informazione collaborativa, oppure ancora il ricorso al crowd come rete di sensori umani (crowdsensors). In particolare, l'utilizzo dei "sensori umani" ha dato vita in questi ultimi anni a una nuova frontiera di applicazioni mobile, denominata mobile crowdsensing (MCS), in cui si utilizzano i dispositivi mobili (sensing and computing devices), per consentire di misurare e mappare fenomeni di interresse comune basandosi sullo cambio e sulla condivisione di informazioni tra gli individui [GYL11].
La diffusione di dispositivi mobili quali Smartphone, gaming console e dispositivi di navigazione veicolare risulta costantemente in crescita, di pari passo con la rapidissima evoluzione che sta avendo la tecnologia in questa area, tanto che ormai in tutti questi dispositivi sono presenti uno o più sensori (accelerometri, microfoni, GPS, sensori luce, fotocamere, sonar) che permettono di collezionare un gran numero di informazioni. Di conseguenza, il termine mobile crowdsensing abbraccia un'ampia gamma di applicazioni di rilevamento e di monitoraggio di fenomeni collettivi sia participatory sensing [B+06] che opportunistic sensing [N+10] classificabili in tre grandi categorie principali:
- ambientali: livelli di illuminazione, livelli di rumore, qualità dell'aria, immagini e riprese,
- infrastrutturali: posizione, mobilità, traffico e controllo del transito,
- sociali: condivisione di percorsi, foto, frequentazione di luoghi.
Un esempio è di applicazione MCS ambientale è quello di Common Sense (http://www.sense-os.nl/crowd-sensing), una piattaforma cloud-based per la raccolta, l'integrazione e la condivisione di dati sensoriali provenienti da Sense Platform app, MyriaNed wireless sensor networks, GPS-trackers e Open data per il rilevamento del livello di CO2 e NOx in diverse zone della città.
Relativamente alle applicazioni MCS infrastrutturali sono stati realizzati due progetti, CarTel del MIT [HBC+06] e Nericell del laboratorio di ricerca della Microsoft [MPR08], dove si utilizzano dispositivi di rilevamento in-vehicle e telefoni cellulari per fornire informazioni sulle strade con rallentamenti, sulle zone di traffico ma anche sui livelli di inquinamento acustico da clacson e sulla presenza di buche in strada. Il progetto ParkNet [M+10], invece, fornisce informazioni in tempo reale sulla disponibilità di parcheggi in città a tutti quegli utenti che ne fanno richiesta a partire dei dati sensoriali inviati al server centrale dai veicoli equipaggiati di ricevitore GPS e di un telemetro a ultrasuoni per la determinazione dell'occupazione del posto auto.
Per concludere, con le applicazioni MCS sociali è possibile raccogliere e condividere con la comunità un insieme di dati e informazioni legate ad attività giornaliere, come ad esempio andare in bicicletta [E+07] oppure cucinare [R+07] con l'obiettivo di migliorare lo stile di vita e preservare la salute
Gli aspetti differenzianti di queste nuove classi di sensori rispetto alle comuni reti di sensori sono:
- dispongono di elevate capacità di computazione, di connettività e di immagazzinamento dei dati,
- la loro diffusione sul campo è già molto vasta ed in continuo e rapido aumento,
- si possono realizzare ad un costo minore e in minor tempo applicazioni sensor-based sfruttando i dispositivi mobili già dispiegati sul campo,
- si tratta per lo più di sensori multimodali, ovvero in grado di fornire varie tipologie di misure.
La grande varietà di questi dispositivi, tuttavia, porta con sè una intrinseca non uniformità dei dati forniti, soprattutto in termini di precisione, sensibilità e taratura delle misurazioni, dovuta principalmente ai diversi sensori utilizzati dai produttori, ma anche al software che si trova a bordo dei dispositivi (OS). Per questo motivo è richiesta una fase di preprocessing per fare in modo che i dati inviati ai centri di raccolta dati siano resi uniformi e compatibili per successive fasi di analisi e correlazione, e questo è possibile proprio grazie alla capacità computazionale già disponibile a bordo, che può ospitare una micro applicazione mediatrice.
Alla fase di preprocessing, inoltre, è affidato il problema della gestione degli aspetti di privacy.Infatti, poiché i dispositivi sono associati (di proprietà) ai singoli individui, di solito quest'ultimi sono parte attiva del ciclo stesso. Questo vuol dire che da una parte, si può sfruttare l'intelligenza umana per la raccolta di dati più affidabili e realistici di quanto non si faccia con sofisticati sistemi hw e sw. D'altra parte, vi sono delle forti ripercussioni sugli aspetti di privacy e sui meccanismi di incentivazione, legati alla reticenza di condividere o inviare dati sensibili.
Una successiva fase di analisi dei dati, eseguita generalmente nel backend dei centri di raccolta dati, permette di filtrare le informazioni rilevanti, correlare dati ed eventi, individuare eventuali dipendenze e/o pattern e possibilmente elaborare modelli predittivi a supporto di una moltitudine di attività sul

territorio.
L'applicazione dei principi e degli strumenti di crowdsourcing alla gestione di situazioni di emergenza, per quanto ancora agli albori, presenta ovviamente alcune infrastrutture di supporto ed alcune sperimentazioni. Alcuni casi applicativi sono già stati riportati nella sezione precedente ("Idea alla base del progetto"); altri sono riportati nella sezione "Obiettivo generale". Al livello tecnologico, Ushahidi è un'infrastruttura Open Source che consente di segnalare incidenti/problemi e di ricevere avvisi. È stata inizialmente sviluppata per riportare ed aggregare su una mappa incidenti di violenza e sforzi di pace in Kenia dopo le elezioni del 2008, segnalazioni pervenute via Web e telefoni cellulari. Oggi Ushahidi è una soluzioni di crowdsourcing e filtraggio in tempo reale di informazioni.
Avanzamenti rispetto allo stato dell'arte.
Le applicazioni del crowdsensing e del crowdsourcing per la prevenzione, anticipazione e gestione di situazioni di emergenza/crisi, di sicurezza pubblica e di protezione civile sono ancora oggi ad uno stato decisamente non maturo, dal punto di vista teorico (es. lo studio olistico del sistema soci-tecnico che risulta), dal punto di vista tecnologico (tutte le problematiche di raccolta, estrazione, analisi, correlazione dei dati e delle informazioni e dei meccanismi di supporto decisionale, nonché gli aspetti di sicurezza, privacy, trust, affidabilità; tali problematiche sono discusse in dettaglio nel resto di questa sezione sullo stato dell'arte) e dal punto di vista organizzativo (es. come cambiano i processi ed i modelli di organizzazione con l'adozione del crowsourcing).
In particolare i social media ed il crowdsourcing sono stati parzialmente utilizzati nel contesto di gestione di crisi ed emergenze soprattutto per distribuire informazioni e ricevere feedback dalla gente durante la situazione da gestire (come nel caso dell'uragano che ha investito un'area in Belgio in cui si teneva un festival musicale; i partecipanti, circa 60.000 mila persone, sono stati avvertiti ed istruiti via SMS, come riportato qui http://www.bbc.co.uk/news/world-europe-14582448). La stessa piattaforma Ushahidi, per quanto possa costituire un ottimo punto di partenza infrastrutturale, non possiede tutte le caratteristiche per la prevenzione, anticipazione e gestione delle emergenze, così come immaginato nel contesto di questo progetto.
In questo senso mancano ancora tanti elementi che il progetto Secure! propone, come componenti innovative per l'estrazione automatica di informazioni da sorgenti dati non strutturate (testo, immagini, ecc.), l'analisi di dette informazioni al fine di determinare un "quadro della situazione", il coordinamento degli interventi in maniera flessibile ed orientato al raggiungimento di certi obiettivi, il collegamento logico-informativo tra tutti gli attori coinvolti nelle fasi di prevenzione, anticipazione e gestione di emergenze e situazioni pericolose. Tutti questi elementi innovativi, insieme ad altri descritti nel seguito, sono presenti nella proposta Secure!.
Altre problematiche, come la diversità dei vari social media, la verifica e la valutazione della veridicità e dell'attendibilità delle informazioni fornite dagli utenti o presenti sui social media, la selezione di informazioni realmente utili e rilevanti tra tutte quelle ricevute dalla folla o inserite nei social media, la motivazione dei sensori umani nel fornire informazioni utili, saranno tutte studiate ed analizzate, al fine di determinare soluzioni e componenti da integrare nel Secure! Framework e che rappresenteranno altri elementi di innovazione rispetto a soluzioni esistenti. Soprattutto l'integrazione di tutti i suddetti aspetti rappresenta il maggiore elemento di innovazione che il progetto propone, a fronte di soluzioni ed approcci che includono solo uno o pochi di essi. A titolo di esempio, l'apparentemente semplice "bi-direzionalità" nella comunicazione tra gli attori coinvolti è una caratteristica praticamente inesistente nel panorama delle applicazioni "reali" del crowdsorcing alle situazioni di emergenze e pericolo. Ed ovviamente la bi direzionalità è un requisito fondamentale della presente proposta.

2. Acquisizione di informazione da sorgenti multiple (web, crowds, sensors, …)
Un problema molto attuale e spesso ricorrente è relativo alla collezione, manutenzione ed analisi di grandi moli di dati da sorgenti eterogenee e distribuite. Questo problema si presenta in molteplici ambiti; si pensi ad esempio ai grandi sistemi di telecomunicazione e alle relative applicazioni per il marketing e l'identificazione di frodi, dove i dettagli della chiamate sono di fondamentale importanza: conseguentemente, le compagnie di telecomunicazioni mantengono registrate e gestiscono informazioni per miliardi di chiamate effettuate [IF11]. Altri esempi possono essere invece la gestione dei dati privati dei cittadini da parte delle infrastrutture di servizi offerti dalla pubblica amministrazione, oppure ancora la mole di informazioni fornite dai vari sensori installati ai fini del monitoraggio e controllo delle grandi infrastrutture critiche. Al problema della gestione di grandi moli di dati, si affianca sempre più spesso la necessità di manipolare dati di vario tipo e provenienti da differenti sorgenti; ovvero dati eterogenei, che devono essere comunque uniformati, integrati e gestiti in contemporanea. Lo stato dell'arte degli ultimi anni ha evidenziato importanti sforzi per affrontare queste problematiche, esplorati brevemente di seguito nei due temi:
- acquisizione, filtraggio ed analisi di grandi moli di dati, e
- diversità ed eterogeneità dei dati considerati.
Acquisizione, filtraggio e analisi di grandi moli di dati.
Menzioniamo per prima cosa approcci largamente impiegati per la gestione ed analisi di grandi

quantità di dati: per primo, citiamo approcci per l'analisi offline dei dati, ed in particolare data mining ed OLAP, e quindi citiamo approcci per l'analisi online, in particolare concentrandosi su Complex Event Processing (CEP).
Data mining è l'estrazione offline da ampi database di informazioni nascoste, ed è una tecnologia con potenziale per aiutare a identificare le informazioni più importanti in grandi database [HKP12]. L'istituto SAS definisce il data mining come il processo di selezionare, esplorare e modellare larghe quantità di dati per scoprire (ad esempio, al fine di studi economici o commerciali) pattern precedentemente sconosciuti [Sas00]. Ad esempio, alcune tecniche di data mining permettono alle industrie di telecomunicazioni di stimare quanto un cliente sta per abbandonarli (valutare altre offerte) [IF11]. In maniera correlata al data mining, l'OLAP (On-Line Analytical Processing, [KRT08]) è una tecnologia che permette di effettuare analisi complesse su informazioni memorizzate in una struttura dati multi-dimensionale, tipicamente un data warehouse (un repository globale che contiene grandi quantità di dati estratte da sistemi eterogenei) [KRT08], per mettere in evidenza un'analisi particolare dei dati.
Quando l'obiettivo dell'analisi è osservare un flusso di informazioni online e non offline su dati raccolti in precedenza, è necessario appoggiarsi a tecniche differenti da OLAP e data warehouse, ad esempio per raccogliere e filtrare i dati, ricavandone risultati intermedi da offrire poi a servizi decisionali. Con Complex Event Processing (CEP, [BK09]) si intende un insieme di tool e tecnologie per analizzare e controllare la complessa serie (il flusso) di eventi correlati che caratterizzano i sistemi di informazioni moderni. Un sistema CEP monitorizza flussi di eventi e contiene informazioni riguardo cose che accadono in tempo reale, differentemente dalle tecnologie menzionate in precedenza, che analizzano dati statici raccolti e memorizzati in precedenza. Le applicazioni che devono gestire flussi di eventi ed effettuare rapidamente decisioni (intelligenti) come risposta ai cambiamenti e alle condizioni che si evolvono come nel caso di Secure! sono validi candidati per l'utilizzo di tecnologie basate sull'Event Processing. Per capire l'impatto di queste applicazioni, citiamo come esempio le real-time supply chain (letteralmente, catene per la fornitura in tempo reale): nella industria della vendita al dettaglio e relativa logistica, tecnologie quali RFID (Radio Frequency Identification) rappresentano un'opportunità per automatizzare la catena delle forniture, identificano, tracciando e registrando gli oggetti, nelle varie fasi della catena produttiva fino all'acquisto, per definire le strategie più opportune per la gestione della produzione, la distribuzione degli ordini, ecc.
Diversità ed eterogeneità dei dati considerati.
La diversità ed eterogeneità dei dati richiede l'applicazione di opportune trasformazioni e integrazioni, prima che i dati possano essere passati al sistema decisionale vero e proprio. L'integrazione di dati è tuttora un tema rilevante in vari ambiti, dove è necessario effettuare una rapida integrazione di informazioni provenienti da sorgenti eterogenee, che possono includere sia dati strutturati che non strutturati.
Nello scenario moderno dei sistemi d'informazioni globali si trova un numero sempre crescente di sorgenti di dati strutturati (si pensi alle varie tipologie di database), che necessitano di uniformare le interfacce per le query, al fine di accedere a dati distribuiti su una eterogeneità di piattaforme, dove sono rappresentati in modo eterogeneo [CdA01].
Questa situazione è resa più complessa quando si considerano le sorgenti di informazioni multimediali, come nel caso di Secure!, dove si attinge contemporaneamente a dati provenienti da differenti sorgenti (immagini fornite da video-camere di sorveglianza, fornite da utenti del sistema Secure!, oppure prelevate automaticamente da social-network). Ovviamente tali dati sono eterogenei sia nella forma che nei contenuti, richiedendo una attenta logica di analisi e di filtraggio. Si rilevano in questo settore alcune interessanti iniziative, quali quelle del progetto TSIMMIS (The Stanford - IBM Manager of Multiple Information Sources, [CGHI94]), che si propone di fornire strumenti per accedere in modo integrato a molteplici sorgenti di informazioni sia strutturate che semi-strutturate, e assicurare che le informazioni ottenute siano consistenti. Ad esempio, si propone di identificare soluzioni per tradurre query ed informazioni, estrarre dati dal Web, combinare informazioni da varie sorgenti. Similarmente si possono identificare molte iniziative nella stessa area, come il Web mining [KB00], cioè l'applicazione di tecniche di data mining volte a scoprire pattern sul Web, o la integrazione di informazioni semantiche mediante ontologie [Noy04].
Avanzamenti rispetto allo stato dell'arte.
Secure! richiede di raccogliere, armonizzare e fondere informazioni provenienti da differenti social network e media, con informazioni raccolte tramite altri mezzi di informazione quali la segnalazione da parte del cittadino tramite applicazioni mobile specifiche, oppure fornite interconnettendosi con servizi pubblici quali 118 e 113. Le problematiche illustrate sopra sono esacerbate nel contesto di Secure!, che richiederà quindi di avanzare lo stato dell'arte costruendo una rete di servizi tale da risolvere le seguenti problematiche:
- l'eterogeneità e la mole dei dati gestiti in Secure! richiede la definizione di procedure e soluzioni apposite per la loro integrazione e gestione, nonché per la rapida scalabilità per includere nuove tipologie di dati. A titolo di esempio, si consideri la possibile introduzione del sistema di nuovi sensori, e quindi di nuovi tipi di dati (e una nuova quantità addizionale di dati) che saranno gestiti dal sistema

di collezione, filtraggio e integrazione.
- l'eterogeneità e la quantità delle sorgenti richiede un layer di integrazione per gestire informazioni da differenti canali, quali canali tradizionali di segnalazione, apps, fino a social network o siti web. Questo richiede di definire non anche una serie di politiche per la valutazione delle sorgenti e la loro rilevanza, nonché una differenziazione sull'analisi effettuabile a seconda della sorgente. A titolo di esempio, si pensi a fotografie su cui si possono prevedere attività di analisi diverse qualora la foto sia scattata da un umano, che è in grado di "elaborare" la scena per focalizzare la foto sull'oggetto in esame, oppure da una telecamera fissa.
Secure! avanza quindi lo stato dell'arte definendo sia un modello informativo per la gestione dei dati per crisi ed emergenze, sia un layer di interfacciamento e integrazione con tutti i più importanti e rilevanti social media e network, nonché con svariate sorgenti di dati. Questo richiederà di integrare tecnologie state-of-the-art per la gestione di grandi moli di dati, sia online che offline, con servizi e soluzioni ad-hoc per il loro filtraggio, integrazione, trasformazione e analisi.

3. Integrazione ed analisi dei dati
Arricchimento e dei contenuti testuali.
Negli ultimi anni è apparso evidente uno sforzo nella direzione del cosiddetto Web of Knowledge, con l'intenzione di creare e condividere basi di dati che contengono elementi di conoscenza strutturata. Wikipedia ne è l'esempio più popolare. Queste basi di dati esterne sono spesso usate per consentire a strumenti automatici di analisi del testo, come ad esempio i motori di ricerca web, una maggior comprensione dei contenuti testuali. Tramite un processo di Entity Linking (EL), in un testo vengono identificati tutti i riferimenti a entità e concetti descritti in dettaglio in basi di dati esterne come Wikipedia. Questo processo permette di integrare un testo con la conoscenza derivata da queste basi di dati: categorizzazione, coordinate spazio-temporali, concetti correlati, ecc. Una delle maggiori difficoltà in questo processo è quello della disambiguazione nei casi di polisemia [C07,FSE09], ad esempio il temine "Jordan" potrebbe riferirsi al giocatore di pallacanestro oppure al meno noto professore dell'università di Berkeley. Per disambiguare un termine in maniera efficace è possibile analizzare le interdipendenze con le altri entità rilevate nel documento. Se nel documento è presente il termine "NBA", quasi certamente il termine "Jordan" è un riferimento al giocatore. Tipicamente, le correlazioni fra tutte le possibili coppie di entità vengono valutate prima di scegliere la migliore disambiguazione [MW08,MWM08,KSR09]. Recentemente un nuovo approccio è stato presentato in [HSZ11] che permette di analizzare il grafo completo delle dipendenze fra le entità ed i topic che occorrono in dato documento, permettendo così di individuare e disambiguare con maggiore precisione le entità presenti. L'algoritmo proposto, inoltre, garantisce anche migliori performance in termini di costo computazionale.
Avanzamenti rispetto allo stato dell'arte.
Nell'ambito del progetto Secure! intendiamo definire delle nuove tecniche di Entity Linking che si adattino specificatamente all'analisi di contenuti testuali provenienti da Social Media. Questi sono caratterizzati da testi molto brevi, dall'uso di un linguaggio informale, e dall'uso di costruzioni sintattiche specifiche, come ad esempio gli "hashtags" di Twitter. Queste caratteristiche richiedono quindi la progettazione di nuovi algoritmi che superino lo stato dell'arte dell'analisi di contenuti testuali "tradizionali".
Raccolta e diffusione dell'informazione nei social media.
Un crawler è un sistema software progettato per la raccolta di dati dal web. Molti sono gli obiettivi perseguiti nella progettazione e nello sviluppato di un crawler, fra queste l'efficienza rispetto all'uso delle risorse sia computazionali che di rete, e rispetto (politeness) delle risorse di chi ospita contenuti web evitando accessi troppo frequenti che ne sovraccaricherebbero le infrastrutture. Ma l'obiettivo più importante rimane la copertura del maggior numero possibile di pagine web, e quest'obiettivo diventa sempre più difficile da raggiungere sia perché il web continua a crescere (si stima nell'ordine delle decine di miliardi di pagine), sia per la diffusione dei fenomeni di "web spam" che popolano una buona proporzione del web stesso. La progettazione e l'analisi di crawler ha ricevuto grande interesse da parte della comunità scientifica, a partire dai lavori di Brin and Page [BP99], Heydon and Najork [HN99], fino a lavori più recenti [SS02,BCS04,LLW08] nei quali efficienza e scalabilità sono gli obiettivi più importanti.
Esistono diversi studi che cercano di modellare le reti sociali, come ad esempio Twitter, e il processo di diffusione di informazione nei social media [BHM11, CDS10, EOS10]. Uno studio molto interessante è stato condotto su un ampio campione di Twitter da Kwak et al. [KLP10]. Gli autori hanno prodotto diverse analisi interessanti. Dopo il primo aumento di popolarità, il numero cumulativo di tweet di un trending topic aumenta in maniera lineare, come suggerito anche in [AHS11], e indipendentemente dal numero di utenti coinvolti. Quasi lo 80% dei trending topic hanno un singolo periodo di attività, e cioè spariscono subito dopo il loro periodo di popolarità, ed il 93% di questi periodi di attività dura meno di 10 giorni. Infine, una volta pubblicato un tweet, la metà dei suoi re-tweet (ovvero ri-pubblicazioni da altri utenti) ha luogo in meno di un'ora, ed il 75% in meno di un giorno. Tramite il meccanismo dei re-tweet, un'informazione raggiunge in pochissimo tempo tutti gli utenti a distanza 4

nella rete sociale (amici di amici di amici di amici). Questo ed altri studi confermano come l'informazione si possa diffondere in maniera quasi istantanea attraverso le social network come Twitter.
Data l'abbondanza di contenuti relativi a notizie in Twitter, molti degli studi relativi alla diffusione della informazioni hanno l'obiettivo di scoprire argomenti emergenti di interesse al fine di suggerire news di interesse in tempo reale. Akcora et al. [ABD10] usa Twitter per individuare improvvisi cambi di opinione basandosi su un corpus di parole che possono essere associate a specifici stati emotivi. Un cambiamento nel modo o nella frequenza dell'uso di certi termini può indicare l'accadimento di un evento o di una notizia particolare. Un primo tentativo di individuare topic emergenti ed al tempo stesso creare dei profili utente è quello proposto da Michelson and Macskassy [MM10]. Prima i tweet vengono analizzati e filtrati estraendo tutti i termini con una iniziale maiuscola, assumendo che tali termini possano essere associati ad una entità (personalità, luoghi, concetti). In seguito, questi termini vengono usati per trovare un articolo corrispondente, se esiste, in Wikipedia, e le categorie di Wikipedia associate vengono usate per etichettare tweet e profilare gli utenti. In maniera simile, il sistema descritto in [DGL12] mappa ogni singolo tweet in un insieme di entità, ciascuna corrispondente ad una pagina in Wikipedia. Lo stesso processo è applicato allo stream the news più recenti, con l'obiettivo di mappare sia le news che i contenuti prodotti dagli utenti in uno stesso spazio di entità in modo da renderli confrontabili. Il modello proposto usa anche informazioni derivate dalla rete sociale di ciascun utente, per individuare presto i topic emergenti e per produrre raccomandazioni di notizie in maniera personalizzata rispetto agli interessi del singolo utente.
Avanzamenti rispetto allo stato dell'arte.
Nell'ambito del progetto Secure! intendiamo definire nuove tecniche che permettano una analisi aggregata di molteplici sorgenti di informazione con lo scopo di individuare topic emergenti di interesse nel tempo più breve possibile. In particolare, verranno sviluppati nuovi algoritmi per condurre raccolta dati ed analisi specializzata rispetto a luoghi specifici (es. i trending topics a Firenze), o oggetti/entità di interesse (es. i trending topics relativi alla torre di Pisa).
Image Analysis.
Il progetto realizzerà strumenti per analizzare i contenuti visuali provenienti da sorgenti diverse con lo scopo di mettere in relazione contenuti equivalenti o relativi alla stessa situazione, argomento, o oggetto di interesse. Le sorgenti dei dati potranno essere devices a disposizione degli utenti o dati provenienti dal web e dalle reti sociali.
I contenuti visuali saranno analizzati per riconoscere ed identificare oggetti e situazione di interesse. Le tecniche di riconoscimento della immagini sono state usate con success in scenari limitati e ben definiti come ad esempio "Landmark recognition" [VIS] [ZZS09] [GOO], riconoscimento di dipinti [GOO], riconoscimento delle pubblicità [KOO], ect.
Per effettuare il riconoscimento tipicamente si fa uso di algoritmi di classificazione [Dud76], [AFG11] che, dato un insieme di esempi, e facendo affidamento su tipi particolari di "visual features" [Low04], sono capaci decidere se il soggetto di interesse è contenuto nell'immagine. Recentemente la ricerca si è particolarmente concentrata su tecniche capaci di ottenere allo stesso tempo alta efficacia ed efficienza.
Avanzamenti rispetto allo stato dell'arte.
Nel progetto si andrà oltre lo stato dell'arte investigando tecniche che permettono di allargare la tipologia di soggetti e situazioni che possono essere riconosciute automaticamente, cercando di andare un passo oltre alle limitazioni esistenti nelle tecniche attuali, che offrono risultati molto buoni ma in scenari molto limitati. Lavoreremo in particolare sulla scalabilità e su tecniche che permetteranno anche agli utenti non esperti di costruire riconoscitori adatti allo scopo.

4. Situation awareness, early warning system e supporto decisionale nella gestione delle crisi/ emergenze
Il supporto decisionale nell'ambito di un sistema di gestione delle situazioni di emergenza si fonda su due elementi molto importanti: il primo punto è la consapevolezza della situazione, basata sulla raccolta e l'elaborazione di informazioni provenienti da molteplici sorgenti (le sezioni 3 e 4 dello stato dell'arte affrontano proprio questi temi) e sulla successiva creazione di un "quadro complessivo ed aggiornato" della situazione da gestire, da prevenire, da prevedere, ecc.; l'altro punto è la determinazione e la gestione del cosiddetto early warning e della risposta all'emergenza, dell'intervento, delle azioni, dei piani, ecc. Questi due aspetti sono descritti e discussi nel seguito di questo paragrafo dello stato dell'arte.
Inoltre, fortemente legato alla determinazione della consapevolezza della situazione, il progetto Secure! propone anche l'integrazione di informazioni geospaziali: pertanto nel seguito viene anche descritto e discusso questo tema.
Lo stato dell'arte (rilevante per il progetto) delle suddette tre tematiche è brevemente descritto nel seguito. Dato che la soluzione proposta dal progetto Secure! per le componenti di supporto decisionale mira ad integrare (anche concettualmente) gli aspetti di situation awareness, early warning e gestione dei piani di intervento, l'avanzamento sullo stato dell'arte proposto dal progetto

sarà unico e riportato dopo le suddetto breve descrizioni separate.
Situation awareness.
Uno dei rischi principali nella gestione di processi complessi e altamente critici (e.g. crisis/emergency/ disasters management) è insito nella mancanza di una conoscenza o percezione approfondita della situazione in corso. I fattori che contribuiscono alla complessità sono: la sorpresa, la velocità con cui la crisi/emergenza si può sviluppare, la possibile estensione spaziale, il numero di persone coinvolte, l'incertezza, la possibile mancanza di risorse, la difficoltà nelle comunicazioni ed il cosiddetto effetto domino (gli eventi a cascata) [WYB06].
Diversi modelli di gestione dell'emergenza sono presenti in letteratura, ognuno con un focus diverso sui diversi aspetti proprio della gestione delle emergenze (alcuni esempio sono [WIS03] [JIN04] [SHA03] [SUJ08]). La maggior parte di questi modelli manca della capacità di adattamento dei piani di risposta ai fattori di contingenza che possono emergere durante l'emergenza. Quello che serve è mantenere in tempo reale l'interdipendenza tra eventi, azioni, attori, contesto e piani; e prevedere e supportare un elevato grado di flessibilità e dinamicità nella gestione di tali entità.
La definizione della cosiddetta "situation awareness" e la corrispondente gestione della comunicazione e dell'informazione tra i vari stakeholder rappresenta una della questioni principali da affrontare quando ci si riferisce a processi ritenuti critici [MCM07] [MIL07] [KAN06]. Nell'ambito dei progetti CHORIST (http://www.chorist.eu/) e LIAISON (http://www.liaison-project.eu/) sono state affrontate queste tematiche relativamente alle squadre di soccorso dei vigili del fuoco.
La Situational Awareness (SA) fa riferimento a quell'area di ricerca che si occupa di definire modelli, tecniche, algoritmi e sistemi in grado di percepire e rappresentare l'ambiente in contesti decisionali critici (e.g. controllo del traffico aereo, azioni militari, gestione delle emergenze), in modo da stabilire come informazioni, eventi e azioni possono condizionare in un lasso di tempo relativamente breve, i desideri e gli obiettivi finali. La chiave del concetto di situation awareness è la continua estrazione di informazioni dall'ambiente osservato e l'integrazione di tali informazioni con la conoscenza pregressa, al fine di formare un'immagine complessiva, che può essere usata anche per pilotare e/o anticipare eventi futuri [SAL08].
Dalla fine degli anni '80, diversi modelli di situation awareness sono stati proposti. Alcuni esempio sono: il modello a tre livelli di Endsley [END95]; il modello iterativo di Bedny e Meister basato sulla teoria delle attività [BED99]; il modello di Smith e Hancock [SMI95] basato su un approccio ecologico che si basa sul concetto di interazione.
Tutti questi modelli si basano sulla costruzione della situation awareness fatta da un individuo: il passo successivo (ampiamente riconosciuto dalla comunità scientifica, es. [HAY06]) è l'utilizzo della collettività per la costruzione della situazione awareness. Un tema interessante collegato è il cosiddetto "mutual monitoring", in cui i vari attori coinvolti nei processi di gestione dell'emergenza si controllano a vicenda [SAL08]. Stanton et al. [STA06] popone un modello collaborativo molto vicino al concetto del crowdsourcing, fortemente orientato al coordinamento degli attori coinvolti. In [SAP09] gli autori propongono un modello basato sulla cosiddetta "Team SA", in cui è forte il concetto di condivisione delle informazioni, delle esigenze di informazioni e dei processi coordinati.
In questo ambito, le informazioni pubblicate dalle singole persone sui social media o fornite attraverso meccanismi di crowdsensing possono essere raccolte e analizzate per fornire un quadro della situazione, tempestivo e storico di eventi, bisogni, sentimenti, ecc.
Gli individui, collaborando in modo asincrono e disaccoppiato, possono segnalare un evento (anche in continua evoluzione), coordinare gli aiuti, e produrre conoscenza profonda su uno specifico, time-sensitive topic (es. http://www.everyblock.com/; Matt Williams Governments use Twitter for emergency alerts, Traffic notices and more. Government Technology, January 2009; http://e2campus.com/; http://juntosdenunciamos.org.mx/; http://ireport.cnn.com/).
Early warning systems (EWS).
Nel contesto della gestione delle emergenze, l'"early warning" rappresenta una pronta ed efficace azione informativa, che permette di preparare una risposta anch'essa efficace [UN06].
Un Early Warning System (EWS) è in genere caratterizzato da un'infrastruttura ICT munita di sensori e reti di sensori in grado di predire disastri naturali, emergenze, situazioni di pericolo, e di allertare la popolazione, le autorità pubbliche e gli organini di soccorso preposti sui rischi imminenti in modo da consentirgli di evitarli o mitigarli e preparare una risposta efficace [GRA06].
Un efficace EWS comprende tutti gli aspetti della gestione delle emergenze: gestione del rischio (al fine di determinare le priorità di intervento); monitoraggio e predizione del luogo e dell'intensità dell'emergenza; sistema di comunicazione con le autorità ed in generale con tutte le persone potenzialmente coinvolte (coordinamento, piani di intervento, formazione, ecc.); risposta al disastro, all'emergenza, alla situazione di pericolo.
Un elemento importante degli EWS è la "tempestività", che ovviamente spesso contrasta con la precisione delle informazioni raccolte e gestite, la loro attendibilità e la determinazione di un quadro della situazione chiaro e completo [GRA07].
In molti casi gli EWS non hanno opportuni sistemi di comunicazione e piani di risposta adeguati. Si parla di local early warning applications oppure di regional or global early warning applications

quando l'informazione raggiunge rispettivamente singoli utenti o comunità e regioni.
Gli EWS esistenti rappresentano degli investimenti estremamente complessi e costosi ed inoltre si focalizzano tipicamente su specifici disastri ed emergenze di notevole entità (e.g. terremoti ed eruzioni vulcaniche [JMA] [NEIC], tsunami ed emergenze costiere [NOS] [MOR] [HEL08], incendi [EFFIS]) facendo uso di dati e vincoli georeferenziati.
Di conseguenza, gli EWS non sono stati ad oggi molto utilizzati in contesti in cui vi è un elevato numero di aree tematiche e applicazioni con un forte impatto negativo sul benessere del cittadino. Recentemente si è cercato di utilizzare gli EWS in contesti meno critici e meno stringenti, tutti caratterizzati da tempestiva predizione dell'emergenza, comunicazione urgente alle parti interessate, esecuzione di azioni per la mitigazione dell'impatto negativo. Tra questi si riporta qui la gestione delle frodi [EWCOM], la sicurezza [TEWS], l'identificazione di malware [WOMBAT] [MAN08] [APE10], contaminazione del cibo e/o dell'acqua [GIEWS], ecc.
Notevoli progressi sono stati fatti dagli EWS in numerosi campi applicativi grazie soprattutto ai progressi nella ricerca scientifica e nelle tecnologie ICT. Tuttavia, rimane ancora parecchio lavoro da fare per colmare il gap tecnologico, comunicativo e geografico esistente. In particolare, esiste ancora un forte divario tecnologico tra i paesi sviluppati e quelli in via di sviluppo. Per quel che concerne gli aspetti operativi, occorre invece rafforzare i collegamenti tra i settori coinvolti (si pensi alle organizzazioni responsabili di diramare i warning e alle autorità responsabili di rispondere a tali warning). Per rispondere a queste esigenze, i nuovi modelli di EWS, in grado di agire su scala mondiale, dovranno ottimizzare la gestione dei pericoli (multi-hazard EWS), estendere la copertura geografica e migliorare la componente tecnologica.
Informazioni geospaziali e crowdmapping
La recente disponibilità in Europa di dati geospaziali aperti ([PSI03], [INS07], [AAR]) e di Spatial Data Infrastructures (SDIs) fornisce nuove opportunità per un rapido utilizzo delle informazioni geospaziali. In aggiunta a ciò, si assiste a un nuovo fenomeno nei social network, il crowdmapping, che rende possibile la segnalazione di luoghi pericolosi o interessanti, fondendo le segnalazioni di singoli individui in un'unica mappa sempre consultabile e sempre più completa, in grado di fornire informazioni geocodificate (geotagged) a chiunque. Diverse applicazioni commerciali esistenti si basano su contenuti geocodificati dei social media per fornire value added services che sfruttano la posizione o la tematica catturata.
Attraverso l'aggregazione di contenuti crowd-generated (messaggi di testo, social media feeds) con dati georeferenziati forniti in tempo-reale è possibile avere informazioni interattive (mappe di crisi) su eventi critici come guerre (libyacrisismap.net), crisi umanitarie, crimini (http://southafricancrimemap.crowdmap.com/main) o disastri naturali, come recentemente dimostrato nei disastri di Haiti e in Giappone (http://www.telegraph.co.uk/technology/twitter/8379101/Japan-earthquake-how-Twitter-and-Facebook-helped.html; http://news.nationalgeographic.com/news/2006/10/061019-tsunami-maps.html). Chiunque è in grado di creare una crowdmap utilizzando lo strumento Crowdmap (http://crowdmap.com), sviluppato sopra la piattaforma open source Ushahidi (http://www.ushahidi.com/), iniziativa tecnologica kenyana realizzata nel 2008 in risposta agli scontri post-elettorali. Una caratteristica peculiare del Framework Ushahidi è quella di consentire diverse modalità per inserire i "Geo Reports": Web, SMS, eMail, Twitter, mobile apps gratuite per iPhones e Android.
Tra i vari progetti esistenti, Voice of America (http://www.voanews.com/english/news/), canale di comunicazione ufficiale del governo degli Stati Uniti d'America, ha prodotto una serie di contenuti crowdsmaps multimediali (video, immagini e report). Il progetto, Behind the Wall, ha finora prodotto tre mappe per Siria (https://behindthewallsyria.crowdmap.com), Bahrain (https://behindthewallbahrain.crowdmap.com) e Yemen.
Il progetto Wikinarco.com (https://www.wikinarco.com/) permette ai cittadini di geolocalizzare, online e in forma totalmente anonima, le attività illecite relazionate al narcotraffico registrate in tutto il territorio messicano, vari tipi di crimini, come ad esempio scontri armati, episodi di corruzione, rapine, arresti e per attribuirli poi a 8 cartelli della droga attivi sul territorio nazionale. Una funzione permette inoltre di visualizzare le zone interessate dal conflitto tra i principali cartelli.
Inoltre, i progetti AED4.us (http://www.aed4.us/) e Green Directory (http://witzenhausen.crowdmap.com) mirano, sfruttando il crowdmapping, a realizzare rispettivamente una mappa dei defibrillatori e dello sviluppo sostenibile nella propria regione.
Avanzamento dello stato dell'arte.
Nel progetto Secure! si affronterà la tematica del Situation Awareness ponendo l'attenzione sul processo di rappresentazione della conoscenza e di conseguenza della percezione della situazione all'interno di un sistema di ragionamento pratico che gestirà in maniera olistica la costruzione della situation awareness, la determinazione degli early warning e la relativa gestione dei piani di intervento e delle azioni necessarie.
Il ragionamento pratico è il ragionamento diretto alle azioni, cioè il processo che consiste nel ragionare su quale azione intraprendere (M. E. Bratman. Intention, Plans, and Practical Reasoning.

Harward University Press, 1987). Il ragionamento pratico è differente dal ragionamento teoretico, che è infatti è diretto alle credenze, alla conoscenza, alle deduzioni. Un esempio è il seguente: se credo che tutti gli uomini sono mortali e credo che Socrate sia un uomo, allora concluderò che Socrate è mortale. Il processo per arrivare ad una tale conclusione riguarda solo le mie credenze sul mondo, ed è per tale ragione che è chiamato teoretico; mentre il processo che consiste nel decidere, per esempio, se prendere l'autobus o andare in treno afferisce al ragionamento pratico perché riguarda l'azione da intraprendere. Il ragionamento pratico degli umani consiste di due diverse attività: decidere quale stato si vuole raggiungere - deliberation; decidere come raggiungerlo - means-ends reasoning.
In un contesto di complessità informativa (e non solo), pensare di adottare solo meccanismi di ragionamento teorico e di integrazione delle informazioni per la determinazione del "quadro della situazione" porterebbe all'adozione di un approccio passivo, non in grado di supportare e gestire le continue esigenze che emergono (per esempio dovute al succitato "effetto domino", dall'emergenza di nuove opportunità di sorgenti informative, dalla consapevolezza che lo stato della situazione "ricostruito" sarà una prospettiva (sicuramente parziale ed incompleta) della situazione "reale", dalla necessità di gestire ed integrare informazioni a volte contrastanti tra di loro ed infine dalla necessità di dover perseguire degli obiettivi (di conoscenza, ma anche di performance), a volte anche di dover scegliere tra più opzioni o di determinare un trade-off opportunistico. Tutto questo necessità di meccanismi di ragionamento più sofisticati e la gestione integrata ed olistica delle varie componenti coinvolte.
In particolare, la determinazione e la consapevolezza della situazione sono da intendere come il risultato della fusione di due approcci: uno bottom-up (reattivo), con le informazioni provenienti in maniera spontanea dall'ambiente osservato; l'altro top-down, fatto da un insieme "intenzionale" e "pianificato" di azioni informative (atte a raccogliere, estrarre, correlare, integrare, approfondire, ecc. dati ed informazioni). Entrambe le modalità saranno basate sulle componenti innovative e sulle tecniche discusse nei precedenti punti 2 e 3 dello "Stato dell'arte". L'integrazione di queste due modalità, permetterà l'estrazione di informazioni dall'ambiente osservato e l'integrazione di tali informazioni con la conoscenza pregressa (che include anche l'esperienza passata), al fine di formare un'immagine complessiva della situazione, che può essere usata anche per pilotare e/o anticipare eventi futuri.
Con riferimento agli aspetti di early warning e gestione operativa della crisi, rispetto ai tradizionali modelli "stages-view" [KEL98], con fasi sequenziali (prima-durante-dopo) caratterizzate da azioni ed eventi classificabili e indipendenti, nel progetto verrà sperimentato un nuovo modello iterativo (basato sul ragionamento pratico) di gestione delle situazioni di emergenza basato prevalentemente sulla generazione in continuo di "eventi" in tempo reale e sulla conseguente rappresentazione della "situazione" attuale in modo tale da poter gestire le evoluzioni e i cambiamenti del contesto di riferimento e suggerire l'azione ritenuta più idonea e in linea con gli obiettivi generali del sistema.
A tal proposito, il progetto Secure! mira ad includere e supportare tutti gli elementi di un generico EWS: gestione del rischio; monitoraggio e predizione del luogo e dell'intensità dell'emergenza; sistema di comunicazione; risposta. Si valuterà l'utilizzo di canali di comunicazione non tradizionali (social media) e di "sensori umani" per realizzare un EWS altamente economico, efficace, scalabile e indipendente dal dominio. Infine, per la diffusione delle informazioni ad un elevato numero di persone in un formato user-friendly (e.g. mappe interattive e digitali, email, SMS), si utilizzeranno i risultati ottenuto nell'ambito delle applicazioni di crowd-sourcing e crowd-mapping (OO 3 e 4). Sarà altresì investigato nell'ambito del progetto l'utilizzo di modelli e tecniche per la gestione della sicurezza e della privacy (OO 2) applicate in un contesto globale che coinvolge diversi soggetti pubblici e privati e in cui vengono scambiati numerosi dati e informazioni sensibili. Infine, verrà inoltre proposto l'utilizzo di protocolli standard relativamente alla gestione delle emergenze, allo scambio di informazioni e alla diffusione dei warning (es. Common Alerting Protocol)
Le componenti innovative ed un sistema di supporto decisionale basati sul ragionamento pratico si baserà sulla piattaforma PRACTIONIST (PRACTIcal reasONIng sySTem), realizzata da ENGINEERING in precedenti iniziative di ricerca. L"intera suite PRACTIONIST è rilasciata secondo i termini definiti dalla licenza LGPL (Lesser General Public License v2.1) e comprende:
? la metodologia PRACTIONIST, che consiste in un processo di sviluppo iterativo e incrementale che utilizza il linguaggio PAML (PRACTIONIST Agent Modelling Language), il quale è basato su UML ed è specifico per PRACTIONIST;
? il PRACTIONIST runtime and framework (PRF), che definisce e supporta la logica di esecuzione degli agenti e fornisce le componenti built-in che implementano il modello di ragionamento pratico. Tali componenti sono realizzate in JAVA e Prolog. Il PRF include anche il PAM (PRACTIONIST Autonomic Manager), per il controllo autonomico dei sistemi realizzati e delle loro caratteristiche Self-CHOP (Self-Configuring, Self-Healing, Self-Optimizing, Self-Protecting);
? il PRACTIONIST Studio, un tool di progettazione e sviluppo a supporto della metodologia, implementato sulla piattaforma ECLIPSE, usando alcuni suoi plugin, come UML2, EMF e GMF.
Il sistema, grazie al modello computazionale ed alle caratteristiche di goal-orientation di PRACTIONIST, sarà dotato della capacità di adattamento dei piani di risposta ai fattori di contingenza

che possono emergere durante l'emergenza, supportando così le capacità di riconfigurazione e di rideterminazione degli obiettivi e delle azioni
Inoltre, nel contesto del progetto Secure!, le informazioni geospaziali contribuiranno alla determinazione del "quadro della situazione" nelle seguenti due maniere:
? analizzando molteplici sorgenti di informazioni geospaziali (anche istituzionali) che possono essere integrate con le altre informazioni gestite;
? i contenuti spaziali generati attraverso i social media (es. check-in su Foursquare o Facebook, inserimento di una foto geo-taggata su Flickr) possono arricchire lo spettro delle informazioni che determinano e caratterizzano la "situazione.
Nel progetto sarà investigata la disponibilità di differente sorgenti di dati geospaziali, con particolare riferimento alle Spatial Data Infrastructures, alle social network, ai portali di dati aperti. Sarà inoltre realizzato un nuovo strumento che consentirà agli operatori coinvolti nel processo di gestione della crisi di sfruttare le potenzialità del crowdsorcing e delle informazioni georeferenziate prodotte (crowd-mapping) per incentivare la partecipazione sociale in modo solidale ma controllato.
Infine, un altro elemento di innovazione introdotto dal progetto è la definizione e lo sviluppo di un set di servizi di analisi off-line (si veda sotto i servizi di Secure! Analtytics). Questo soluzione risponde ad alcune importanti esigenze:
? la capacità di analizzare "a bocce ferme" le situazioni passate ed il funzionamento del sistema in risposta ad esse, al fine di determinare miglioramenti nei processi (che potranno essere opportunamente riconfigurati, come appena descritto) e nei singoli servizi (effettuando operazioni di fine-tuning e configurazione, supportate dall'architettura orientata ai servizi di Secure!);
? la possibilità di studiare (e se necessario, influenzare e contrastare) alcuni fenomeni che si verificano tipicamente nelle situazioni di emergenza, come l'orientamento degli atteggiamenti, delle decisioni e dei comportamenti, oppure l'emergenza di modelli di "leadership" (che possono essere anche sfruttati per influenzare i comportamenti e gestire la crisi in maniera più efficiente e/o efficace);
? la possibilità di "simulare" alcuni possibili eventi e situazioni di pericolo o emergenza al fine di prevederne l'andamento, seppur per un set limitato di variabili.
Tutti questi aspetti saranno affrontati, studiati ed integrati nei sevizi di analytics che il progetto Secure! mira a definire e sviluppare.

5. Sicurezza, affidabilità, fiducia e privacy
La piattaforma Secure! consiste di molte componenti (anche di natura eterogene), che variano dai servizi web e cloud, passando dai sensori per acquisire informazione, per giungere ai dispositivi mobili ed applicazioni per utente. Le problematiche di affidabilità e di sicurezza che si devono considerare sono molte, ed anche specifiche, basta considerare che in presenza di emergenze si possono manifestare aspetti di criticità, p.es. le comunicazioni possono non essere affidabili (mancanza/ discontinuità delle connessioni). Queste problematiche richiedono varie approcci (e alcuni sono già direttamente utilizzabili) per ognuno di questi settori, p.es. meccanismi come WS-Security [NIST800-95], cloud security [MKL09] e protezione delle applicazioni per devices mobili [LMS12]. Tra le varie attività che richiedono una particolare attenzione vi è certamente la gestione della identità e della autenticazione anche mediante strumenti di autenticazione forte anche basata su metodi biometrici.
Avanzamenti rispetto allo stato dell'arte.
Si intende migliorare le tecnologie per la protezione dei servizi, dei dispositivi mobili e dei dati, con particolare attenzione agli aspetti di privacy. La piattaforma Secure! adotterà meccanismi per garantire la sicurezza e l'affidabilità del servizio, anche in contesti ad elevata criticità (anche in presenza di disfunzione). Di particolare interesse sarà la protezione di dispositivi mobili che interagiscono con gli utenti cosi come rendere affidabili le comunicazioni.
Distribuzione dell'informazione, controllo accessi ai servizi della piattaforma.
La piattaforma acquisisce, gestisce e distribuisce informazione. Si deve quindi prevedere che l'uso di questa informazione sia autorizzato per gli scopi previsti e nei modi previsti. Per quello che riguarda il controllo accessi in generale esistono molti approcci, e recentemente si è diffuso il concetto di "usage control" [PS04], che considera non solo se l'accesso è autorizzato in un dato momento ma anche nella continuità della azione in esame. Tale modello permette di definire politiche di controllo accessi (o meglio uso) continue sugli risorse, permettendo al contempo di esprimere politiche di privacy sui propri dati e politiche di controllo di uso sugli oggetti ed i servizi offerti. Il modello è stato esteso ed implementato per sistemi distribuiti e mobili in vari lavori, es. [MMV05],[CMMR08], e [HMMV06], ed le potenzialità offerte da tali approcci sembrano molto promettenti. Avere linguaggi che permettono un livello di dettaglio molto fine per specificare il controllo degli accessi è molto importante. In questo ambito consideriamo linguaggi per specificare politiche di controllo accessi avanzati come XACML che possono essere estesi anche per usage-control.
Avanzamenti rispetto allo stato dell'arte.
La piattaforma dovrà garantire gli accessi ai servizi in maniera appropriata, in base al livello di sicurezza dettati dal contesto ed il rischio della emergenza in esame. La condivisione di dati personali

e la loro correlazione può suggerire di utilizzare politiche di sicurezza per i dati che siano direttamente associate ai dati stessi (sticky policies). Il loro uso su telefoni cellulari pone delle sfide significative. Si intende, lato server ottenere un sistema completo di "usage control" per l'infrastruttura del progetto. I linguaggi di controllo accessi e delega di diritti, che permettono anche di poter esprimere opinioni su altri utenti, sono per il momento usati solo su sistemi desktop, e loro applicazioni sui cellulari sarebbero molto significative. Si intende anche incrementare l'uso di meccanismi per protocolli di comunicazione anonima ove richiesto dalle politiche di privacy del utente. È anche importante avere meccanismi per mediare i conflitti che nascono dalla gestione condivisa dei dati.

Gestione della fiducia e meccanismi di credibilità delle fonti di informazione.

La gestione della fiducia in sistemi digitali, in particolare social networks /crowds in cui utenti hanno la necessità di considerare come altri utenti si comporteranno in certe situazioni, è cruciale in un progetto come Secure! Esistono numerosi modelli per descrivere la formazione, la modifica, e l'evoluzione dei rapporti di fiducia tra le varie entità di interesse, sia basati su osservazione diretta che indiretta tramite raccomandazioni [ZXLJC12]. Questi modelli devono essere adattati ai vari contesti dove la piattaforma Secure! può essere applicata.

Vista la varietà dei media è importante sia considerare la confidenza nella precisione sul fornire informazioni dirette che in quelle indirette, problematiche di collaborative information filtering sono essenziali, p.es. [SK09].

È inoltre importante notare come la gestione dei dati, possibilmente da fonti informative distribuite, possibilmente sotto un controllo amministrativo decentralizzato (non tutte le componenti della piattaforma Secure! necessariamente sono sotto lo stesso controllo amministrativo, oppure con gli stessi privilegi di uso) necessità di di linguaggi e meccanismi per descrivere le relazioni di fiducia e di delega di diritti di uso su risorse. Questi linguaggi hanno subito un nuovo sviluppo, in particolar modo dal tentativo di unire linguaggi per la delega dei diritti e degli attributi degli utenti [JNW05] con linguaggi per esprimere informazioni circa la reputazione degli utenti nel sistema [IBJR04] dando vita a linguaggi integrati più espressivi [MP07].

Avanzamenti rispetto allo stato dell'arte.

Saranno di interesse anche aspetti di politiche di sicurezza in social networks, di cui il concetto sopra esposto di gestione della fiducia è uno degli aspetti rilevanti. Le sfide da considerare sono molte, partendo dalla credibilità; dei dati raccolti, dalla robustezza del sistema di raccomandazione e conseguentemente di gestione della fiducia. La necessità di creare on-line valori di fiducia non necessariamente da dati noti richiede un alto grado di interoperabilità e la capacità di fondere e rendere interoperabili modelli di gestione della fiducia diverse, ad esempi usati in due social networks o crowds diversi.

Gestione della privacy.

La piattaforma Secure! ha tra i suoi scopi la raccolta, la gestione e la diffusione dei dati, per cui le problematiche di gestione della privacy sono significative (inoltre nell'ambito di Secure! le informazioni sensibili possono essere acquisite in maniera non volontaria e consapevole - si pensi all'acquisizione di informazioni su persone effettuata tramite sensori e telecamere, oppure tramite segnalazioni). Negli anni si stanno diffondendo varie privacy-enhancing-technologies [SBK03] che permettono un approccio privacy-by-design in cui gli aspetti di privacy devono essere gestiti in maniera nativa della piattaforma.

Le problematiche principali sono anche basate sulla necessita di mediare tra il livello di precisione dei dati acquisiti, con lo scopo (ed il corrispondente impatto) per cui sono gestiti dalla piattaforma. Modelli di gestione del rischio per usage-control di informazione esistono e possono essere adattati ai nostri scopi. Alcuni lavori su aspetti di privacy nell'information sharing per social networks sono già disponibili, p.es. [XCF11].

Avanzamenti rispetto allo stato dell'arte.

Per la gestione di aspetti di privacy, per i dati acquisiti dobbiamo poter usare politiche fini di controllo accessi ai dati che permettono di usarli solo in certi contesti e non in altri (context aware data centric policies). Al contempo i meccanismi per integrare le informazioni devono poter avere strumenti per incrementare il livello di anonimato e non-tracciabilità dei dati stessi. Si dovranno identificare soluzioni per la protezione delle informazioni personali da parte di utenti malintenzionati, includendo tra questi non soltanto malintenzionati quali hacker o sabotatori, ma anche personale addetto interessato a sapere dettagli su alcuni eventi, situazioni o persone. Inoltre alcune metodologie si occupano ad esempio di effettuare in maniera confidenziale il calcolo di alcune funzioni in maniera distribuita di modo che solo il risultato sia noto a tutti i partecipanti, ma non i dati iniziali. Tali metodologie note come secure-multy-party computation [CDM00] stanno raggiungendo una notevole maturità e scopo del progetto è verificare la loro realizzabilità anche per telefoni cellulari. Recentemente questi algoritmi sono proposti per scambiare l'importazione in retei peer-to-peer in maniera confidenziale ed intendiamo continuare questo studio per i crowd del progetto Secure!.

Obiettivo generale

In un contesto di diffusione dei social media, l'obiettivo generale del progetto Secure! è studiare l'applicabilità e le modalità di applicazione di meccanismi, modelli, tecniche, tecnologie e strumenti di crowdsourcing per la prevenzione (quando possibile), l'anticipazione e la gestione di eventi e situazioni di emergenza relativi alla sicurezza pubblica e alla protezione civile: questo può includere eventi fortuiti e accidentali, infortuni e disastri naturali, climatici, o di qualunque altro genere; oppure identificare comportamenti illeciti e prevenirne l'aggravio del danno attraverso l'organizzazione di forme di prevenzione e di intervento.
In pratica si vogliono definire e realizzare strumenti e servizi che complimentino e integrino gli attuali sistemi di gestione delle suddette situazioni, sfruttando le potenzialità offerte dall'enorme mole di informazioni presenti sui social media e la disponibilità di "sensori umani" coinvolgibili in processi di crowdsensing, sia nella modalità partecipatoria (gli utenti sono consapevoli e attivi nel fornire le informazioni) che nella modalità opportunistica (le informazioni sono raccolte in maniera quasi autonoma dai dispositivi personali e il coinvolgimento degli utenti è ridotto).
In termini più concreti, si vuole:
(i) definire e realizzare un'infrastruttura abilitante orientata ai servizi (il Secure! Framework) per la costruzione di servizi di gestione della sicurezza pubblica e delle infrastrutture e di protezione civile basati sui meccanismi del crowdsensing e del crowdsourcing;
(ii) applicare la suddetta infrastruttura a due scenari dimostrativi (la protezione del patrimonio artistico-culturale, la protezione di infrastrutture critiche).
Al fine di realizzare il suddetto Secure! Framework, saranno studiati, definiti e sviluppati nuovi modelli, metodi e tecnologie da integrare in un'architettura orientata ai servizi in grado di raccogliere, analizzare, prevedere, investigare in maniera integrata, coerente e consistente sorgenti di dati aperte (OSINT – Open Source INTelligence) multi-modali (testi, immagini, video, audio, ...) presenti sui social media, integrate con dati acquisiti tramite tradizionali infrastrutture e sistemi esistenti, al fine di ottenere una conoscenza situazionale aggiornata (in tempo-reale) e migliorare la gestione delle piccole e grandi emergenze e della sicurezza pubblica e del territorio, attraverso un attivo coinvolgimento dei cittadini sia nella fornitura di informazioni sia nelle operazioni durante le emergenze.
In Figura 1 (riportata nel file allegato "Figura 1 - L'architettura del sistema.gif") è mostrata l'architettura logica di sistemi di gestione delle emergenze secondo la logica proposta dal progetto e la centralità del Secure! Framework rispetto allo sviluppo di tali sistemi.
Come si può osservare dalla suddetta figura, il sistema sarà in grado di ricevere dati e informazioni multimodali da
- social media (attraverso un opportuno insieme di componenti e servizi di integrazione, Social Media Data Collection Services);
- reti di sensori, in accordo a standard consolidati, quali ad esempio Sensor Web Enablement (SWE), definito dall'Open Geospatial Consortium (OGC);
- sistemi informativi esistenti che forniscono dati e informazioni rilevanti, da identificare e integrare in funzione delle specifiche applicazioni del sistema, mediante opportuni adattatori (Integration of external information systems and services);
- applicazioni installate su dispositivi mobili personali (Secure! Crowdsourcing Apps), opportunamente realizzate per supportare i sensori umani sul campo.
A partire da tali sorgenti di dati multimodali e dai "dati rilevanti" da essi raccolti, saranno studiate, analizzate, definite e integrate tecniche innovative per l'estrazione e il filtraggio di caratteristiche e "informazioni utili" e di data mining (Information Extraction and Integration). A tal fine il progetto userà e coniugherà tecniche, tecnologie e modelli innovativi di image recognition e text mining, unitamente a modelli e tecniche di information fusion e di machine learning. Il progetto inoltre definirà anche nuovi modelli e tecniche innovative per analizzare le dinamiche sociali all'interno di gruppi e comunità, allo scopo di prevedere la genesi e il flusso di informazioni che potrebbero essere di rilevante importanza per la sicurezza, così come per studiare e applicare criteri di trust delle informazioni ricevute e degli utenti che le forniscono. L'integrazione e la correlazione delle informazioni utili estratte produrranno l'immagine informativa di uno o più eventi da monitorare, controllare, evitare, ecc.
Le informazioni utili estratte e gli eventi dedotti o determinati, congiuntamente a uno studio di aggregazione e correlazione degli stessi, consentirà di fare emergere "situazioni" di potenziale pericolo o di emergenza, che vanno dal riconoscimento, la validazione e localizzazione di segnali ed eventi, alla scoperta di dinamiche comunicative che possano far pensare alla necessità di un monitoraggio o un avvertimento a fini preventivi, la valutazione del livello di rischio, ecc. (Real-time analysis for situation awareness). Tali analisi saranno condizionate e vincolate dall'esigenza di rispondere in tempo reale o in tempo quasi reale, che inevitabilmente inciderà sulle tecniche di analisi adottabili e sulla quantità di informazioni analizzabili (questo vincolo è assente nei servizi di analisi off-line, descritti sotto).
Il progetto intende inoltre dotare il sistema della capacità di gestire, sia su richiesta dell'utente (reattivo) sia autonomamente (proattivo), processi decisionali che possano rispondere in modo

adeguato alle varie situazioni di pericolo riconosciute (intese come configurazioni di eventi significativi forniti dalla correlazione di informazioni). Questo include meccanismi di ragionamento automatico che permetteranno al sistema di reagire e/o agire autonomamente, strumenti per l'assegnazione di micro-task a utenti sul campo, l'invio di avvertimenti e/o notifiche (Action Management and Decision-making).
Il framework fornirà strumenti per l'arricchimento delle informazioni estratte dalle varie sorgenti, e successivamente elaborate e analizzate, con informazioni geospaziali (Geo-spatial information and Crowd-mapping). Questi strumenti partendo dalle segnalazioni di luoghi pericolosi o interessanti, fondono le segnalazioni di singoli individui in un'unica mappa sempre consultabile e sempre più completa, in grado di fornire informazioni geolocalizzate a chiunque.
Al fine di valutare le performance del sistema e di avere dei miglioramenti (in termini sia di efficacia sia di efficienza) nei successivi utilizzi, il framework metterà a disposizione un set di strumenti e servizi per l'analisi post-emergenza. Al contrario dell'analisi in tempo reale, sono rilasciati i vincoli temporali sulle tecniche di analisi, correlazione e data mining e, di conseguenza, sulla mole di informazioni oggetto di osservazione. Infatti, mentre nel caso real-time, sono considerate prevalentemente le informazioni recenti che si riferiscono allo stesso evento/fenomeno, nel caso di questi servizi di analisi off-line sono considerate anche le informazioni storiche, cercando correlazioni e pattern non identificabili in presenza di vincoli di tempo e della necessità di rispondere tempestivamente. In questo senso, a titolo di esempio, potranno essere analizzati i flussi informativi da e verso i social media, scoperti pattern (anche comportamentali) ricorrenti, fare considerazioni geo-spaziali, fare analisi what-if, misurare le performance dei processi di gestione, ottenere indicazioni per migliorare (fine-tuning) gli algoritmi e i servizi di analisi in tempo reale, ecc.
Infine nell'ambito del progetto saranno definite e sviluppate alcune applicazioni che sfruttano i servizi offerti dal framework e implementano le funzionalità richieste per la gestione di situazioni di emergenza:
- Applicazioni mobile utilizzate "sul campo" per la generazioni di informazioni (Secure! Crowdsorcing Apps): queste applicazioni saranno in grado sia di raccogliere informazione fornite esplicitamente da parte degli utenti, sia di inviare notifiche agli utenti (ad esempio, per segnalare come comportarsi in situazioni di pericolo).
- Applicazioni desktop/mobile per la gestione operativa delle crisi/emergenze, utilizzate dal personale addetto sul campo (Secure! Situation-awareness Apps).
- Secure! Analytics Services: applicazioni per l'analisi offline di grandi moli di dati e volte a identificare le informazioni rilevanti e utili al miglioramento del sistema.
I seguenti sono solo alcuni esempi di servizi applicativi che il progetto mira ad abilitare e (in alcuni casi) a sviluppare in versione prototipale:
- Early warning detection
- Comunicazione di situazioni di emergenza alla popolazione ed eventuali azioni (generali per l'intera popolazione o specifiche per utente)
- Identificazione di necessità di interventi a scopo preventivo
- Collezione e gestione di richieste di assistenza
- Situation awareness
- Stima di danni in strutture e infrastrutture pubbliche, inclusi monumenti e edifici storici
- Coinvolgimento volontario e solidarietà
La Figura 2 (riportata nel file allegato "Figura 2 - I flussi di dati e informazioni.gif") presenta una prospettiva orientata alle informazioni dei concetti che il progetto vuole adottare. In particolare, come già detto i "Relevant Data" sono quelli raccolti da tutte le sorgenti considerate attraverso processi e componenti di selezione, monitoraggio, osservazione, filtraggio, valutazione, ecc. Esempio di "Relevant Data" sono i tweet, un'immagine, i post di un blog o di un forum, i dati provenienti dalle reti di sensori, o i dati provenienti da sistemi esterni esistenti.
I "Relevant Data" saranno analizzati per estrarre "Useful Info". Ad esempio da un tweet sono estratti alcuni segnali di pericolo o segnalazioni di incidente o stati d'animo delle persone; da un'immagine possono essere stratte informazioni utili quali il numero minimo di persone coinvolte in un incidente. L'aggregazione e la correlazione di "Useful Info" produce un'istanza di un concetto centrale per il progetto, ossia l'"evento", che rappresenta un accadimento, qualcosa che è successo (es. un incidente stradale caratterizzato da tutte le informazioni utili estratte da tutte le sorgenti disponibili). Un evento è tipicamente legato a un intervallo di tempo ridotto, idealmente istantaneo.
L'elaborazione delle informazioni relative agli eventi, la correlazione con altri eventi, l'aggregazione di più eventi permette di ricostruire il quadro della "situazione", che arricchisce l'evento centrale di altre informazioni di contesto (es. altre persone presenti sulla scena, valutazione dei danni, presenza di feriti, ecc.). Sarà proprio la situazione a essere valutata e gestita, attraverso la determinazione di azioni da intraprendere e decisioni da prendere.
Tutti i suddetti livelli informativi saranno raccolti ed elaborati producendo le "analytics" descritte sopra.
Si può anche notare che i social media, le crowdsourcing apps e le situation-awareness apps saranno

usate anche come strumenti attuativi, per la gestione operativa delle emergenze e degli interventi.
Il progetto intende anche realizzare un insieme di Application Programming Interface (API) da utilizzare per lo sviluppo di applicazioni, servizi e sistemi specifici di gestione di situazioni di emergenza nel contesto della sicurezza pubblica e della protezione civile. Le Secure! APIs consentiranno anche l'integrazione di altre sorgenti di informazione e di altre tecniche di analisi come servizi.
Si vuole precisare che il Secure! Framework sarà agnostico rispetto al tipo di emergenza e sarà progettato per essere flessibile in modo da adattarsi alle varie esigenze degli analisti e/o gestori di tali fenomeni.
Un'ulteriore parte importante del Secure! Framework riguarda la gestione della sicurezza delle informazioni scambiate, della privacy degli utenti, del livello di trust degli utenti e dell'affidabilità del sistema: in un contesto di applicazioni del crowdsourcing, tali tematiche rivestono un ruolo molto importante. In particolare saranno affrontate e studiate problematiche come:
- Identificare e valutare il set minimo di dispositivi che possono produrre "reliable" data;
- Stessi sensori sono condivisi tra diverse applicazioni di mobile crowdsourcing: ci sono problemi di allocazione delle risorse del dispositivo mobile, che devono essere affrontati in maniera unificata e integrata per tutte le applicazioni;
- Trade-off tra local analytics (analisi sul dispositivo mobile dei dati raccolti) e aggregate analytics (analisi dei dati sul lato server/servizio);
- Alcune applicazioni sono intrinsecamente "delay sensitive" e quindi la tempestività nella generazione dei dati dal dispositivo mobile e nelle successive analisi è un requisito fondamentale;
- Si possono avere dati differenti dagli stessi sensori e stessi dati da diversi sensori;
- Privacy: ogni utente ha diverse percezioni di privacy; crittografia, tecniche di perturbazione, ecc.
- Meccanismi di incentivazione degli utenti
Il risultato di tali studi e analisi sarà un middleware di gestione di privacy, trust e sicurezza delle informazioni scambiate (Security, Privacy, and Trust Management) e un insieme di soluzione architetturali da adottare per la realizzazione di applicazioni di crowdsourcing, tenendo in considerazione le suddette problematiche.
Lo sviluppo del sistema sarà guidato da un'architettura di riferimento che fornirà le specifiche che definiscono le componenti funzionali del sistema, le relazioni tra dette componenti e i vincoli che le componenti dovranno soddisfare. Le tecnologie che si svilupperanno si baseranno sullo stato dell'arte, con particolare attenzione per gli ambienti open source, con l'obiettivo di avanzare il suddetto stato dell'arte con riferimento ad alcuni aspetti specifici.
L'obiettivo generale descritto sopra sarà raggiunto attraverso il perseguimento di cinque obiettivi operativi in cui il progetto è suddiviso (si veda la Figura 3 nel file allegato "Figura 3 - Dipendenze fra gli obiettivi operativi.gif", che riporta graficamente tali obiettivi e le interdipendenze tra di loro):
- Obiettivo Operativo 1: La definizione dell'architettura complessiva del sistema Secure! e l'integrazione delle sue componenti e servizi. Questo obiettivo include anche la definizione e sviluppo di alcune applicazioni e servizi per la gestione delle emergenze basate sul crowdsourcing. Questo obiettivo funge da guida e da contenitore per le attività e i risultati dei successivi obiettivi operativi 2, 3 e 4, fornendo requisiti, l'architettura di riferimento, l'infrastruttura di integrazione e integrando le componenti innovative risultanti dai suddetti obiettivi operativi nel Secure! Framework e in un set di servizi e applicazioni in esso contenute.
- Obiettivo Operativo 2. Lo studio delle problematiche di sicurezza, trust. privacy, affidabilità nel contesto delle applicazioni e dei processi di crowdsorcing: il risultato sarà un middleware che implementa le risultanze di questo studio, in termini di strumenti e meccanismi, e un insieme di pattern architetturali da adottare nella definizione dell'architettura e nello sviluppo delle suddette applicazioni.
- Obiettivo Operativo 3. Lo studio e l'analisi di tecniche di raccolta di "dati rilevanti" dalle varie sorgenti considerate nel progetto (e discusse sopra), di tecniche di estrazione di "informazioni utili" e di correlazione delle stesse finalizzata alla ricostruzione e determinazione di "eventi" da considerare. Tale studio produrrà alcune componenti innovative che implementano le suddette tecniche.
- Obiettivo Operativo 4. Lo studio e l'analisi di tecniche di aggregazione e correlazione di informazione al fine di determinare il quadro generale delle "situazioni" da gestire. Lo studio di meccanismi di ragionamento e pianificazione automatici per la gestione e il coordinamento degli interventi sul campo.
- Obiettivo Operativo 5: L'applicazione del Secure! Framework in due casi piloti, opportunamente definiti per la dimostrazione e la validazione del'approccio, delle tecnologie e del sistema proposti nel progetto. I due casi scelti riguardano (1) la protezione del territorio e del patrimonio artistico-culturale e (2) la protezione di infrastrutture critiche.
Gli obiettivi operativi suddetti saranno perseguiti attraverso alcune attività, che produrranno risultati intermedi (deliverable). Il diagramma di Gantt delle attività del progetto, allegato al presente documento, mostra anche tali risultati intermedi (indicati con Dx.y, dove "x" rappresenta il numero dell'obiettivo operativo e "y" indica un progressivo numerico nell'ambito dell'obiettivo operativo stesso) e i punti di controllo, le milestone (indicate con Mx.y, dove "x" rappresenta il numero

dell'obiettivo operativo e "y" indica un progressivo numerico nell'ambito dell'obiettivo operativo stesso). Si noti che, mentre ogni deliverable è sempre il risultato di una sola attività (che potrebbe produrne anche più di uno), ogni milestone potrà coinvolgere anche più attività. Inoltre alcune attività produrranno dei risultati parziali e non definitivi (indicati nel Gantt con "ID"), utili anche per il coordinamento interno del progetto e i collegamenti tra le attività e gli obiettivi operativi.
Il ciclo di vita del progetto prevede 4 fasi principali (di sei mesi ciascuna). La prima fase (dal mese 1 al mese 6) raccogli principalmente attività di analisi: dei requisiti, dello stato dell'arte e delle tecniche di estrazione e integrazione delle informazioni dalle varie sorgenti considerate. La seconda fase (dal mese 7 al mese 12) prevede la costruzione di una priva versione "usabile" del Secure! Framework, che includerà le varie componenti innovative definite e realizzate negli obiettivi 2, 3 e 4; anche l'architettura del sistema sarà completata al termine di questa fase. La terza fase (dal mese 13 al mese 18) mira a costruire e validare il primo dimostratore, ossia l'applicazione e la specializzazione del Secure! Fremework ai due piloti previsti nel progetto. L'ultima fase (dal mese 19 al mese 24) mira alla finalizzazione dei risultati ed alla validazione nel dimostratore finale.
Il sistema risultante sarà sperimentato e validato nel contesto di 2 piloti dimostrativi:

1. Protezione del territorio e del patrimonio artistico-culturale.
Nell'ambito dello scenario proposto, il sistema Secure! viene impiegato per la salvaguardia e la tutela del territorio, per mezzo di azioni di monitoraggio in tempo reale di vaste aree, analisi di dati e informazioni multimodali provenienti da sorgenti eterogenee e distribuite. Queste informazioni che saranno estratte da diverse fonti e diverse apps saranno analizzate, mappate e elaborate allo scopo di ottenere una corretta valutazione in tempo reale di ciò che sta accadendo.
Lo scenario prevede anche la gestione dell'intervento e dell'emergenza (prima, durante e dopo) in caso di situazioni critiche, mediante un utilizzo sinergico di modelli e strumenti innovativi del Web 2.0 (e.g. social media, crowdsensing, sensor web, mobile apps, etc.).
Potrebbe essere un dato non strutturato come tanti, ma quel tweet di @ibleonet (si vada la Figura 4 riportata nel file allegato "Figura 4 - Un tweet "rilevante".gif"), catturato dal componente Social Media Data Collection Services, desta qualche preoccupazione di sicurezza pubblica (il termine "occuperemo" lascia intendere che ci possano essere degli scontri) e di tutela del patrimonio culturale (l'occupazione riguarda un monumento del IX secolo, principale attrazione turistica del patrimonio culturale). Altri tweet inviano altri messaggi simili ("spaccheremo tutto!"). Alcuni utenti dotati di specifiche apps forniscono informazioni sulla reale emergenza e gravità della situazione.
Per avere un quadro completo di quanto potrebbe accadere servono altri dati rilevanti: mentre alcuni servizi del Social Media Data Collection continuano la ricerca nei vari Social Media, altri servizi visionano (web crawling) i contenuti dei siti Web delle principali agenzie di stampa italiane (Adn Kronos, Agenzia Giornalistica Italia, ANSA, ASCA) non trovando nessun riferimento ufficiale alla manifestazione di domani. Altri dati rilevanti provengono dalle telecamere poste ai caselli autostradali dell'autostrada che rilevano un elevato transito di mezzi articolati pesanti (TIR) e da una serie di video girati nelle aree di sosta dell'autostrada che riprendono gruppi di persone con bandiere del movimento e poi caricati su Youtube.
1. Il componente Geo-spatial Information and Crowd-mapping consente, inoltre, di georeferenziare gli stessi dati rilevanti mappandoli con informazioni geospaziali in un'unica mappa disponibile a chiunque.
2. L'estrazione, l'aggregazione, la correlazione e l'integrazione dei dati rilevanti, ad opera del componente Information Extraction and Integration, ha l'obiettivo di produrre informazioni utili (le persone alle aree di sosta fanno parte del movimento) ed eventi (presenza in autostrada di numerosi TIR e di gruppi di persone facenti parte del movimento che si dirigono verso la città) per il sistema Secure! che possano aiutare a comprendere la situazione su cui, eventualmente, agire.
3. L'elaborazione e l'analisi delle informazioni e degli eventi rilevanti finalizzata alla consapevolezza della situazione attuale (situational awareness) è il compito principale del Real-time Analysis for Situational Awareness. A questo punto la situazione è un po' più chiara: il movimento sta organizzando una manifestazione popolare che coinvolge un elevato numero di persone e di mezzi e che avrà un forte impatto sul piano della sicurezza pubblica, della viabilità cittadina e della tutela dei beni culturali, anche perché, l'organizzazione non ha seguito i canali ufficiali.
4. Rimane ancora qualche elemento da chiarire: quante persone parteciperanno alla manifestazione e come si sposteranno? Sfruttando gli stessi canali utilizzati dal movimento per comunicare la loro intenzione, mediante le Secure! Crowdsourcing Apps o attraverso altri social media (es. Twitter, Facebook) il sistema Secure! invia un open call in cui chiede alla gente (crowd) se intendono partecipare alla manifestazione di domani e con quali mezzi.
5. L'elaborazione di questi ulteriori dati rilevanti consente al sistema Secure! di avere la situazione maggiormente sotto controllo e di prendere delle decisioni, possibilmente, nel minor tempo possibile. Il sistema, una volta valutato il rischio, elaborerà un piano di intervento (action management e decision making) individuando le attività necessarie e notificando l'evento mandando degli alert ai vari organismi di competenza.

6. Attraverso l'utilizzo delle Secure! Situation-Awareness Apps sono allertati tempestivamente gli organi preposti alla sicurezza pubblica, alla viabilità e alla salvaguardia del patrimonio culturale chiedendo un intervento puntuale e preciso. Sui dispositivi mobili degli agenti incaricati saranno visualizzate, su mappe georeferenziate, un insieme micro-task, come ad esempio, "Recarsi in prossimità dei punti di accesso alla città per controllare e monitorare il regolare deflusso di mezzi pesanti e di persone", "Recarsi in prossimità del monumento, per garantire un adeguato livello di sicurezza pubblica e tutela del patrimonio culturale", oppure "Recarsi presso la zona interessata dalla manifestazione e chiudere i principali varchi di accesso ".
Lo scenario sulla protezione del territorio avrà due tipi di ricadute, a) aumentare la sicurezza e prevenire il deturpamento o addirittura la distruzione dei beni del patrimonio culturale del territorio, b) agevolare e aumentare il coinvolgimento dell'indotto coinvolto nella manutenzione e tutela del territorio (ricaduta industriale).

2. Sicurezza delle infrastrutture industriali.
Le infrastrutture industriali sono sempre più articolate, di ampie dimensioni e complesse, caratterizzate da un elevato (quando non innumerevole) numero di componenti ed agenti con cui interagiscono. Esistono variegati esempi di tali infrastrutture industriali, quali centrali elettriche e la relativa rete per la distribuzione dell'energia, gasdotti, porti e loro logistica, raffinerie e piattaforme petrolifere, fino anche ad includere strutture come server-farm e grandi data-center, nonché le grandi reti di telecomunicazioni. È facile notare come impianti quali raffinerie, impianti chimici o porti hanno spesso un enorme impatto sul territorio circostante e possono causare essere all'origine di crisi ed emergenze che devono essere trattate in maniera ampia e completa, coinvolgendo la protezione civile e le persone che vivono o si trovano a transitare nelle vicinanze (ad esempio, ai fini dell'evacuazione della zona).
Come esempio di infrastruttura industriale critica consideriamo una raffineria (ad esempio la Stanic di Livorno). Infatti, strutture per il raffinamento di petrolio rappresentano un'infrastruttura critica, dato il largo utilizzo del petrolio per la produzione di energia, nel settore dei trasporti, e nella produzione di beni e materiali: disservizi nelle forniture e nel raffinamento di petrolio portano effetti negativi direttamente sulla vita quotidiana delle persone e del Paese in genere. Inoltre, il petrolio è molto infiammabile e quando brucia sprigiona sostanze nocive e molto inquinanti. Incidenti (casuali o dovuti a sabotaggio) in una raffineria possono causare ingenti incendi, esplosioni, fumi che coinvolgono non solo l'area della raffineria, ma anche le aree circostanti. Si pensi che la raffineria del gruppo Saras in Sarroch (Sardegna), una delle più grandi e complesse di Europa, con una capacità di lavorazione di circa 300.000 barili al giorno, è collocata nelle prossimità di un paese di 5.327 persone (molte di più nel periodo estivo).
È facile vedere tanto la difficoltà quanto l'importanza di effettuare un'accurata attività di sorveglianza di tali infrastrutture, e di definire accurati piani operativi di crisi management. Data la complessità di tali infrastrutture ed impianti, è facile notare come le attività di sorveglianza, e gli interventi scaturiti da eventuali segnalazioni, sono sempre più importanti, sofisticati, e costosi.
Il pilota sarà implementato con le soluzioni definite e realizzate nel progetto Secure! ed integrate nel relativo Secure! Framework al fine di offrire un supporto per integrare, centralizzare e coordinare le attività di sorveglianza e manutenzione e gestione delle crisi per infrastrutture industriali, quindi per semplificarne la gestione. Questi scenari permetteranno di evidenziare i benefici dell'applicazione della piattaforma Secure! per infrastrutture industriali.
Come primo esempio, supponiamo vi siano sabotatori nei pressi od all'interno di un'infrastruttura critica, quale la raffineria presentata sopra. Le reti di sensori distribuite nell'infrastruttura critica forniscono Secure!Relevant Data relativamente ad una attività sospetta registrata, che sono trasformati in Secure!Useful Info a seguito di una prima attività di analisi. In seguito i Secure!Event generati, analizzati in tempo reale, permettono di evincere (Secure!situation) che c'è un movimento anomalo nei pressi della raffineria. Opportune segnalazioni da parte di persone casualmente nelle vicinanze si potrebbero rivelare determinanti per alzare il livello di allerta con sufficiente anticipo; tramite le Crowdsourcing Mobile Apps si acquisiscono così Secure!Relevant Data addizionali, che opportunamente integrati ai dati già disponibili permettono al sistema Secure! di capire con precisione la gravità della situazione, ed indicare con certezza le azioni da intraprendere (Secure! decisions and actions). Questo scenario permette di verificare l'applicabilità del sistema Secure! per soluzioni di early warning e prevenzione, per identificare rapidamente e con un elevato coverage possibili attività sospette (di sabotaggio), raccogliendo, integrando e analizzando informazioni provenienti dalla sensoristica dislocata nell'infrastruttura e da possibili segnalazioni di persone o del personale sul luogo (anche non specificatamente addetto alla sorveglianza) tramite specifiche applicazioni per dispositivi mobili.
Come secondo esempio, consideriamo il caso in cui nell'infrastruttura critica quale la raffineria di sopra si sia verificato un grave incidente, ad esempio un incendio. In questo caso, è importante evacuare il personale della raffineria ed i civili che si trovano nelle vicinanze di questa.
1. Secure! permette di raccogliere dai sensori della raffineria, dai social network e tramite le

Crowdsourcing Mobile Apps, informazioni sulle caratteristiche dell'incendio, sulla posizione delle persone, oppure su eventuali segnalazioni utili per guidare le operazioni di soccorso (tutte queste informazioni sono raccolte nelle Secure! Useful Info, ed integrate generando Secure! Event).
2. Le informazioni integrate permettono un'attenta analisi della situazione (Secure!situation) e importanti Secure!decisions and actions che permettono operazioni di soccorso accurate ed efficienti.
In questo scenario Secure! è molto importante non solo in quanto raccoglie input da varie sorgenti e fornisce output per il personale addetto, ma anche perché permette di distribuire output (informazioni) importanti a civili e al personale localizzato nell'area coinvolta (tramite le Situation-Awareness-Apps. Questo scenario mostra come l'utilizzo di Secure! e dei suoi supporti informatici, opportunamente integrato con logiche di crisis management, permette di aiutare le operazioni di localizzazione delle persone, studio e analisi del disastro e identificazione delle migliori linee di intervento, cosi come di raggiungere un ampio numero di persone tramite le applicazioni ad-hoc per dispositivi mobili. Si nota inoltre il possibile impatto, in casi del genere, dell'analisi offline (Secure! Analytics) effettuata sulla mole di dati raccolti, che può essere sfruttata per evidenziare le cause e ricostruire la situazione a posteriori.
Nell'ambito del progetto saranno implementati i 2 piloti sopra descritti che sperimenteranno i risultati di ricerca raggiunti all'interno dei vari obiettivi operativi e attività. Tuttavia, il sistema Secure! può essere personalizzato in diversi casi d'uso che vanno oltre agli scenari usati per la sperimentazione. Per esemplificazione riportiamo qui di seguito un ulteriore potenziale caso d'uso che può essere realizzato usando le tecnologie di Secure! Ciò va a dimostrare le forti potenzialità di replicabilità del sistema e di conseguenza il forte impatto che tali servizi possono avere sul territorio, le relative ricadute economiche e le potenzialità di mercato che Secure! può offrire.
Rilevamento frodi fiscali
L'interesse in sistemi automatici per il rilevamento di frodi fiscali è di forte attualità: da Gennaio 2012 i conti corrente dei contribuenti potranno essere sottoposti a controllo da parte dell'Agenzia delle Entrate per individuare casi di evasione fiscale, senza previa autorizzazione dell'autorità giudiziaria. Queste, ed altre informazioni saranno gestite da un sistema informatico chiamato "Serpico". Semplificando, possiamo dire che Serpico è un sistema avanzato di analisi di dati "top-down" che, dato un insieme di schemi di comportamento fraudolento definiti da un esperto o dedotti in maniera automatica, permette di individuare situazioni sospette che meritano ulteriori indagini fiscali. È evidente quale sia la complessità del sistema, e quanto siano numerosi i fattori da prendere in considerazione per una analisi affidabile (liquidità, investimenti, proprietà, beni di vario tipo, ecc.). Noi crediamo che un approccio bottom-up possa fornire informazioni complementari altrimenti non disponibili che migliorerebbero la precisione delle indagini fiscali.
1. Strumenti di crowd-sensing permetterebbero ad esempio al cittadino di segnalare situazioni anomale o irregolari, ad esempio la mancata emissione di scontrini fiscali, oppure la vendita di prodotti contraffatti o adulterati, etc.
2. Il crowd-sensing potrebbe anche generare informazioni senza una partecipazione volontaria da parte dei cittadini, ad esempio, stimando il numero di clienti di un esercizio sulla base dei commenti presenti in social network come Twitter o Facebook, o del matching tra dispositivi wireless o bluetooth.
3. In maniera complementare, il crowd-sourcing potrebbe supportare una analisi di livello più alto, suggerendo interventi di controllo da parte di personale abilitato. Il sistema potrebbe richiedere di valutare la veridicità di alcune segnalazioni riguardo l'emissione di ricevute fiscali, o ad un esperto di valutare il valore attuale di un immobile. Tutte queste informazioni sarebbero di grande supporto a sistemi informativi di più alto livello.
Un approccio secondo la filosofia del progetto Secure! permetterebbe di:
(a) ottenere informazioni rilevanti per la lotta all'evasione tramite la collaborazione con i cittadini,
(b) di produrre stime statistiche basate sull'analisi di social network, di altre sorgenti Web, o di dati di sensori,
(c) di svolgere compiti di verifica e controllo estensivi sfruttando "personale esterno",
(d) più in generale di raggiungere una capillarità e una adattabilità a casi localizzati e specifici che non sarebbero possibili altrimenti.
Sfruttamento della piattaforma Secure! insieme ad infrastrutture esistenti
Un'altra delle possibili applicazioni della piattaforma Secure!, riguarda il suo utilizzo integrato con l'infrastruttura TIX di Regione Toscana per la gestione di situazioni di emergenza ambientale.
La piattaforma Secure! sarà in grado di interagire in maniera interoperabile con alcuni degli altri servizi di raccolta dati già presenti al TIX stesso in maniera bidirezionale. Potrà infatti, sia accrescere il numero dei propri canali informativi da cui raccogliere informazioni per sviluppare il processo decisionale, sia distribuire, in maniera opposta, messaggi informativi, allarmi, indicazioni di intervento, relativi ad un certo evento sotto osservazione, verso soggetti pubblici e non, incaricati di intervenire (e.g. vigili del fuoco, strutture sanitarie, uffici di polizia, istituzioni locali). La piattaforma costituirà quindi uno strumento di supporto integrativo, a livello regionale, alle ordinarie procedure adottate per la gestione di situazioni di crisi o di emergenza, e, potenzialmente, per la previsione delle

stesse.
Impatto
Ormai è un dato di fatto che l'utilizzo efficace ed efficiente di tecnologie informatiche possa favorire l'efficacia dell'azione di operatori pubblici e privati, coinvolgendo anche come attori principali i cittadini. Secure! andrà a dimostrare che benefici importanti si possono ottenere attraverso l'utilizzo di tecnologie e metodi innovativi quali il crowdsourcing, in un modello di innovazione dove il servizio è creato e reso efficace direttamente dalle persone organizzate in una comunità virtuale.
Più specificamente il framework Secure! e le sue specifiche specializzazioni potrà essere impiegato come un importante strumento di supporto alla gestione dell'emergenza (prima, durante e dopo), mettendo a frutto sinergicamente gli approcci del crowdsensing e del crowdsourcing alle necessità di monitoraggio e d'intervento sul territorio.
Il framework Secure! si presta ad essere impiegato in numerosi domini applicativi. In ogni dominio, il progetto Secure! offre la possibilità di utilizzare apps specifiche per permettere al cittadino di fare segnalazioni e ricevere istruzioni da seguire in caso di pericolo. In aggiunta ai due scenari sopra descritti su cui si realizzeranno i piloti dimostrativi, di seguito sono descritte brevemente altre valide possibili implementazioni
Scenario protezione beni architettonici e Culturali: Il patrimonio culturale rappresenta una importantissima fonte, non solo di cultura e qualità della vita, ma anche di ritorno economico per l'Italia in generale e in particolare per la Toscana. Oltre 10 milioni di visitatori all'anno arrivano in Toscana, ed ogni fenomeno di deturpamento o deterioramento del patrimonio culturale Toscano, oltre che essere moralmente inaccettabile, avrebbe conseguenze estremamente negative sull'economia regionale.
Molte imprese garantiscono la propria sostenibilità sui servizi turistici e culturali ed è di fondamentale importanza proteggere le straordinarie ricchezze culturali che ne consentono lo sviluppo economico e la competitività (in un settore in cui peraltro la concorrenza si fa sempre più agguerrita).
Il sistema Secure! una volta rilevate le varie situazioni di rischio di deterioramento o di danneggiamento organizzerà un piano d'intervento che sarà messo in atto tempestivamente dalle organizzazioni competenti assicurando così una migliore prevenzione, una più agevole manutenzione e una più attenta protezione dei vari beni architettonici.
Scenario protezione infrastrutture industriali. Le grandi infrastrutture civili e industriali sono oggi sistemi complesse, spesso di grandi dimensioni, e sono purtroppo molto soggette al rischio di incidenti o peggio di eventuali attacchi esterni che possono provocare delle situazioni di pericolo, anche molto grave, per l'industria stessa o per l'ambiente e la popolazione. La tempestiva rilevazione di situazioni a rischio ottenuta attraverso il sistema Secure! porterà ad una maggiore efficienza nelle azioni di intervento e ad una riduzione dei danni. L'impatto (benefici) potrebbero essere molto significative sia a livello economico, sia ambientale, sia, infine e soprattutto, di salvaguardia di vite umane.
Scenario frode fiscale. Il problema della riduzione dell'evasione fiscale è sempre più attuale. Nel periodo di crisi economica in cui stiamo vivendo è stata stimata una perdita di oltre 100 miliardi di Euro all'anno causata dalle evasioni fiscali, una cifra prossima al 7% del Pil, e compresa tra il 15 e il 20% delle entrate fiscali. L'infrastruttura Secure! offre la possibilità di sviluppare applicazioni specifiche di crowdsourcing e crowdsensing per contribuire a combattere l'evasione fiscale , con possibili benefici economici e sociali che sarebbero importantissimi (vedi scenario descritto nella sezione precedente)
Scenario ordine pubblico. Un aspetto molto importante che porta a ricadute sia sociali sia economiche è la garanzia della sicurezza della popolazione e del territorio sia in situazioni di normalità che in situazioni di potenziale rischio. Il crowdsourcing è applicabile a situazioni in cui gli eventi si verificano di frequente (es. il traffico, mobilità sostenibile, situazione di aggregazione di masse come manifestazioni, eventi pubblici, sportivi,...). Le segnalazioni dei cittadini diventano una fonte fondamentale per prevenire o gestire le situazioni a rischio. Ciò avrebbe un forte impatto sociale e ambientale ed economico.
La semplice considerazione a titolo di esempio dei suddetti scenari applicativi consente di rendersi conto che un framework come Secure! potrà avere importanti aspirazioni in termini di risultato economico, perché consentirà di relazionarsi con un importante mercato potenziale a livello nazionale ed internazionale, di soggetti che potrebbe essere interessato all'adozione.
Durante lo svolgimento delle attività progettuale, precisamente all'interno dell'obiettivo 5, sarà svolta una attenta analisi di mercato e saranno valutati e definiti modelli di business applicabili alla soluzione Secure!.
Beneficiari e potenziali clienti della infrastruttura Secure!:
I benefici che Secure! potrà apportare riguarderanno sia le organizzazioni e le imprese nel settore pubblico e privato che potranno usufruire di servizi e applicazioni ICT avanzate per migliorare la protezione e sicurezza soprattutto in situazioni di crisi, sia i cittadini sia attraverso il loro intervento potranno vivere situazioni più protette e sicure.
Qui di seguito alcuni dei potenziali beneficiari e clienti del sistema Secure!
Settore pubblico:

- Comuni, I comuni attraverso le applicazioni offerte da Secure! potranno in maniera efficiente avere un controllo a 360° sul territorio assicurando un continuo monitoraggio in tempo reale e garantendo una maggiore sicurezza sia al cittadino sia alle varie infrastrutture. I comuni sarebbero nel contempo beneficiari e potenziali clienti della soluzione Secure!
- Protezione civile, La protezione Civile potrebbe essere agevolata nello svolgimento del proprio lavoro accedendo ad informazioni sul territorio in tempo reale e potendo definire e eseguire al meglio il proprio piano di intervento. Anch'essi sono potenziali utenti del sistema.
Settore privato:
- Industrie: Le industrie attraverso il continuo monitoraggio delle loro infrastrutture potrebbero ridurre al minimo i rischi ed eventualmente in situazioni di crisi, un tempestoso intervento ridurrebbe al minimo i danni sia interni all'industria sia esterni: sicurezza dei cittadini e sicurezza ambientale. Quindi i soggetti che gestiscono impianti industriali fanno parte del mercato di Secure!. Anche industrie interessate a tecnologie di sorveglianza troveranno il framework Secure! di interesse.
- PMI sviluppatori di componenti: I componenti possono essere riutilizzati ed adattati per un range molto più largo di possibili applicazioni. Gli sviluppatori trarranno benefici da servizi di supporto, customizzazione, e consulenza che offriranno sui propri componenti nonché di visibilità all'interno dell'ecosistema territoriale.
- Organizzatori di eventi: una delle maggiori responsabilità degli organizzatori di grandi eventi è il controllo e il monitoraggio della sicurezza. Essi otterrebbero forti benefici dall'utilizzazione di Secure! Questi attori sono sicuramente dei potenziali clienti della soluzione Secure!
-Cittadini: I cittadini possono trarre vantaggio nella fruizione dei servizi avanzati rispetto allo stato dell'arte nonché di un numero maggiore di servizi personalizzati rispetto alle proprie esigenze, realizzabili grazie alla piattaforma Secure!. Inoltre saranno parte fondamentali per la popolazione di informazione all'interno della piattaforma Secure!
I partner del progetto
I partner partecipanti al progetto Secure! costituiscono una compagine ben affiatata (avendo già collaborato in a precedenti iniziative progettuali di ricerca e sviluppo) e che garantisce tutte le competenze richieste per il corretto svolgimento delle attività ed il pieno raggiungimento dell'obiettivo generale suddetto ed i relativi obiettivi operativi in cui lo stesso è decomposto.
In termini generali, la suddetta compagine consta di una grande azienda ICT (ENGINEERING Ingegneria Informatica s.p.a.), due PMI ICT (Crowd e Resiltech) e tre organismi di ricerca (Università di Firenze, Centro per la Comunicazione e l'Integrazione dei Media dell'Università degli Studi di Firenze, il Consiglio Nazionale delle Ricerche di Pisa). Questo equilibrio tra mondo della ricerca accademica e mondo della ricerca industriale, a nostro avviso, costituisce la giusta miscela per garantire un elevato grado di avanzamento dello stato dell'arte tecnologico-scientifico (come descritto nella relativa sezione) e l'effettiva applicazione dei risultati del progetto in contesti reali, come quelli degli scenari previsti per il progetto (descritti sopra) e scenari possibili (anch'essi brevemente accennati sopra).
Entrando più nel merito delle attività del progetto Secure!, in relazione alla partecipazione dei partner, si vuole rimarcare che la responsabilità obiettivi relativi di impostazione, integrazione (OO 1 - Secure! Framework) ed applicazione (OO 5: Applicazione e validazione in contesti reali) è affidata ad ENGINEERING, la quale ha anche la responsabilità delle componenti innovative per il supporto decisionale (obiettivo operativo 4). La responsabilità delle componenti innovative per il crowd-sensing è invece affidata a Crowd, laddove il CNR assume la responsabilità dell'obiettivo operativo 2 per la realizzazione dell'infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy. La seguente lista nostra le partecipazioni ed i ruoli dei partner nei vari obiettivi operativi:
? OO1 - Secure! Framework: ENGINEERING (responsabile), RESILTECH, Università di Firenze, MICC (partecipanti)
? OO2 - Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy: CNR (responsabile), RESILTECH, Università di Firenze, MICC, ENGINEERING (partecipanti)
? OO3 - Tecniche e componenti innovative di Crowd-sensing: CROWD (responsabile), MICC, ENGINEERING, CNR (partecipanti)
? OO4 - Tecniche e componenti innovative per il supporto decisionale: ENGINEERING (responsabile), RESILTECH, Università di Firenze, CNR (partecipanti)
? OO5 - Applicazione e validazione in contesti reali: ENGINEERING (responsabile), RESILTECH, Università di Firenze, MICC, CNR (partecipanti)
Le competenze ed il profilo tecnologico-scientifico dei suddetti partner sono brevemente riportati nel seguito.
ENGINEERING è un player globale e il primo gruppo di system integration in Italia, leader nell'offerta integrata e completa lungo l'intera catena del valore del software: progettazione, sviluppo, servizi di outsourcing, prodotti e soluzioni verticali proprietarie, consulenza IT e strategica, su misura per i modelli di business dei clienti su tutti i mercati. L'azienda conta 6.300 dipendenti, 37 sedi con una distribuzione capillare nelle Regioni italiane, presenza commerciale diretta nell'UE, in Irlanda e in Belgio, ed extra-UE in Brasile e area America latina. Grazie al piano di acquisizioni e alla capacità di

apertura di nuovi mercati, il Gruppo dispone di una capacità produttiva globale in 40 diversi Paesi. Con un valore della produzione di oltre 700 milioni di euro ed un market share del 7%, il gruppo ENGINEERING opera con 7 business unit: Finance, Pubblica Amministrazione Centrale, Pubblica Amministrazione Locale e Sanità, Oil & Services, Energy & Utility, Industry e Telecom, supportate da 5 centri competenza trasversali rispetto alle business unit e ad elevata specializzazione e dalla Divisione Ricerca & Innovazione che ha il doppio ruolo di promuovere la ricerca sul software a livello internazionale e trasferire l'innovazione al ciclo produttivo delle strutture di business.
ENGINEERING è partner e socio fondatore della piattaforma di software e servizi NESSI che ha già ricevuto 200 milioni di investimenti per progetti da sviluppare in ambito UE. ENGINEERING ha partecipato e partecipa costantemente a progetti di ricerca europei e nazionali, insieme ai principali player ICT, università e centri di ricerca.
Il progetto Secure! sarà prevalentemente realizzato nell'ambito dell'unità di ricerca "Intelligent Systems". Un risultato di tale ricerca è la suite di sviluppo PRACTIONIST (www.practionist.org), che sarà estesa ed utilizzata nel presente progetto, soprattutto per il supporto ai processi decisionali. Inoltre l'unità "Intelligent Systems" ha maturato negli anni competenze e risultati nei ambiti rilevanti per il progetto Secure!: sistemi intelligenti, interfacce intelligenti, sistemi di ragionamento pratico, infrastrutture autonomiche di erogazione di servizi, goal-oriented business process management, servizi ubiquitous, user profiling e social network analysis.
ENGINEERING partecipa a quasi tutte le attività del progetto, con una minore intensità sull'Obiettivo Operativo 2, in cui la maggiore competenza è espressa da CNR, Resiltech ed Università di Firenze.
L'Università degli Studi di Firenze è una Università con circa 25000 studenti, e che svolge attività di ricerca in svariati domini, dall'ingegneria alle scienze umane, architettura, medicina o informatica. Il gruppo di ricerca RCL (Resilient Computing Lab) presso il Dipartimento di Sistemi e Informatica ha il suo obiettivo centrale nella ricerca e sperimentazione di architetture e sistemi resilienti e sicuri. Il gruppo è attualmente coinvolto nella ricerca in due macro-aree: i) architetture e tecniche per i sistemi fault tolerant, infrastrutture e reti, e ii) validazione della dependability, trust e Qualità del Servizio (QoS) di sistemi informatici, attraverso tecniche analitiche, simulative e sperimentali. Membri del gruppo sono stati coinvolti in molti progetti cooperativi, inclusi progetti Nazionali e finanziati dalla Comunità Europea dal Framework 2 al Framework 7. Attualmente il gruppo è coinvolto nei progetti Europei FP7-SST-2008-234088 ALARP (A railway automatic track warning system based on distributed personal mobile terminals) ed ARTEMIS-JU-100022 CHESS, nel progetto Nazionale MIUR-PRIN DOTS-LCCI - - Dependable Off-The-Shelf based middleware systems for Large-scale Complex Critical Infrastructures", e nel Progetto Regionale Bando Unico R&S 2008-POR CREO attività 1.5 "SILFI - Sistema Intelligente per la Lotta al Fuoco Integrata". Le competenze apportate dal gruppo DSI nel progetto sono inerenti alla identificazione ed analisi dei requisiti critici per la sicurezza (obiettivo operativo 1 e 2), alla definizione di soluzioni architetturali e meccanismi per garantire la resilienza e sicurezza del sistema Secure! (obiettivo operativo 1 e 2), all'attività di validazione del sistema tramite approcci analitici, simulativi e sperimentali (obiettivo operativo 5), ed infine nella disseminazione dei risultati del progetto tramite presentazioni e partecipazioni a convegni di rilevanza Internazionale relativi all'ambito dei sistemi critici.
Resiltech è una giovane Società a Responsabilità Limitata, nata nel Settembre del 2007, che integra l'esperienza di ricerca accademica con competenze di verifica e validazione e di sviluppo nell'ambito dei sistemi resilienti. Il team fondatore di Resiltech è infatti composto da personale con Dottorato di Ricerca nell'ambito della progettazione e validazione sistemi critici, e da personale con ampia esperienza industriale nella medesima area. L'ampia esperienza di Resiltech nell'ambito della Verifica e Validazione la qualificano come un importante consulente per la certificazione di prodotti critici, principalmente nell'ambito ferroviario e dell'automotive, dove Resiltech offre il suo supporto a molte compagnie sia di piccole che di grandi dimensioni. Resiltech vanta importanti esperienze nell'ambito della ricerca e tecnologia ICT, in particolare nel campo della teoria e pratica dei sistemi resilienti.
Resiltech è stata coinvolta nel progetto Europeo FP7-ICT-CA-216295 AMBER Coordination Action ed è attualmente coinvolta nel progetto Europeo FP7-SST-2008-234088 ALARP (A railway automatic track warning system based on distributed personal mobile terminals) e nel Progetto Regionale Bando Unico R&S 2008-POR CREO attività 1.5 "SILFI - Sistema Intelligente per la Lotta al Fuoco Integrata".
Resiltech attualmente contribuisce alla definizione dello standard ISO26262 ed in AUTOSAR (principalmente nel settore WP1.3 Safety). Le competenze apportate da Resiltech nel progetto sono inerenti all'analisi dei requisiti, ed alla attività progettazione, sviluppo e validazione del sistema Secure! (obiettivo operativo 1), con attenzione agli aspetti critici, in particolare privacy e disponibilità (obiettivo operativo 2), riguardo ai quali Resiltech vanta ampia esperienza. Resiltech offre la possibilità di disseminazione dei risultati del progetto tramite presentazioni a corsi di formazione, partecipazioni a gruppi di lavoro, e convegni di rilevanza Internazionale.
Il Laboratorio Comunicazioni e Immagini (LCI) (http://lci.micc.unifi.it/labd/) è uno dei laboratori del Centro di Eccellenza MICC (Centro per la Comunicazione e l'Integrazione dei Media) dell'Università degli Studi di Firenze. LCI svolge attività di ricerca di base e azione di trasferimento tecnologico verso le imprese e gli enti pubblici. L'attività di ricerca si colloca nell'ambito dell'Ingegneria

dell'Informazione e della Multimedialità, qui di seguito sono elencati i principali settori di interesse.
Multimedia Forensics. Il gruppo di lavoro ha sviluppato metodologie per l'identificazione della sorgente di acquisizione (ad esempio marca e modello di fotocamere digitali) che esplorino le varie fasi di acquisizione di una fotocamera digitale cercando imperfezioni nel sensore di acquisizione (CCD) o sono volti a rintracciare il tipo di interpolazione cromatica nelle fotocamere dotate di Color Filter Array (CFA). Vengono sviluppate applicazioni e metodi indirizzati a identificare le operazioni di post-processing sull'immagine come la compressione (doppio JPEG), le trasformazioni affini (rotazioni, ridimensionamento), il cloning (regioni duplicate nell'immagine) e fotomontaggi volti a individuare regioni contraffatte all'interno dell'immagine sotto osservazione.
Television e Digitale Terrestre (DTT) e Applicazione MHP. Il gruppo di lavoro ha progettato e sviluppato applicazioni standard MHP per la DTT mediante l'utilizzo di software dedicati (authoring tool specifici) o direttamente in linguaggio Java. Il risultato di tale lavoro ha portato alla realizzazione di applicazioni di servizio di tipo sia statico che interattivo.
Il laboratorio è stato partner del Centro di Competenza sulla Televisione Digitale Terrestre (DTT-Toscana Lab).
Applicazioni Multimediali per i Beni Culturali. Le attività del laboratorio concernono anche la progettazione e lo sviluppo di applicazioni multimediali dedicate alla messa in rete di contenuti digitali e alla loro protezione con tecniche opportunamente sviluppate. Quest'ambito di ricerca tipicamente multidisciplinare coinvolge diverse esperienze e professionalità tra cui: programmazione Java, gestione di database e banche dati. Attualmente vengono realizzate applicazioni dedicate alla esposizione web di database di immagini e metadati di interesse culturale, messi a disposizione dalla Direzione Regionale per i Beni Culturali e Paesaggistici della Toscana.
Gli apporti tecnici che il gruppo LCI può fornire nell'ambito del progetto SECURE! sono inerenti alla definizione e accrescimento della sicurezza (obiettivi operativi 1 e 2), all'attività forense relativa ai media digitali (obiettivo operativo 3) e all'acquisizione di dati multicanale, con particolare riferimento al canale DTT, Televisione Digitale Terrestre, (obiettivo operativo 3). Un contributo è altresì fornito nell'ambito dell'attività di validazione del sistema tramite approcci analitici, simulativi e sperimentali (obiettivo operativo 5), nonché nella disseminazione dei risultati del progetto tramite presentazioni e partecipazioni a convegni di rilevanza Internazionale.
Il Consiglio Nazionale delle Ricerche (CNR) è un Ente pubblico nazionale con il compito di svolgere, promuovere, diffondere, trasferire e valorizzare attività di ricerca nei principali settori di sviluppo delle conoscenze e delle loro applicazioni per lo sviluppo scientifico, tecnologico, economico e sociale del Paese. Gli istituti del CNR sono le unità che svolgono le attività di ricerca e si caratterizzano per le competenze, le attrezzature sperimentali e l'eccellenza dei ricercatori. Successivamente all'entrata in vigore del DL di riordino del CNR nel giugno 2003, il CNR è organizzato in una rete di 107 istituti, tra questi lo IIT e L'ISTI sono all'interno dell'area della ricerca di Pisa, la più grande della rete scientifica del CNR.
L'unità di ricerca CNR (Pisa) che partecipa al progetto Secure! si avvale della competenza di 3 gruppi di ricerca: Sicurezza (SEC), High performance Computing (HPC) e multimedia (NeMIS) di seguito descritti.
Il gruppo sicurezza (SEC) ha maturato una notevole esperienza nel settore della sicurezza, inclusi aspetti di cyber-security. Le tematiche principali di ricerca vertono sulla sicurezza di servizi web e cloud e di devices mobili, sull'analisi di sistemi critici, su sistemi di trust (fiducia) e risk management ed sulla sicurezza di social networks/dynamic coalitions. Il gruppo di ricerca, composto da circa 20 persone, è attivamente coinvolto in diversi importanti progetti europei in corso di svolgimento, tra cui Contrail, CONNECT, SESAMO, ANIKETOS, ed ha lavorato sul progetto regionale VISITOTuscany. Il gruppo coordina attualmente il progetto Europeo NESSoS, una rete di eccellenza per la sicurezza dell'Internet del Futuro. Il gruppo e'è anche attivo nel coordinamento della piattaforma tecnologica italiana SERIT (Security Research in ITaly).
La ricerca svolta dal Laboratorio di High Performance (HPC) è finalizzata alla ricerca, progettazione e sviluppo di sistemi e soluzioni per problemi complessi, utilizzando tecniche di calcolo ad alte prestazioni. Settori principali di ricerca sono: Data and Web Mining, Information Retrieval, Distributed Search Engines, Service-Oriented Architectures, Cloud and Peer-to-Peer Systems. L'enfasi è posta sui requisiti di alte prestazioni, sia dei servizi offerti che delle applicazioni finali. Il gruppo di ricerca, composto da circa 20 persone, è attivamente coinvolto in diversi importanti progetti europei in corso di svolgimento, tra cui S-Cube, Contrail, Assets, IngeoClouds.
Il gruppo NeMIS ha maturato una lunga esperienza sullo studio e realizzazione di tecniche di image searching e content recognition. In particolare, le tecniche sviluppate, oltre ad offrire un alto grado di accuratezza, sono altamente scalabili e permettono di gestire sull'ordine delle centinaia di milioni di immagini. Il gruppo ha una lunga esperienza nella gestione di progetti di ricerca europei e finanziati da fondi strutturali. Il gruppo e'è stato anche recentemente coordinatore del progetto regionale VISITOTuscany.
In questo progetto il CNR è coinvolto in molte attività ed in tutti gli obiettivi operativi. Il CNR è responsabile dell'obiettivo operativo 2: Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e

privacy.
Crowd è un'azienda che ha innovato il modo di collaborare su Internet mediante l'applicazione del crowdsourcing ai processi di business. Crowd svolge tutta la ricerca e sviluppo tra le sedi di Pisa e di Catania, sedi nelle quali impiega una quindicina di persone altamente specializzate e votate all'innovazione tecnologica e di processo.
Crowd ha una presenza diretta oltre che in Italia in altri paesi europei quali Francia, Inghilterra, Germania e Spagna, e extra europei come gli Stati Uniti attraverso la controlla CrowdEngineering.
Crowd si è già distinta nell'innovazione sul crowdsourcing meritando dei riconoscimenti quale il titolo di "Cool Vendor in Social Software and Collaboration" di Gartner, "Company to watch in Social CRM" di Altimiter.
All'interno del progetto Crowd si occupa della ricerca e sviluppo delle tecnologie e modelli di crowdsourcing e della realizzazione di componenti innovative di crowdsensing (nell'ambito dell'obiettivo operativo 3).

Eventuale documentazione aggiuntiva

File:	Figura 1 L'architettura del sistema.gif
File:	FIgura 2 I flussi di dati ed informazioni.gif
File:	Figura 3 Dipendenze fra gli obiettivi operativi.gif
File:	Figura 4 Un tweet %22rilevante%22.gif
File:	Secure Gantt.pdf.p7m
File:	bibliografia secure.pdf
File:	Nessun file Caricato

OBIETTIVI OPERATIVI

Obiettivo operativo 1: *Secure! Framework*

- Attività 1.1: *Analisi dei requisiti*
- Attività 1.2: *Definizione dell'architettura del sistema*
- Attività 1.3: *Definizione ed implementazione dell'infrastruttura di integrazione*
- Attività 1.4: *Definizione ed implementazione di servizi ed applicazioni*
- Attività 1.5: *Integrazione del sistema*

Obiettivo operativo 2: *Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy*

- Attività 2.1: *Analisi dei requisiti di affidabilità, sicurezza, fiducia e privacy dell'infrastruttura di raccolta dei dati e gestione dei dati e dei servizi disponibili*
- Attività 2.2: *Definizione di soluzioni architetturali per i vari domini applicativi in esame, inclusi dispositivi mobili e di sensori/attuatori*
- Attività 2.3: *Strumenti e meccanismi per garantire aspetti di affidabilità, sicurezza fiducia e privacy per la rete di raccolta di informazioni per la infrastruttura di gestione dei dati e di decisione.*
- Attività 2.4: *Modelli e algoritmi per la privacy dei dati, sia in fase di acquisizione che di gestione e diffusione.*
- Attività 2.5: *Modelli e algoritmi per la gestione di reti sociali autonome e della credibilità dell'informazione raccolta e diffusa.*

Obiettivo operativo 3: *Tecniche e componenti innovative di Crowd-sensing*

- Attività 3.1: *Analisi tecniche crowd-sensing e crowd-sourcing*
- Attività 3.2: *Definizione di tecniche e servizi per la raccolta dati*
- Attività 3.3: *Definizione di tecniche e servizi per l'estrazione di informazioni rilevanti da sorgenti multimodali*
- Attività 3.4: *Preparazione delle informazioni per la successiva fase di decisioning/acting*
- Attività 3.5:

Obiettivo operativo 4: *Tecniche e componenti innovative per il supporto decisionale*

Attività 4.1: *Definizione di modelli di gestione dei contenuti e delle decisioni*

Attività 4.2: *Definizione ed implementazione di tecniche e servizi di elaborazione ed analisi in tempo reale (situation awareness)*

Attività 4.3: *Definizione ed implementazione di servizi e meccanismi decisionali*

Attività 4.4: *Definizione ed implementazione di tecniche e servizi per l'analisi off-line (Secure! Analytics)*

Attività 4.5:

Obiettivo operativo 5: *Applicazione e validazione in contesti reali*

Attività 5.1: *Definizione e pianificazione dei piloti per la sperimentazione*

Attività 5.2: *Sviluppo applicazioni specifiche per i piloti*

Attività 5.3: *Test e validazione*

Attività 5.4: *Impatto*

Attività 5.5:

OBIETTIVO OPERATIVO N. 1

Denominazione: Secure! Framework

Descrizione dell'obbiettivo operativo

Questo obiettivo operativo ha il compito di definire il framework metodologico, concettuale e tecnologico dell'intero progetto Secure! e di integrazione dei risultati prodotti da tutti gli altri obiettivi operativi ed attività.
In particolare, dal punto di vista logico-concettuale verranno raccolti ed analizzati i requisiti funzionali ed non funzionali per lo sviluppo di sistemi basati sul crowdsourcing e sui social media per la gestione delle emergenze o di situazioni pericolose (attività 1.1).
Sulla base di questi requisiti verrà definito un modello di architettura orientata ai servizi che possa fungere da riferimento per la definizione e lo sviluppo delle varie componenti e servizi realizzati negli obiettivi operativi 2, 3 e 4 (attività 1.2).
A partire dalla suddetta architettura, verrà definito e realizzato un framework di integrazione delle diverse componenti risultanti dal progetto (attività 1.3), sia esterne (dati provenienti dai social media, da reti di sensori, da sistemi informativi già esistenti, ed infine dati ed informazioni acquisiti da applicazioni mobile), che interne (i vari servizi che implementano le tecniche innovative di estrazione ed analisi di informazioni e di supporto alle decisioni e l'infrastruttura di gestione della sicurezza, della privacy e del trust). Tale framework sarà fondamentalmente l'implementazione dell'architettura definita nell'attività 1.2, mediante l'adozione e l'opportuna estensione di uno o più middleware Open Source per l'integrazione e la composizione di servizi e di informazioni eterogenee. La suddetta infrastruttura integrerà anche l'infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy risultante dall'obiettivo operativo 2.
Sulla base di tale infrastruttura di integrazione e delle componenti/servizi definiti negli obiettivi operativi 3 e 4, verranno anche realizzate alcune applicazioni e servizi la gestione delle emergenze e delle situazioni di pericolo, per la sicurezza pubblica e la protezione civile (attività 1.4): queste saranno le Secure! Crowdsourcing Apps, le Secure! Situation-awareness Apps e le Secure! Analytics Services.
Si noti che le suddette applicazioni e servizi avranno un carattere generale, agnostico rispetto allo specifico dominio o scenario da istanziare: nell'ottica del framework, saranno pertanto prevalentemente degli artefatti software che validano il modello di servizi concepito integrando tutte le innovazioni proposte dal progetto. Tali artefatti saranno comunque un importante "punto di partenza" per loro personalizzazione e la costruzione di applicazioni e servizi specifici per settori e scenari specifici (come quelli definiti ed implementati nell'obiettivo operativo 5).
Infine in questo obiettivo operativo verranno integrate tutte le componenti del sistema realizzate nel progetto e le varie componenti/servizi/sistemi esterni sia per l'integrazione logica nel Secure! Fremework che da utilizzare nelle le fase di validazione (e quindi specifiche per i piloti considerati).

Risultati Attesi: deliverable e milestones

Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito del presente obiettivo operativo, sono previsti i seguenti risultati misurabili e verificabili (deliverable):
- D1.1 - Specifica dei requisiti (Mese 6) [si prevede una versione draft al Mese 3]
- D1.2 - Architettura orientata ai servizi del Secure! Framework (Mese 12) [si prevede una versione draft al Mese 8]
- D1.3 - Specifica dell'infrastruttura di integrazione (Mese 15) [si prevede una versione draft al Mese 10]
- D1.4 - Servizi ed applicazioni di crowsourcing, situation-awareness ed analytics (Mese 12, 21)
- D1.5 - Secure! Framework (Mese 12, 18, 24)
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M1.1 - Analisi dei requisiti per il Secure! Framework completata (Mese 6)
- M1.2 - Prima versione dell'architettura e delle scelte infrastrutturali completati (Mese 8)
- M1.3 - Definizione dell'architettura completata (Mese 12)
- M1.4 - Prima versione del Secure! Framework disponibile ed utilizzabile per lo sviluppo di applicazioni specifiche (Mese 12)

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**
I deliverable precedentemente elencati sono i risultati delle attività secondo quanto di seguito specificato:
- D1.1 - Specifica dei requisiti [Risultato dell'attività 1.1]
- D1.2 - Architettura orientata ai servizi del Secure! Framework [Risultato dell'attività 1.2]
- D1.3 - Specifica dell'infrastruttura di integrazione [Risultato dell'attività 1.3]
- D1.4 - Servizi ed applicazioni di crowsourcing, situation-awareness ed analytics [Risultato dell'attività 1.4]
- D1.5 - Secure! Framework [Risultato dell'attività 1.5]

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**
Le milestone precedentemente elencate sono punti di verifica relative alle attività secondo quanto di seguito specificato:
- M1.1 - Analisi dei requsiiti per il Secure! Framework completata [Risultato dell'attività 1.1]
- M1.2 - Prima versione dell'architettura e delle scelte infrastrutturali completati [Risultato dell'attività 1.2]
- M1.3 - Definizione dell'architettura completata [Risultato dell'attività 1.2]
- M1.4 - Prima versione del Secure! Framework disponibile ed utilizzabile per lo sviluppo di applicazioni specifiche [Risultato delle attività 1.3, 1.4, 1.5]

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Obbiettivo operativo

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Costo toale dell'obbiettivo

Indicare il costo complessivo dell'obbiettivo Operativo

Costo totale dell'obbiettivo: 1.748.261,83

ATTIVITÀ N. 1.1

Denominazione: Analisi dei requisiti

Descrizione singola attività

In questa attività verrà effettuata l'analisi dei requisiti del Secure! Framework, al fine di definire l'insieme delle proprietà e le caratteristiche logiche di un sistema caratterizzato dall'utilizzo del crowdsourcing e dei social media per la gestione delle emergenze o di situazioni pericolose.
In questo senso, verranno analizzati i sistemi esistenti e le modalità di gestione delle suddette situazioni di emergenza, al fine di tracciare uno stato dell'arte (as-is) sul quale provare a costruire i modelli e le soluzioni innovative proposte dal presente progetto. Come parte di questa attività, verrà svolta anche l'analisi preliminare (ed un censimento aggiornato) delle soluzioni open source integrabili nel Secure! Framework. Tale analisi sarà poi completata e specializzata nelle altre attività di questo obiettivo operativo (soprattutto 1.2, 1.3 ed 1.4), ognuna con riferimento specifico agli aspetti in essa considerati.
Verranno altresì studiati ed analizzati esempi di applicazione del crowdsourcing a situazioni di emergenza, di sicurezza pubblica e protezione civile, considerando anche l'applicazione a scenari di gestione di crisi e situazioni catastrofiche (terremoti, alluvioni, ecc.), al fine di determinare un insieme di requisiti e casi d'uso che potranno essere applicati ed estesi nel presente progetto. Questa analisi sarà ulteriormente sviluppata con il coinvolgimento di alcuni utenti potenziali, opportunamente selezionati e coinvolti nel progetto, al fine di studiare insieme a loro la reale applicabilità dei meccanismi del crowdsourcing nel contesto di situazioni reali.
Un aspetto importante che sarà studiato nel corso di questa attività è lo studio degli aspetti motivazionali degli utenti coinvolgibili nei processi e nei meccanismi di crowdsourcing oggetto del progetto. In questo senso saranno identificati, analizzati e specificati alcuni indici (da misurare nelle analytics), linee guida (da seguire nello sviluppo delle applicazioni), requisiti specifici da soddisfare (sia a livello di framework che di applicazioni) e di processi da seguire sfruttando al massimo le folle.
Collegati agli aspetti motivazionali vi sono le modalità di interazione e di utilizzo delle applicazioni di crowdsourcing: è fondamentale definire meccanismi e strumenti affinché gli utenti possano facilmente fornire le informazioni che poi servono a gestire le situazioni di emergenza. Anche in questo caso saranno definite alcune linee guida, requisiti ed pattern di presentazione ed interazione (che includono anche esempi di widget o componenti di interfacce utente).
Da un punto di vista metodologico, tale analisi dei requisiti sarà effettuata utilizzando insieme tecniche goal-oriented (soprattutto per la cosiddetta early requirement analysis) come i e specifica dei casi d'uso, al fine di sfruttare le potenzialità di entrambi.*
Il risultato di tale analisi sarà quindi un documento di specifica dei requisiti che mira ad essere di riferimento per il progetto intero (D1.1 - Specifica dei requisiti).

Strumenti/attrezzature

Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane

Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 35 mesi uomo.

Subcontratti

Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività

Non prevista.

Risultati Attesi: deliverable e milestones

Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.

Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D1.1 - Specifica dei requisiti (Mese 6) [si prevede una versione draft al Mese 3]
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M1.1 - Analisi dei requisiti per il Secure! Framework completata (Mese 6)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 188.196,22

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

ATTIVITÀ N. 1.2

Denominazione: Definizione dell'architettura del sistema

Descrizione singola attività
Sulla base dei requisiti definiti nell'attività 1.1, in questa attività verrà studiata, definita e specificata l'architettura orientata ai servizi (logica e concreta) del Secure! Framework e l'architettura logica del modello di sistemi specifici di gestione delle emergenze realizzabili con esso.
Tale architettura dovrà essere il riferimento per la definizione e lo sviluppo delle varie componenti e servizi realizzati negli obiettivi operativi 2, 3 e 4. In tal senso, saranno specificate le interfacce e il modello delle informazioni per la comunicazione tra le componenti/servizi del framework e con i sistemi/servizi esterni.
L'architettura, definita sia come hardware (server) e software (infrastruttura in cui integrare i servizi offerti) dovrà soddisfare requisiti di elevata disponibilità, sicurezza e prestazioni, ed offrire soluzioni (servizi dedicati) per la gestione di eventuali vincoli temporali o priorità nelle richieste. Per soddisfare tali requisiti, si includeranno nell'architettura soluzioni hardware e software volte a garantire la resilienza del sistema; in particolare, si prevede la definizione e introduzione di meccanismi di monitoring dell'infrastruttura e dei suoi servizi, al fine di valutare in modo continuo lo stato del sistema ed innescare rapidamente azioni di recupero/ripristino/manutenzione qualora necessario. In questo contesto si investigheranno anche soluzioni per garantire il corretto funzionamento dell'architettura in caso di aggiornamento di servizi esistenti od introduzione (online; cioè mentre il sistema è in esecuzione ed aperto agli utenti) di nuovi servizi; a tal riguardo si prevede l'introduzione nell'architettura di meccanismi di supporto (basati su soluzioni per il testing online ed automatico dell'architettura) volti a validare online la corretta installazione ed il corretto comportamento dei nuovi servizi introdotti, oppure dell'aggiornamento dei servizi esistenti.
L'architettura sarà specificata utilizzando diagrammi in linguaggio Unified Modelling Language (UML), ed eventualmente alcuni suoi profili opportunamente definiti) e le interfacce saranno specificate utilizzando standard e linguaggi tipici dei Web Services (es. WSDL, BPEL, WSCDL e tutti gli altri linguaggi ad essi correlati).
Il risultato dell'attività sarà pertanto un documento di specifica architetturale ed un insieme di specifiche di servizi e di modelli di informazioni per le interfacce (D1.2 - Architettura orientata ai servizi del Secure! Framework).

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 96 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D1.2 - Architettura orientata ai servizi del Secure! Framework (Mese 12) [si prevede una versione draft al Mese 8]
Analogamente è previsto i seguenti punti di verifica dei risultati di progetto:
- M1.2 - Prima versione dell'architettura e delle scelte infrastrutturali completati (Mese 8)
- M1.3 - Definizione dell'architettura completata (Mese 12)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività
Costo totale dell'attività: 507.802,31

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

ATTIVITÀ N. 1.3

Denominazione: Definizione ed implementazione dell'infrastruttura di integrazione

Descrizione singola attività
A partire dalla specifica dell'architettura (si veda l'attività 1.2), in questa attività verrà definito e realizzato un framework di integrazione delle diverse componenti coinvolte nel progetto. Queste includono sia componenti/servizi interni al Secure! Framework (definiti negli obiettivi operativi 2, 3 e 4), sia servizi esterni di raccolta di: (i) dati estratti dai social media (es. Twitter, Facebook, blog, forum, ecc.), (ii) dati provenienti da reti di sensori dispiegate nel territorio, (iii) dati provenienti da sistemi informativi esistenti (diversi da caso a caso, ma comunque da integrare nel caso di deployment del framework in contesti reali), (iv) dati ed informazioni raccolte da applicazioni mobile opportunamente sviluppate per servizi specifici (anche questi dipendenti dallo scenario applicativo).

Per tutti questi casi, che presentano una notevole eterogeneità, verranno analizzati ed adottati standard diffusi per l'interoperabilità e l'integrazione. Ad esempio, nel caso dei social media verranno adottate le APIs già offerte dai più diffusi; nel caso delle reti di sensori, esistono alcuni standard (es. OGC SWE) che verranno opportunamente studiati, valutati ed eventualmente integrati.
Per quanto riguarda le componenti interne del Secure! Framework (i vari servizi che implementano le tecniche innovative di estrazione ed analisi di informazioni e di supporto alle decisioni e l'infrastruttura di gestione della sicurezza, della privacy e del trust), verranno invece implementati i meccanismi di integrazione in accordo alle specifiche definite nell'architettura, sfruttando ed appoggiandosi su infrastrutture Open Source di integrazione ed orchestrazione di servizi (es. Spagic), di integrazione e di gestione di informazioni eterogenee e di creazione di applicazioni Web 2.0. A tal fine, nell'ambito di questa attività verranno anche ulteriormente analizzati (ed eventualmente integrati) alcuni strumenti open source precedentemente identificati nell'attività 1.1, al fine di determinare la migliore soluzione per le esigenze del progetto.
La suddetta infrastruttura integrerà anche i risultati dell'obiettivo operativo 2, in termini di infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy.
Il risultato di questa attività sarà un middleware di integrazione di servizi ed informazioni (D1.3 - Specifica dell'infrastruttura di integrazione), accompagnato da un report di progettazione e descrizione dello stesso.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 46.8 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D1.3 - Specifica dell'infrastruttura di integrazione (Mese 15) [si prevede una versione draft al Mese 10]
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M1.4 - Prima versione del Secure! Framework disponibile ed utilizzabile per lo sviluppo di applicazioni specifiche (Mese 12)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 264.180,53

Eventuale documentazione Aggiuntiva

Upload:	Nessun file Caricato
Upload:	Nessun file Caricato
Upload:	Nessun file Caricato

ATTIVITÀ N. 1.4

Denominazione: Definizione ed implementazione di servizi ed applicazioni

Descrizione singola attività

In questa attività verranno definiti, progettati ed implementati alcuni servizi che, integrando i componenti/servizi definiti negli obiettivi operativi 3 e 4, offrono funzionalità per la gestione delle emergenze e delle situazioni di pericolo, per la sicurezza pubblica e la protezione civile. Tali servizi ed applicazioni saranno realizzati sfruttando le funzionalità offerte dall'infrastruttura di integrazione definita e realizzata nell'attività 1.3.
In particolare verranno definite e sviluppate alcune applicazioni installabili su dispositivi mobili personali (smartphone e tablet con sistemi operativi Android ed iOS) ed alcune applicazioni Web (fruibili attraverso un Web browser).
Le applicazioni mobili saranno principalmente rivolte ai sensori umani che forniscono informazioni sul campo e che possono essere anche coinvolti in micro-task opportunamente coordinati dal sistema per la gestione dell'emergenza (Secure! Crowdsourcing Apps). In questo senso verranno realizzati alcuni semilavorati software per la raccolta di informazioni sul campo, da integrare ed estendere nel contesto di applicazioni specifiche di crowdsourcing.
Vi saranno poi anche applicazioni dedicate agli operatori sul campo, i quali potranno direttamente eseguire delle attività di prevenzione o mitigazione o intervento nelle specifiche situazioni di emergenze (Secure! Situation-awareness Apps). Anche in questo caso, saranno realizzate alcune componenti applicative da integrare nello sviluppo di servizi specifici legati al dominio o scenario applicativo.
Le applicazioni Web saranno invece dedicate al personale operante nelle varie sale operative o di coordinamento, o agli analisti, al fine di fornire loro strumento di analisi off-line, atte ad estrarre e valutare informazioni addizionali e supportare, nelle fasi post-emergenza, tutti i processi di miglioramento del sistema complessivo (Secure! Analytics Services). In questo caso saranno realizzate alcune componenti di analytics che potranno poi essere personalizzate ed integrate per lo sviluppo di dashboard specifiche sulla base di requisiti specifici legati al dominio applicativo considerato.
Si noti che la realizzazione di applicazioni specifiche, nel caso dei piloti realizzati nel progetto, è prevista nel contesto dell'attività 5.2, sulla base dei requisiti e delle esigenze specifiche raccolte ed elaborate nell'attività 5.1.
Il risultato di questa attività sarà pertanto un set integrato di applicazioni e servizi, secondo quanto detto sopra, accompagnato da un documento di descrizione e progettazione delle stesse.

Strumenti/attrezzature

Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane

Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 46.8 mesi uomo.

Subcontratti

Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività

Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D1.4 - Servizi ed applicazioni di crowsourcing, situation-awareness ed analytics (Mese 12, 21)
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M1.4 - Prima versione del Secure! Framework disponibile ed utilizzabile per lo sviluppo di applicazioni specifiche (Mese 12)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività
Costo totale dell'attività: 264.180,53

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

ATTIVITÀ N. 1.5

Denominazione: Integrazione del sistema

Descrizione singola attività
In questa attività verranno integrate tutte le componenti ed i servizi e componenti realizzati nelle attività di questo obiettivo operativo e di quelli realizzate negli obiettivi realizzativi 2, 3 e 4.
Il risultato sarà pertanto il Secure! Framework, corredato della documentazione per il suo utilizzo (manuali). Il Secure! Framework sarà un sistema consistente sul quale sarà possibile sviluppare ed integrare nuove applicazioni e servizi ed estendere/personalizzare quelle esistenti (risultanti dall'attività 1.4) nel contesto di sistemi di gestione delle emergenze, sicurezza pubblica e protezione civile basati sui meccanismi del crowdsourcing.
La versione finale del framework (disponibile al mese 24, alla fine del progetto) integrerà tutti i miglioramenti ed evoluzioni risultanti dalle due fasi di validazione.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 95.8 mesi uomo.

Subcontratti

Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D1.5 - Secure! Framework (Mese 12, 18, 24)
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M1.4 - Prima versione del Secure! Framework disponibile ed utilizzabile per lo sviluppo di applicazioni specifiche (Mese 12)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Costo totale dell'attività

Indicare il costo complessivo dell'attività
Costo totale dell'attività: 523.902,24

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

OBIETTIVO OPERATIVO N. 2

Denominazione: Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy

Descrizione dell'obbiettivo operativo
Scopo di quest' obiettivo operativo è lo studio, la progettazione e la realizzazione di architetture, metodologie, tecniche, protocolli e algoritmi per garantire la sicurezza, la privacy, l'affidabilità dell'infrastruttura del progetto Secure!. L'obiettivo deve coprire varie fasi del trattamento dei dati, ognuna con delle sue specificità e criticità. In particolare si devono prevedere soluzioni per l'acquisizione sicura dei dati, il loro trattamento garantendo la massima privacy possibile (dato il contesto), tecniche di fusione ed integrazione dei dati, gestione ed uso dei dati per i vari servizi offerti dalla piattaforma ed infine trasmissione dei dati.
La sicurezza e l'affidabilità della piattaforma sono cruciali per permettere l'adozione di questo tipo di tecnologie. I servizi offerti dalla piattaforma Secure! devono essere usufruiti solo dagli utenti autorizzati per gli scopi appropriati. La gestione dei dati, con aspetti legati alla persona, deve essere fatta con metodologie appropriate per permettere un bilanciamento tra gli aspetti di privacy e la loro utilità per prevenire e risolvere le emergenze (l'accesso ai dati dipende quindi anche dal contesto operativo). Vi è inoltre la necessità di rendere sicura ed affidabile l'infrastruttura, intesa come componenti hardware e software e le loro interazioni, sia con una progettazione efficace che con attività di monitoring continua.
Di particolare interesse, data la natura eterogena dei vari domini applicativi considerati nel progetto (che includono spesso comunità aperte e dinamiche di utenti), possiamo considerare la gestione della credibilità' dell'informazione, anche in presenza di canali di comunicazioni non affidabili in ambienti potenzialmente non controllati (e probabilmente con disconnessioni intermittenti come durante le emergenze) e la necessità che tutte le componenti della infrastruttura usino, quando appropriato, Privacy Enhanching Tecnologies (PET).
Abbiamo quindi due attività specifiche per questi due aspetti rilevanti.
La gestione di aspetti di privacy, legate alla acquisizione di dati legati alla persona, è di particolare

interesse in questo tipo di tecnologia. Da una parte si deve aumentare il livello di precisione di accesso ai dati (di modo da rendere molto fin-grained l'accesso e quindi permettere di sapere solo a chi deve operare need-to-know principle) dall'altro anche in fase di acquisizione si possono decidere strategie che minimizzano l'impatto sugli utenti (certamente mediando con il livello di criticità della situazione in oggetto). Anche le problematiche di integrazioni e operazioni su dati distribuiti tra più organizzazioni ha un suo rilievo e si pensa di poter usare tecnologie per la secure-multi-party computation.
La gestione della fiducia ed in generale la sicurezza nei social networks (o crowds) occupa un aspetto centrale nel progetto. In effetti tale gestione può avere unruolo sia come capacità di usare la fiducia per creare queste reti sociali e farle cooperare che come capacità di acquisire e filtrare l'informazione in maniera corretta e precisa . I modelli di cooperazione all'interno di questa comunità possono essere eterogenei così come i modelli di fiducia e tutte le varie situazioni (e possibili attacchi) vanno gestiti. In effetti, dovendo usare informazioni da più fonti, magari non interoperabili, il problema di riconoscere l'informazione credibile da quella non è cruciale.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito del presente obiettivo operativo, sono previsti i seguenti risultati misurabili e verificabili (deliverable):
- D2.1 - Requisiti di affidabilità, sicurezza, fiducia e privacy per l'infrastruttura (Mese 6) [si prevede una versione draft al Mese 3]
- D2.2 - Architettura della infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy (Mese 12) [si prevede una versione draft al Mese 8]
- D2.3 - Realizzazione delle componenti della infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy (Mese 18) [si prevede una versione draft al Mese 10]
- D2.4 - Modelli ed algoritmi per la gestione degli aspetti di privacy (Mese 15) [si prevede una versione draft al Mese 8]
- D2.5 - Modelli ed algoritmi per la gestione della fiducia in resti sociali e della credibilità dell'informazione (Mese 15) [si prevede una versione draft al Mese 8]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M2.1 - Analisi dei requisiti di affidabilità, sicurezza, fiducia e privacy completata (Mese 6)
- M2.2 - Prima versione dei modelli e delle soluzioi di affidabilità, sicurezza, fiducia e privacy completati (Mese 8)
- M2.3 - Prima versione dell'infarstruttura di gestione degli aspetti di affidabilità, sicurezza, fiducia e privacy completata (Mese 12)
- M2.4 - Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy completata (Mese 18)

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**
I deliverable precedentemente elencati sono i risultati delle attività secondo quanto di seguito specificato:
- D2.1 - Requisiti di affidabilità, sicurezza, fiducia e privacy per l'infrastruttura [Risultato dell'attività 2.1]
- D2.2 - Architettura della infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy [Risultato dell'attività 2.2]
- D2.3 - Realizzazione delle componenti della infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy [Risultato dell'attività 2.3]
- D2.4 - Modelli ed algoritmi per la gestione degli aspetti di privacy [Risultato dell'attività 2.4]
- D2.5 - Modelli ed algoritmi per la gestione della fiducia in resti sociali e della credibilità dell'informazione [Risultato dell'attività 2.5]

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**
Le milestone precedentemente elencate sono punti di verifica relative alle attività secondo quanto di seguito specificato:
- M2.1 - Analisi dei requisiti di affidabilità, sicurezza, fiducia e privacy completata [Risultato dell'attività 2.1]
- M2.2 - Prima versione dei modelli e delle soluzioni di affidabilità, sicurezza, fiducia e privacy completati [Risultato dell'attività 2.2]
- M2.3 - Prima versione dell'infrastruttura di gestione degli aspetti di affidabilità, sicurezza, fiducia e privacy completata [Risultato delle attività 2.3, 2.4, 2.5]

- M2.4 - Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy completata [Risultato delle attività 2.3, 2.4, 2.5]

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Obbiettivo operativo

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐

Costo toale dell'obbiettivo

Indicare il costo complessivo dell'obbiettivo Operativo

Costo totale dell'obbiettivo: 688.200,79

ATTIVITÀ N. 2.1

Denominazione: Analisi dei requisiti di affidabilità, sicurezza, fiducia e privacy dell'infrastruttura di raccolta dei dati e gestione dei dati e dei servizi disponibili

Descrizione singola attività
Scopo dell'attività è l'analisi dei requisiti di affidabilità, sicurezza, fiducia e privacy nelle varie componenti della infrastruttura. Per ogni fase della gestione dei dati, è necessario considerare una serie di requisiti di sicurezza. Ad esempio dovendo prevedere la possibilità di raccogliere informazioni da vari flussi di informazione, è doveroso assumere che non tutti siano sotto lo stesso dominio amministrativo e quindi è necessario considerare aspetti sia riguardanti l'interoperabilità' che la gestione della fiducia tra i vari fruitori ed i fornitori delle informazioni. Tra l'altro, per gli aspetti di affidabilità, si prevede anche l'uso di tecniche di analisi quali Hazard Analysis ed FMEA/FMECA (Failure Mode and Effects Analysis/Failure Mode and Effects and Criticality Analysis) al fine di identificare gli azzardi principali del sistema, le loro cause, e valutare possibili contromisure.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 16.9 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D2.1 - Requisiti di affidabilità, sicurezza, fiducia e privacy per l'infrastruttura (Mese 6) [si prevede una versione draft al Mese 3]
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M2.1 - Analisi dei requisiti di affidabilità, sicurezza, fiducia e privacy completata (Mese 6)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività
Costo totale dell'attività: 77.144,79

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

ATTIVITÀ N. 2.2

Denominazione: Definizione di soluzioni architetturali per i vari domini applicativi in esame, inclusi dispositivi mobili e di sensori/attuatori

Descrizione singola attività
Altra problematica significativa è lo studio di architetture che permettano una gestione sicura dei dati raccolti, la possibilità di elaborare questi dati in maniera confidenziale ed anche la gestione della distribuzione di tali informazioni a tutti gli utenti interessati in maniera appropriata e secondo specifiche regole di autorizzazione. Queste regole, da un lato devono essere precise, dall'altro sufficientemente flessibili per essere adottate anche in caso di emergenza (politiche tipo break-the-glass in cui si permette l'azione ma rimane traccia del fatto). In questo ambito di particolare interesse possono essere le problematiche riguardo l'uso di security patterns applicabili in vari contesti o ad esempio l'uso di modelli ed architetture data-centric per la gestione dei dati che permettano di default la loro protezione (e.g., sticky policies, encrypted containers), in quanto sono sempre cifrati tranne che durante l'uso in ambiente protetto.
A livello architetturale, per problematiche di affidabilità e sicurezza, si considerano anche soluzioni per il monitoring online ed in tempo reale dei servizi che fanno parte dell'architettura, al fine di identificare rapidamente possibili situazioni di degrado e fallimento. Tra i meccanismi di monitorig, considereremo anche meccanismi di self-stimulation, che permettano di interagire (stimolare) con i vari servizi presenti nel sistema al fine di facilitare la raccolta dei dati necessari agli strumenti di monitoring e di diagnosi dello stato del sistema e dei servizi.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 32.3 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D2.2 - Architettura della infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy (Mese 12) [si prevede una versione draft al Mese 8]
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M2.2 - Prima versione dei modelli e delle soluzioi di affidabilità, sicurezza, fiducia e privacy completati (Mese 8)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività
Costo totale dell'attività: 168.448,80

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

ATTIVITÀ N. 2.3

Denominazione: Strumenti e meccanismi per garantire aspetti di affidabilità, sicurezza fiducia e privacy per la rete di raccolta di informazioni per la infrastruttura di gestione dei dati e di decisione.

Descrizione singola attività
Scopo dell'attività è la progettazione di strumenti, meccanismi, algoritmi e protocolli per garantire tutti gli aspetti di sicurezza e di affidabilita' nelle varie componenti della infrastruttura e durante la varie fasi della gestione dei dati. Questo include anche la sicurezza delle comunicazioni (sia in fase di acquisizione di dati che di distribuzione). Di particolare interesse vi è la protezione del sistema decisionale (possibilmente distribuito). Le problematiche da considerare vanno dalla autenticazione alla autorizzazione ed accounting dei dati. Per citare tra i meccanismi di autenticazione, possiamo anche pensare meccanismi basati su biometria (nei casi in cui questa sia utile, per esempio per controllare il personale che gestisce i dati). Pensiamo infatti anche a quelli basati su soluzioni biometriche per la continuous authentication; l'idea alla base di tali meccanismi è acquisire tratti biometriche in modo continuo e trasparente all'utente, tramite i sensori disponibili sullo strumento usato per la connessione al sistema (ad esempio, tramite la webcam di un laptop), per confermare continuamente l'autenticità (ed i relativi privilegi) dell'utente. Di interesse vi e' anche la comunicazione sicura dei dati anche in contesti disruptive in cui i normali canali di comunicazione non

possono essere usati. Tra le componenti da sviluppare di particolare interesse sono quelli di monitoring della infrastruttura stessa di Secure!.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 60.4 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D2.3 - Realizzazione delle componenti della infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy (Mese 18) [si prevede una versione draft al Mese 10]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M2.3 - Prima versione dell'infarstruttura di gestione degli aspetti di affidabilità, sicurezza, fiducia e privacy completata (Mese 12)
- M2.4 - Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy completata (Mese 18)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 289.643,96

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

ATTIVITÀ N. 2.4

Denominazione: Modelli e algoritmi per la privacy dei dati, sia in fase di acquisizione che di gestione e diffusione.

Descrizione singola attività

Questa attività rende esplicito l'approccio del progetto di dare precedenza allo studio di architetture e soluzioni che adottino il principio di Privacy-by-Design (ovvero ognuna delle soluzioni architetturale dovrà avere la gestione della privacy come aspetto nativo). Dati i vari contesti applicativi, saranno studiati vari modelli ed algoritmi, partendo dalle problematiche di gestione dell'anonimato (anche durante la fase autenticazione ai servizi), alla gestione sicura dei dati disseminati, e gestione sicura delle decisioni e delle operazioni sui dati (spesso sotto controlli amministrativi diverse, magari tramite secure multi-party computation che stanno divenendo sempre più un meccanismo usabile in contesti applicativi). Per quanto riguarda le problematiche di gestione della privacy, queste dovranno essere mediate con quelle di autenticazione che si avranno per i servizi offerti dalla piattaforma Secure! Meccanismi basati su autenticazione forte (anche biometrica) possono essere modificati per migliorare il livello di privacy degli utenti (es. separazione della informazione sul template dall'identità utente).

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 17.7 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D2.4 - Modelli ed algoritmi per la gestione degli aspetti di privacy (Mese 15) [si prevede una versione draft al Mese 8]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M2.3 - Prima versione dell'infarstruttura di gestione degli aspetti di affidabilità, sicurezza, fiducia e privacy completata (Mese 12)
- M2.4 - Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy completata (Mese 18)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 74.796,84

Eventuale documentazione Aggiuntiva

Upload:	Nessun file Caricato
Upload:	Nessun file Caricato
Upload:	Nessun file Caricato

ATTIVITÀ N. 2.5

Denominazione: Modelli e algoritmi per la gestione di reti sociali autonome e della credibilità dell'informazione raccolta e diffusa.

Descrizione singola attività

Questa attività riguarda i modelli e gli algoritmi per la gestione della fiducia (trust) in comunità sociali e dinamiche (e.g., reti di utenti mobili) per rendere possibile l'acquisizione di dati ed in generale attività di calcolo da queste comunità. Importante sarà la possibilità di costruire in maniera dinamica e on-demand queste comunità per rispondere in maniera adeguata alle crisi che possono emergere, in un dato luogo in un dato momento. Anche in questo ambito gli aspetti di privacy avranno una notevole rilevanza. I modelli di trust e recommendation per studiare il livello di affidabilità e credibilità delle sorgenti informative e dei social media (users in social networks, devices, sensors, ecc.), che non potranno essere considerati come un'infrastruttura sempre disponibile ma potranno essere creati on-demand. Risulteranno anche utili e collegati, eventuali meccanismi di validazione delle informazioni al fine di decretare la fiducia disponibile in queste (soluzioni basate su information filtering e algoritmi di supporto alle decisioni) anche in relazione con altri obiettivi operativi. Per citare anche aspetti specifici di cui dovremo tener conto, consideriamo che in questa attività verranno studiati e implementati strumenti software di image forensics che consentano, principalmente, di analizzare i contenuti digitali (immagini/video) recuperati dalla piattaforma Secure! dal punto di vista della loro autenticità. Ciò permetterà, con una certa precisione , di scartare o di attribuire un peso minore a documenti digitali, relativi ad una certa situazione sotto analisi, che non siano ritenuti realistici ma bensì artefatti dall'utente, al fine di procurare allarme o indurre decisioni d'intervento non pertinenti.

Strumenti/attrezzature

Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane

Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 15.6 mesi uomo.

Subcontratti

Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività

Non prevista.

Risultati Attesi: deliverable e milestones

Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.

Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D2.5 - Modelli ed algoritmi per la gestione della fiducia in resti sociali e della credibilità dell'informazione (Mese 15) [si prevede una versione draft al Mese 8]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M2.3 - Prima versione dell'infarstruttura di gestione degli aspetti di affidabilità, sicurezza, fiducia e

privacy completata (Mese 12)
- M2.4 - Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy completata (Mese 18)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 78.166,40

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

OBIETTIVO OPERATIVO N. 3

Denominazione: Tecniche e componenti innovative di Crowd-sensing

Descrizione dell'obbiettivo operativo

Scopo dell'obbiettivo è lo studio delle tecniche di crowd-sensing e crowd-sourcing e del loro utilizzo all'interno della piattaforma Secure!.
Gli strumenti di nuova generazione che sono messi a disposizione consentono di vedere la comunità degli utenti sotto una diversa prospettiva, in particolare considerando gli utenti stessi come una sorta di "sensori" (paradigma citizens-as-sensors), che rilevano e condividono eventi, esprimono sensazioni e giudizi, producendo informazioni di diversa tipologia, utili alla gestione di particolari situazioni.
I social network sono un canale di comunicazione di grande rilevanza, che si caratterizza per la varietà dell'informazione che ospita e per la velocità con cui questa si diffonde, a volte, persino anticipando canali più tradizionali come la agenzie di stampa. Questo obiettivo operativo studierà nuove metodologie per l'analisi delle informazioni presenti nei social media. In particolare si prenderanno in considerazione sia informazioni di tipo testuale che di tipo visuale (immagini e filmati) pubblicate dagli utenti. Saranno inoltre progettati strumenti utili a identificare, tramite l'analisi di testo e immagini, la presenza di informazioni relative a situazioni di emergenza o argomenti di interesse.
Tali situazioni saranno descritte e ricostruite attraverso un insieme significativo di informazioni "utili" estratte opportunamente da un set (eventualmente voluminoso) di dati "rilevanti" raccolti dalle varie sorgenti considerate nel progetto (si veda flusso informativo riportato e descritto nella sezione relativa all'obiettivo generale del progetto).

Risultati Attesi: deliverable e milestones

Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito del presente obiettivo operativo, sono previsti i seguenti risultati misurabili e verificabili (deliverable):
- D3.1 - Rapporto di ricerca sulle tecniche di crowd-sensing e crowd-sourcing (Mese 3) (Mese 3)
- D3.2 - Rapporto di ricerca sulle tecniche e servizi per la raccolta dati (Mese 12); si prevede una prima versione del D3.2 al Mese 6. (Mese 12) [si prevede una versione draft al Mese 6]
- D3.3 - Rapporto di ricerca sulle tecniche, e componenti sw per l'estrazione di informazioni e modalità di integrazione. (Mese 15); si prevede una prima versione del D3.3 al Mese 9. (Mese 15) [si prevede una versione draft al Mese 9]
- D3.4 - Rapporto tecnico sulle modalità di integrazione dell'informazione. (Mese 15);); si prevede una prima versione del D3.4 al Mese 9. (Mese 15) [si prevede una versione draft al Mese 9]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M3.1 - Analisi dello stato dell'arte sul crowdsourcing completata (Mese 3)

- M3.2 - Definita la versione delle tecniche e servizi di raccolta dati dalle diverse sorgenti considerate nel progetto (Mese 6)
- M3.3 - Definita la prima versione delle tecniche di estrazione e correlazione di informazioni per l'individuazione degli eventi (Mese 10)
- - M3.4 - Tecniche e servizi di crowd-sensing completati (Mese 15)

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**
I deliverable precedentemente elencati sono i risultati delle attività secondo quanto di seguito specificato:
- D3.1 - Rapporto di ricerca sulle tecniche di crowd-sensing e crowd-sourcing (Mese 3) [Risultato dell'attività 3.1]
- D3.2 - Rapporto di ricerca sulle tecniche e servizi per la raccolta dati (Mese 12); si prevede una prima versione del D3.2 al Mese 6. [Risultato dell'attività 3.2]
- D3.3 - Rapporto di ricerca sulle tecniche e servizi per l'estrazione di informazioni e modalità di integrazione. (Mese 15); si prevede una prima versione del D3.3 al Mese 9. [Risultato dell'attività 3.3]
- - D3.4 - Rapporto tecnico sulle modalità di integrazione dell'informazione. (Mese 15);); si prevede una prima versione del D3.4 al Mese 9. [Risultato dell'attività 3.4]

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**
Le milestone precedentemente elencate sono punti di verifica relative alle attività secondo quanto di seguito specificato:
- M3.1 - Analisi dello stato dell'arte sul crowdsourcing completata [Risultato dell'attività 3.1]
- M3.2 - Definita la versione delle tecniche e servizi di raccolta dati dalle diverse sorgenti considerate nel progetto [Risultato dell'attività 3.2]
- M3.3 - Definita la prima versione delle tecniche di estrazione e correlazione di informazioni per l'individuazione degli eventi [Risultato dell'attività 3.3]
- M3.4 - Tecniche e servizi di crowd-sensing completati [Risultato delle attività 3.3, 3.4]

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Obbiettivo operativo

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo toale dell'obbiettivo

Indicare il costo complessivo dell'obbiettivo Operativo

Costo totale dell'obbiettivo: 1.479.087,45

ATTIVITÀ N. 3.1

Denominazione: Analisi tecniche crowd-sensing e crowd-sourcing

Descrizione singola attività
In questa attività si prevede uno studio sullo stato corrente delle tecniche di crowd-sensing e crowd-sourcing.
Gli utenti umani che utilizzano dei dispositivi fissi (PC, smart-tv) o mobili (smartphone, tablet, laptop) sono considerati alla stregua di sensori (paradigma citizens-as-sensors) nella produzione di dati informativi connessi ad un certo evento; gli stessi utenti possono essere anche coinvolti nei processi di analisi di una situazione richiedendo loro valutazioni, dati aggiuntivi e specifici e così via.

In questo senso verranno studiate ed analizzate le problematiche relative all'adozione dei sensori umani, in relazione ed in contrapposizione ai sensori fisici ed alle reti di sensori, con riferimento soprattutto all'applicazione delle suddette tecniche nello specifico settore della gestione delle situazioni di emergenza, della sicurezza pubblica, della protezione civile e delle infrastrutture. Le problematiche si riferiscono agli aspetti scientifico-tecnologici (le tecniche di raccolta dati, le tecniche di estrazione e correlazione degli stessi, ecc.), agli aspetti motivazionali (perché gli utenti dovrebbero fornire informazioni), agli aspetti culturali (in particolare il concetto di crowdsourcing impiegato per attività di tipo civico e/o sociale).
In questa attività sarà analizzato la letteratura relativa ai suddetti aspetti, i progetti sviluppati negli ultimi anni, i sistemi e le applicazioni reali di crowdsourcing in scenari e contesti prossimi a quelli del progetto, le soluzioni open source disponibili per la raccolta, estrazione, integrazione e correlazione di informazioni provenienti dai social media.
Infine in questa attività, verrà studiato lo stato dell'arte dei meccanismi di interoperabilità ed integrazione di reti di sensori (es. OGC Sensor Web Enablement, ecc.).

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 63.6mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D3.1 - Rapporto di ricerca sulle tecniche di crowd-sensing e crowd-sourcing (Mese 3)
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M3.1 - Analisi dello stato dell'arte sul crowdsourcing completata (Mese 3)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 242.458,84

Eventuale documentazione Aggiuntiva

Upload:	Nessun file Caricato
Upload:	Nessun file Caricato
Upload:	Nessun file Caricato

ATTIVITÀ N. 3.2

Denominazione: Definizione di tecniche e servizi per la raccolta dati

Descrizione singola attività

Scopo dell'attività è l'analisi delle varie modalità (canali) da cui raccogliere dati "rilevanti" mediante i sensori-umani della comunità e tutte le altre sorgenti di dati considerate nel progetto (social media, reti di sensori, sistemi informativi esistenti, applicazioni mobile per servizi specifici). L'interazione può provenire attraverso reti di telefonia mobile (UMTS, EDGE), Internet (wired e/o wireless), il GPS, la piattaforma tv digitale terrestre tramite il canale di ritorno dei decoder interattivi. Per ottenere elementi informativi che siano comprensibili e utili, è necessario uniformare questo insieme di dati, al fine di consentire una successiva estrazione delle informazioni di pertinenza (si veda l'Attività 3.3). Nello specifico, si analizzeranno un insieme di componenti e servizi, per il monitoraggio dei diversi canali da cui le informazioni possono pervenire alla piattaforma Secure!. Molteplici sono infatti le modalità con cui gli utenti possono interagire; essi potranno essere parte di una certa infrastruttura di controllo (utenti sottoscrittori) oppure potranno essere utenti generici che distribuiscono informazioni generiche relative ad un certo evento. In questa attività verrà anche definita e realizzata un'infrastruttura per la raccolta di dati ed informazioni attraverso dispositivi mobili personali e verranno studiate anche le modalità di integrazione di reti di sensori (SN) utilizzando standard e tecnologie allo stato dell'arte. Sarà presa anche in considerazione la piattaforma della tv digitale terrestre, attraverso cui un telespettatore può fornire informazioni specifiche interagendo con un'applicazione interattiva (MHP) di servizio trasmessa in broadcast.
All'interno di queste attività verranno inoltre progettate metodologie per la raccolta di contenuti testuali e delle relazioni fra gli utenti di social network. Si svilupperanno anche strumenti per una raccolta dati focalizzata in una specifica area geografica.

Strumenti/attrezzature

Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane

Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 49.5mesi uomo.

Subcontratti

Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività

Non prevista.

Risultati Attesi: deliverable e milestones

Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.

Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D3.2 - Rapporto di ricerca sulle tecniche e servizi per la raccolta dati (Mese 12); si prevede una prima versione del D3.2 al Mese 6. (Mese 12) [si prevede una versione draft al Mese 6]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:

- M3.2 - Definita la versione delle tecniche e servizi di raccolta dati dalle diverse sorgenti considerate nel progetto (Mese 6)
- M3.4 - Tecniche e componenti di crowd-sensing completati (Mese 15)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 232.039,40

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

ATTIVITÀ N. 3.3

Denominazione: Definizione di tecniche e servizi per l'estrazione di informazioni rilevanti da sorgenti multimodali

Descrizione singola attività

Una volta che i dati sono stati reperiti (es. un tweet, un blog, un post su un forum, un insieme di dati sensoriali, dati da un sistema esterno, ecc.), è necessario operare su di essi, in modo da estrarne informazioni "utili" e di confrontarle, correlarle, connotarle nello spazio e nel tempo, ed eventualmente validarle.
Questa attività prevederà l'uso di tecniche di pattern recognition, di analisi testo, audio, video e immagini, di tecniche di classificazione e fusione tra diversi sensori o diversi nodi della comunità, tecniche di image forensics per la valutazione dell'autenticità di immagini digitali e così via.
Da queste tecniche ne deriveranno alcune componenti e servizi (da integrare nel Secure! Framework) che in maniera automatica permetteranno di estrarre informazioni utili per la ricostruzione degli eventi.
Un esempio dell'analisi testuale riguarderà lo studio dei tweet. Il testo dei commenti o dei "post" presenti in una social network sono in genere molto brevi e usano un linguaggio informale ed una sintassi peculiare, come ad esempio gli hashtag di Twitter, e per questo richiedono una fase di analisi specifica. In questa attività si progetteranno le metodologie per estrapolare da brevi contenuti testuali una descrizione di livello più alto che permetta di individuare concetti e luoghi, associando termini presenti nel testo in esame a entità presenti in basi di dati esterne come Wikipedia o Freebase.
L'analisi di queste informazioni di più alto livello permette di aumentare la comprensione dei contenuti raccolti da social network e di aggregare questi "segnali" provenienti da sorgenti diverse anche se sono espressi sintatticamente in maniera diversa.
In questa attività si realizzeranno inoltre strumenti per analizzare i contenuti visuali provenienti da sorgenti diverse con lo scopo di mettere in relazione contenuti equivalenti o relativi alla stessa situazione, argomento, o oggetto di interesse. Questi strumenti si baseranno su tecniche di analisi, matching, e riconoscimento automatico del contenuto visuale. Verrà prestata particolare attenzione alle problematiche di accuratezza nella produzione dei risultati, nonché all'efficienza e scalabilità del sistema.
Oltre a ciò verranno studiati e sviluppati strumenti di image forensics per la validazione delle immagini raccolte al fine di comprendere la veridicità dei dati di cui si è in possesso evidenziando tentativi di falso allarme innescati da fotomontaggi e fotoritocchi.

Strumenti/attrezzature

Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 156.7mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D3.3 - Rapporto di ricerca sulle tecniche, e componenti sw, per l'estrazione di informazioni e modalità di integrazione. (Mese 15); si prevede una prima versione del D3.3 al Mese 9. (Mese 15) [si prevede una versione draft al Mese 9]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M3.3 - Definita la prima versione delle tecniche di estrazione e correlazione di informazioni per l'individuazione degli eventi (Mese 9)
- M3.4 - Tecniche e componnti di crowd-sensing completati (Mese 15)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 577.997,23

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

ATTIVITÀ N. 3.4

Denominazione: Preparazione delle informazioni per la successiva fase di decisioning/ acting

Descrizione singola attività
Al fine di rendere utili i dati elaborati nell'Attività 3.3, è necessario prevedere delle funzionalità in grado di integrare, correlare, in maniera efficace ed efficiente, informazioni generate relative alle stesse entità o evento (es. una o più segnalazioni mediante tweet di danneggiamento di uno specifico monumento, da integrare e fondere con una foto inviata da uno o più passanti).
In pratica, l'obiettivo di questa attività è quello di studiare e mettere a punto tecniche e servizi di

integrazione e correlazione di informazioni (estratte mediante le componenti risultanti dall'attività 3.3), al fine di determinare una immagine informativa complessiva di un determinato "evento", un accadimento, qualcosa che è successo.
Le tecniche da studiare saranno basate su principi di aggregazione, clustering, machine learning, correlazione semantica, ecc. Da queste ne deriveranno alcune componenti e servizi (da integrare nel Secure! Framework) che in maniera automatica e/o semi-automatica permetteranno di ricostruire l'identità e le caratteristiche degli eventi riconosciuti.
Questi dati strutturati costituiranno la base su cui implementare i meccanismi decisionali e di valutazione propri dell'OO4. Infatti gli eventi saranno poi successivamente aggregati e determineranno la situational awareness, che a sua volta rappresenterà la base delle decisioni e delle azioni da perseguire.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 96.9 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D3.4 - Rapporto di ricerca sulle modalità di integrazione dell'informazione. (Mese 15);); si prevede una prima versione del D3.4 al Mese 9. (Mese 15) [si prevede una versione draft al Mese 9]
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M3.4 - Tecniche e componenti di crowd-sensing completati (Mese 15)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 426.591,98

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

ATTIVITÀ N. 3.5

Denominazione:

Descrizione singola attività

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività:

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

OBIETTIVO OPERATIVO N. 4

Denominazione: Tecniche e componenti innovative per il supporto decisionale

Descrizione dell'obbiettivo operativo
L'obiettivo 4 si propone di investigare, progettare ed implementare il sistema di gestione delle azioni e di supporto decisionale (Decisional Support System, DSS) richiesto nell'ambito del progetto Secure!. Tale supporto decisionale riceve come input l'ingente mole di informazioni "utili" estratte, analizzate e generate dai servizi risultanti dall'Obiettivo Operativo 3, al fine di estrarne le decisioni e le informazioni di interesse da rendere disponibili. Tali informazioni possono essere sia informazioni per il personale addetto all'utilizzo del sistema Secure! (attraverso le applicazioni Secure! Situation-awareness e Secure! Analytics), sia decisioni/operazioni da inviare direttamente agli utenti del sistema (attraverso le Secure! Crowdsourcing Apps), sia attraverso l'invio a sistemi esistenti di gestione della sicurezza pubblica e protezione civile, eventualmente integrabili in istanze specifiche del framework Secure!.
Nell'ambito di questo obiettivo operativo, verrà sperimentato un nuovo modello iterativo di gestione delle situazioni di emergenza basato prevalentemente sulla generazione in continuo degli eventi in tempo reale e sulla conseguente rappresentazione della situazione attuale in modo tale da poter gestire le evoluzioni e i cambiamenti del contesto di riferimento e suggerire l'azione ritenuta più

idonea e in linea con gli obiettivi generali del sistema.
Si valuterà, inoltre, l'utilizzo di canali di comunicazione non tradizionali (social media) e di "sensori umani" per realizzare un Early Warning System altamente economico, efficace, scalabile e indipendente dal dominio.
Dati gli obiettivi previsti nell'ambito di Secure!, il sistema DSS dovrà soddisfare i seguenti requisiti:
- elevata integrabilità, scalabilità e componibilità dei servizi decisionali, per permettere di integrare nuovi e differenti servizi, effettuare con efficienza operazioni di manutenzione, e garantire l'evoluzione nel tempo della piattaforma Secure! e la flessibilità dell'architettura a differenti contesti applicativi. Per soddisfare tali requisiti, l'architettura del sistema decisionale, ereditandone le caratteristiche dall'architettura dell'intero framework Secure!, si baserà su una soluzione Service-Oriented Architecture (SOA; è un paradigma architetturale largamente utilizzato come infrastruttura software di molti sistemi moderni, che tramite la composizione e l'interazione dinamica di svariati servizi fornisce proprietà di riutilizzo, adattabilità, interoperabilità, e flessibilità).
- stringenti vincoli temporali per decisioni richieste in situazioni di emergenza, elevata disponibilità e prestazioni del sistema decisionale. L'obiettivo è garantire disponibilità e prestazioni, ed ottimizzare i processi decisionali, adattando dinamicamente a seconda delle situazioni la priorità delle attività svolte e l'ordine delle richieste processate dal sistema.
- elevata sicurezza del sistema, sia ai fini della tutela di eventuali dati sensibili (informazioni private degli utenti acquisite e utilizzate nel processo decisionale), sia per la protezione stessa del sistema decisionale e dei suoi risultati, al fine di evitare che eventuali malintenzionati possano manipolare e facilmente riusare a loro vantaggio. Si noti che questo richiede di garantire protezione non solo verso l'esterno (attaccanti con accesso non autorizzato al sistema), ma anche verso l'interno, cioè dal personale addetto, quindi con possibilità di accesso legittimo al sistema, che utilizza il sistema in modo malevolo.
- Elevata confidenza delle decisioni. Il sistema decisionale Secure! dovrà essere estremamente accurato, sia per evitare di scartare potenziali situazioni di emergenze o allarme, sia per minimizzare il numero di falsi allarmi o di segnalazioni errate. Questo requisito è vitale per l'applicabilità stessa del sistema Secure!, in quanto da questo dipende in modo significativo la fiducia riposta nel sistema dall'utente e dal personale addetto.
Infine il sistema di supporto decisionale includerà un insieme di servizi per l'analisi off-line di tutte le informazioni gestite dalla piattaforma Secure!, al fine di determinare possibili azioni di miglioramento e di fine-tuning delle performance della piattaforma stessa.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito del presente obiettivo operativo, sono previsti i seguenti risultati misurabili e verificabili (deliverable):
- D4.1 - Modelli di gestione dei contenuti e delle decisioni (Mese 12) [si prevede una versione draft al Mese 9]
- D4.2 - Tecniche e servizi di elaborazione ed analisi in tempo reale (situation awareness) (Mese 18) [si prevede una versione draft al Mese 10]
- D4.3 - Servizi e meccanismi decisionali (Mese 18) [si prevede una versione draft al Mese 12]
- D4.4 - Tecniche e servizi per l'analisi off-line (Secure! Analytics) (Mese 18) [si prevede una versione draft al Mese 12]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M4.1 - Prima versione delle tecniche e delle componenti di supporto decisionale completati (Mese 12)
- M4.2 - Tecniche e componenti innovative per il supporto decisionale completati (Mese 18)

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**
I deliverable precedentemente elencati sono i risultati delle attività secondo quanto di seguito specificato:
- D4.1 - Modelli di gestione dei contenuti e delle decisioni [Risultato dell'attività 4.1]
- D4.2 - Tecniche e servizi di elaborazione ed analisi in tempo reale (situation awareness) [Risultato dell'attività 4.2]
- D4.3 - Servizi e meccanismi decisionali [Risultato dell'attività 4.3]
- D4.4 - Tecniche e servizi per l'analisi off-line (Secure! Analytics) [Risultato dell'attività 4.4]

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**
Le milestone precedentemente elencate sono punti di verifica relative alle attività secondo quanto di seguito specificato:

- M4.1 - Prima versione delle tecniche e delle componenti di supproto decisionale completati [Risultato delle attività 4.1, 4.2, 4.3, 4.4]
- M4.2 - Tecniche e componenti innovative per il supporto decisionale completati [Risultato delle attività 4.1, 4.2, 4.3, 4.4]

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Obbiettivo operativo

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐

Costo toale dell'obbiettivo

Indicare il costo complessivo dell'obbiettivo Operativo

Costo totale dell'obbiettivo: 962.006,99

ATTIVITÀ N. 4.1

Denominazione: Definizione di modelli di gestione dei contenuti e delle decisioni

Descrizione singola attività
Questa attività mira a definire e costruire il modello informativo di gestione dei contenuti (informazioni utili, eventi, situazioni) e delle decisioni supportato dalla piattaforma Secure!. Saranno anche realizzati servizi per la classificazione e l'organizzazione delle suddette informazioni da fornire come input ai servizi decisionali descritti nelle Attività 4.2, Attività 4.3 e Attività 4.4.. In questa attività verranno studiate ed analizzate le modalità ed i modelli per integrare informazioni geo-spaziali al fine da arricchire le suddette informazioni gestite dalla piattaforma Secure! ed ad organizzarle su mappe tematiche.
Sarà, inoltre, realizzato un nuovo strumento che consentirà agli operatori coinvolti nel processo di gestione della crisi di sfruttare le potenzialità del crowdsorcing e delle informazioni georeferenziate prodotte (crowd-mapping) per incentivare la partecipazione sociale in modo solidale ma controllato. Nel sistema decisionale previsto in Secure! si dovranno applicare inoltre soluzioni per la gestione sia di dati personali che dati assolutamente anonimi e generici. Si pone quindi l'obiettivo di "nascondere" informazioni non necessarie al personale addetto al sistema decisionale, al fine di evitare che utenti con accesso al sistema ma malintenzionati possano entrare in possesso di dati sensibili in modo illegittimo. A tal fine si prevede la definizione di meccanismi di protezione delle informazioni decisionali, volti a nascondere le informazioni non necessarie (ad esempio, dati personali che non è necessario mostrare) al personale addetto. Questi meccanismi applicheranno continui controlli sulle operazioni (query) effettuate dal personale addetto, al fine di identificare attività di acquisizione informazioni potenzialmente malevole dovute a personale addetto che sta utilizzando il sistema in modo non legittimo.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 42.8 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D4.1 - Modelli di gestione dei contenuti e delle decisioni (Mese 12) [si prevede una versione draft al Mese 9]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M4.1 - Prima versione delle tecniche e delle componenti di supporto decisionale completati (Mese 12)
- M4.2 - Tecniche e componenti innovative per il supporto decisionale completati (Mese 18)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività
Costo totale dell'attività: 251.208,26

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

ATTIVITÀ N. 4.2

Denominazione: Definizione ed implementazione di tecniche e servizi di elaborazione ed analisi in tempo reale (situation awareness)

Descrizione singola attività
Obiettivo di questa attività è definire, implementare ed integrare nel DSS un set di servizi per l'elaborazione, trasformazione, fusione e distribuzione di informazioni relative agli eventi riconosciuti (risultanti dai servizi realizzati nell'OO3) al fine di produrre un'immagine informativa integrata della situazione di pericolo o emergenza da considerare e gestire, ossia la cosiddetta situation awareness.
Si rende necessaria la definizione ed implementazione di servizi che offrano:
- pattern per l'elaborazione (aggregazione, trasformazione, correlazione e fusione) di informazioni eterogenee e per la loro integrazione, in modo che siano facilmente gestibili dai servizi dell'Attività 4.3 e dell'Attività 4.4.
- soluzioni algoritmiche orientate alla identificazione di anomalie (cioè deviazioni dal comportamento normale imputabili a fattori non casuali) basate sia sullo studio statistico (storico) dei dati, che sulla loro analisi semantica. Queste soluzioni permettono al sistema Secure! di effettuare un filtraggio sui dati al fine di selezionare quelli da sottoporre con particolare urgenza all'attenzione dei meccanismi decisionali (Attività 4.3), definendo cosi delle priorità nell'analisi.
Questa attività di filtraggio deve anche permettere di identificare e scartare informazioni inconsistenti

o fuorvianti, che possono generare falsi allarmi, così come deve permettere di identificare e isolare le sorgenti che li hanno generati (ad esempio, permettere di mantenere e aggiornare una blacklist di utenti che forniscono con continuità informazioni fasulle). In tal modo, le attività di filtraggio permettono di ridurre la mole di dati posta all'attenzione del meccanismo decisionale.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 31.24 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D4.2 - Tecniche e servizi di elaborazione ed analisi in tempo reale (situation awareness) (Mese 18) [si prevede una versione draft al Mese 10]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M4.1 - Prima versione delle tecniche e delle componenti di supporto decisionale completati (Mese 12)
- M4.2 - Tecniche e componenti innovative per il supporto decisionale completati (Mese 18)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 156.062,81

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

ATTIVITÀ N. 4.3

Denominazione: Definizione ed implementazione di servizi e meccanismi decisionali

Descrizione singola attività

Il DSS previsto in Secure! richiede di analizzare i dati in maniera semi-automatica, interpretando il valore semantico di dati, definendo correlazioni tra dati provenienti da fonti diverse. Obiettivo di questa attività è definire, implementare ed integrare nel DSS servizi per effettuare la decisione da presentare all'utente o al personale addetto. Si considerano quindi soluzioni basate su machine learning e meccanismi e sistemi di ragionamento pratico per dedurre conclusioni (decisioni) tramite l'analisi delle informazioni. A tutto questo si aggiunge la necessità sia di effettuare decisioni corrette, che di porre evidenza della confidenza nella decisione presa. Queste caratteristiche sono necessarie per la reale applicabilità del progetto Secure!, in quanto influenzano in modo cruciale la fiducia dell'utente del sistema Secure! e del personale addetto.
Addizionalmente, si prevede la definizione di soluzioni per la distribuzione agli utenti ed altri sistemi collegati delle informazioni così sintetizzate con politiche di publish/subscribe o alternative e con attenzione ai livelli di privacy e riservatezza opportuni.
I servizi risultanti da questa attività saranno definiti e realizzati sfruttando le capacità offerte dal framework PRACTIONIST (www.practionist.org), realizzato da ENGINEERING, per lo sviluppo di sistemi intelligenti distribuiti basati sul ragionamento pratico (orientato all'azione).
Da ultimo, si svilupperà inoltre in questa attività un approccio sul dominio della cyber-security, con tecniche di machine learning e clustering per lo sviluppo di strumenti per intrusion detection, applicabile anche per dispositivi mobili. Sarà anche importante lo studio di modelli espressivi e strumenti per fare threat analysis (analisi delle minacce) per le infrastrutture definite nel progetto Secure!. L'obiettivo è definire modelli formali per studiare i possibili attacchi e le possibili contromisure in maniera dinamica e basata su varie metriche di sicurezza. A tal fine si useranno logiche (quali DATALOG) e meccanismi con soft-constraints (basati su semirings) per ottimizzare l'uso delle risorse necessarie per proteggere i sistemi

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 41.1 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D4.3 - Servizi e meccanismi decisionali (Mese 18) [si prevede una versione draft al Mese 12]
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M4.1 - Prima versione delle tecniche e delle componenti di supporto decisionale completati (Mese 12)
- M4.2 - Tecniche e componenti innovative per il supporto decisionale completati (Mese 18)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 236.576,19

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

ATTIVITÀ N. 4.4

Denominazione: Definizione ed implementazione di tecniche e servizi per l'analisi off-line (Secure! Analytics)

Descrizione singola attività

In questa attività verranno definiti ed implementati alcuni servizi per l'analisi off-line (post-emergenza) delle informazioni gestite dalla piattaforma Secure!, al fine di esaminare l'efficienza delle decisioni, degli interventi e delle azioni determinate in risposta a specifiche situazioni di emergenza e con l'idea di poter migliorare attraverso il fine-tuning dei servizi di analisi in tempo reale.

Tali servizi di analytics includeranno funzionalità di reporting, di analisi dei flussi informative e dei gruppi di persone coinvolte nelle situazioni di emergenza, analisi dei trend relativi agli utenti (in termini di trust, affidabilità, partecipazione, ecc.), di analisi what-if e di simulazione, di analisi dei sentimenti delle persone coinvolte nelle suddette situazioni.

Verranno pertanto studiate ed applicate tecniche di social network analysis, di data mining, di text mining, di clustering, ecc., con la possibilità di rilasciare il vincolo sul tempo, potendo così analizzare più in profondità le informazioni gestite.

Strumenti/attrezzature

Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Non è prevista l'acquisizione di strumenti e attrezzature specifiche.

Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane

Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.

I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.

Questa stima è pari a circa 56.1 mesi uomo.

Subcontratti

Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività

Non prevista.

Risultati Attesi: deliverable e milestones

Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.

Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):

- D4.4 - Tecniche e servizi per l'analisi off-line (Secure! Analytics) (Mese 18) [si prevede una versione draft al Mese 12]

Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:

- M4.1 - Prima versione delle tecniche e delle componenti di supporto decisionale completati (Mese 12)

- M4.2 - Tecniche e componenti innovative per il supporto decisionale completati (Mese 18)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 318.159,73

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

ATTIVITÀ N. 4.5

Denominazione:

Descrizione singola attività

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività:

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

OBIETTIVO OPERATIVO N. 5

Denominazione: Applicazione e validazione in contesti reali

Descrizione dell'obbiettivo operativo

Questo obiettivo operativo ha due scopi principali:
a) da una parte la sperimentazione dei risultati di ricerca del progetto attraverso l'implementazione di due piloti nell'ambito della tematica della gestione delle emergenze. Il primo pilota sperimenterà le tecnologie di Secure! per la sicurezza e protezione del territorio implementando uno caso d'uso specifico per la protezione e tutela delle risorse culturali della città di Firenze. Il secondo pilota verrà implementato per la protezione e tutela dei dati nel flusso di informazioni industriali e di business per garantire la sicurezza e dati e proteggere le infrastrutture informatiche da potenziali attacchi. La scelta di sperimentare i risultati di Secure! in due domini completamente diversi ha lo scopo di dimostrare la replicabilità del sistema in diversi domini. Il sistema avrà la possibilità di essere utilizzato in tutte le situazioni di emergenza e personalizzato a secondo del dominio applicativo (Attività 5.1, 5.2, 5.3).
b) dall'altra la creazione di un forte impatto sul territorio mettendo in campo una forte strategia di distribuzione dei risultati scientifici e operativi attraverso l'utilizzo di strumenti di comunicazione multicanali. In quest'ottica saranno organizzati specifici eventi in collaborazione con la Regione Toscana per i potenziali clienti di sistemi realizzati secondo l'approccio ed adottando il framework Secure! Questa attività servirà ad attrarre una massa critica di potenziali utenti e clienti del sistema auspicando ad un vasto utilizzo Secure! in diverse domini e specificità. Gli strumenti e le metodologie adottate verranno descritte nell'attività 5.4. Inoltre verrà definito un modello di business che dimostrerà la sostenibilità dei risultati del progetto dopo la sua conclusione.

Risultati Attesi: deliverable e milestones

Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.

Nell'ambito del presente obiettivo operativo, sono previsti i seguenti risultati misurabili e verificabili (deliverable):
- D5.1 - Specifica degli scenari applicativi del dimostratore e piano di sperimentazione (Mese 12) [si prevede una versione draft al Mese 9]
- D5.2 - Primo versione del dimostratore (Mese 15)
- D5.3 - Dimostratore finale (Mese 21)
- D5.4 - Validazione analitica e simulativa del sistema Secure! (Mese 18)
- D5.5 - Validazione sperimentale (testing) (Mese 24)
- D5.6 - Report delle attività e risultati della comunicazione (Mese 24)
- D5.7 - Modelli e piano di Business (Mese 24)
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M5.1 - Piloti per la sperimentazione completamente definiti e pianificati (Mese 12)
- M5.2 - Prima versione dei dimostratori pronti per la validazione (Mese 15)
- M5.3 - Test e validazione primo dimostratore completati (Mese 18)
- M5.4 - Dimostratore finale pronto per la validazione (Mese 21)

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**

I deliverable precedentemente elencati sono i risultati delle attività secondo quanto di seguito specificato:
- D5.1 - Specifica degli scenari applicativi del dimostratore e piano di sperimentazione [Risultato dell'attività 5.1]
- D5.2 - Primo versione del dimostratore [Risultato dell'attività 5.2]
- D5.3 - Dimostratore finale [Risultato dell'attività 5.2]
- D5.4 - Validazione analitica e simulativa del sistema Secure! [Risultato dell'attività 5.3]
- D5.5 - Validazione sperimentale (testing) [Risultato dell'attività 5.3]
- D5.6 - Report delle attività e risultati della comunicazione [Risultato dell'attività 5.4]
- D5.7 - Modelli e piano di Business [Risultato dell'attività 5.4]

☑ **nel corso dell'obiettivo è prevista l'elaborazione di specifici risultati misurabili e verificabili (deliverable). In caso positivo indicare in quale attività**

Le milestone precedentemente elencate sono punti di verifica relative alle attività secondo quanto di seguito specificato:
- M5.1 - Piloti per la sperimentazione completamente definiti e pianificati [Risultato dell'attività 5.1]

- M5.2 - Prima versione dei dimostratori pronti per la validazione [Risultato dell'attività 5.2]
- M5.3 - Test e validazione primo dimostratore completati [Risultato dell'attività 5.3]
- M5.4 - Dimostratore finale pronto per la validazione [Risultato dell'attività 5.2]

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Obbiettivo operativo

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Costo toale dell'obbiettivo

Indicare il costo complessivo dell'obbiettivo Operativo

Costo totale dell'obbiettivo: 1.371.700,14

ATTIVITÀ N. 5.1

Denominazione: Definizione e pianificazione dei piloti per la sperimentazione

Descrizione singola attività
In questa attività verranno definiti in dettaglio i piloti su cui effettuare la sperimentazione dei risultati del progetto e verranno pianificate le azioni da svolgere per l'attuazione della sperimentazione stessa. Pertanto, saranno ulteriormente elaborati i requisiti ed i casi d'uso specificati nell'attività 1.1, producendone una estensione più dettagliata e specifica per i piloti considerati: questo comporterà una definizione più precisa degli attori e della descrizione degli stessi casi d'uso; richiederà anche una specializzazione dei goal del sistema da realizzare sulla base del Secure! Framework ed un'identificazione più precisa dei sistemi esterni e già esistenti da integrare e dei relativi meccanismi di interoperabilità richiesti; sarà selezionato un insieme di social media da considerare per la sperimentazioni di ogni singolo pilota; saranno altresì definite nel dettaglio le applicazioni ed servizi specifici da implementare per i settori specifici dei piloti considerati ed i relativi casi d'uso da dimostrare.
In questa attività verrà anche predisposto un piano di sperimentazione, che include azioni che vanno dalla preparazione dei piloti, al coinvolgimento degli utenti, alla definizione delle modalità di sperimentazione e di valutazione, alla definizione di una metodologia di raccolta ed analisi dei dati della sperimentazione al fine di misurare le performance ed il valore aggiunto della soluzione proposta nel progetto, fino ad arrivare alla predisposizione dei passi da svolgere durante la sperimentazione vera e propria.
Infine, alcune azioni preparatorie per la sperimentazione (coinvolgimento degli utenti, alimentazione delle basi di dati e di conoscenza, creazione e gestione utenti, ecc.) verranno svolte come parte di questa attività.
Il risultato di questa attività sarà un documento che descrive i piloti, secondo le modalità suddette, ed il piano di sperimentazione e validazione.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 31.4 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D5.1 - Specifica degli scenari applicativi del dimostratore e piano di sperimentazione (Mese 12) [si prevede una versione draft al Mese 9]
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M5.1 - Piloti per la sperimentazione completamente definiti e pianificati (Mese 12)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività
Costo totale dell'attività: 171.241,42

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

ATTIVITÀ N. 5.2

Denominazione: Sviluppo applicazioni specifiche per i piloti

Descrizione singola attività
In questa attività verranno progettate e realizzate le applicazioni ed i servizi specifici definiti nell'attività 5.1. per i settori specifici dei piloti considerati ed i relativi casi d'uso da dimostrare.
In particolare verranno specializzate le applicazione o i semilavorati di applicazione già fornite nel Secure! Framework e verranno realizzate nuove applicazioni specifiche per gli scenari da dimostrare.
Come parte di questa attività, verrà effettuate anche il test e la validazione delle singole applicazioni, che poi verranno ulteriormente validate nel contesto del sistema integrato nell'ambito dell'attività 5.3.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane

Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 111.6 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D5.2 - Primo versione del dimostratore (Mese 15)
- D5.3 - Dimostratore finale (Mese 21)
Analogamente sono previsti i seguenti punti di verifica dei risultati di progetto:
- M5.2 - Prima versione dei dimostratori pronti per la validazione (Mese 15)
- M5.4 - Dimostratore finale pronto per la validazione (Mese 21)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 633.069,44

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

ATTIVITÀ N. 5.3

Denominazione: Test e validazione

Descrizione singola attività
Date le caratteristiche di elevata disponibilità e sicurezza richieste al sistema previsto nell'ambito del progetto Secure!, è importante effettuare una dettagliata attività di assessment volta a porre evidenza quantitativa dell'adeguatezza del sistema rispetto ai requisiti definiti nella sua specifica, ed in particolar modo rispetto ai requisiti di sicurezza, disponibilità, affidabilità e trust.
L'attività di assessment quantitativo di un sistema è tipicamente organizzata in tre macro-categorie, od approcci (ciascuna delle quali ha differenti peculiarità, che la rendono più o meno rilevante per l'analisi del sistema in quella specifica fase del suo ciclo di vita, ed è esplorabile secondo innumerevoli tecniche): approccio analitico, simulativo e sperimentale. L'attività 5.3 amalgama questi tre approcci nel ciclo di vita del sistema Secure! nel modo seguente:
- L'approccio analitico sarà effettuato in una fase iniziale del progetto, con lo scopo di fornire feedback immediati ai progettisti dell'infrastruttura e dei principali componenti del sistema. Questo approccio si baserà principalmente sull'utilizzo di tecniche quali Fault Trees, Reliability Block Diagram, Petri Nets, Attack graphs.
- L'approccio simulativo invece sarà applicato durante tutta la durata della fase di progettazione (sia

dell'infrastruttura che dei singoli servizi in questa collocati). L'obiettivo è la costruzione e il progressivo raffinamento di un modello dettagliato raffigurante l'intero sistema (sia l'infrastruttura che i singoli componenti), allo scopo di effettuare un'analisi approfondita dei requisiti di sicurezza, disponibilità, affidabilità e trust, così come emergono dalla fase progettuale del sistema. Questo ovviamente permetterà di fornire feedback sulla progettazione e evidenziare lacune o confermare la direzione intrapresa. Il formalismo delle Stochastic Activity Networks (SAN) permette di creare modelli stocastici che rappresentano fedelmente il comportamento del sistema, utilizzando diversi tipi di distribuzioni di probabilità. In questo caso, la soluzione analitica del modello non è possibile, ma il modello può essere valutato tramite simulazione a eventi discreti. Inoltre un modello dettagliato dei possibili attacchi al sistema, delle misure di sicurezza adottate e della sicurezza del sistema risultante sarà sviluppato tramite il formalismo ADVISE (ADversary VIew Security Evaluation).
- L'approccio sperimentale invece consisterà nell'effettuare attività di valutazione sperimentale (testing) sul sull'infrastruttura e sui principali servizi del sistema, sia singolarmente in laboratorio che integrati nell'infrastruttura ed operati sul campo per i piloti considerati. A tal fine si prevede l'utilizzo di test funzionali, volti a valutare il comportamento (qualitativo) delle funzionalità del sistema operante in condizioni nominali, e di robustezza, volti invece ad analizzare (sia qualitativamente che quantitativamente) il comportamento del sistema in condizioni non-standard. I test di robustezza saranno in particolar modo orientati a valutare la robustezza dei servizi, della loro integrazione nell'infrastruttura, e dell'infrastruttura stessa.

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività
Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.
Questa stima è pari a circa 83.4 mesi uomo.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D5.4 - Validazione analitica e simulativa del sistema Secure! (Mese 18)
- D5.5 - Validazione sperimentale (testing) (Mese 24)
Analogamente è previsto il seguente punto di verifica dei risultati di progetto:
- M5.3 - Test e validazione primo dimostratore completati (Mese 18)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività: 414.578,31

Eventuale documentazione Aggiuntiva

Upload:	Nessun file Caricato
Upload:	Nessun file Caricato
Upload:	Nessun file Caricato

ATTIVITÀ N. 5.4

Denominazione: Impatto

Descrizione singola attività

Il successo dell'iniziativa Secure! dipende, in buona parte, dalle attività di promozione e diffusione dei risultati che i partner sapranno attuare sin dalle fasi iniziali del progetto. È, infatti, fondamentale creare un consenso diffuso presso amministrazioni regionali, provinciali e comunali, presso le industrie che possono essere interessate all'utilizzo dei servizi Secure! e non ultimo presso gli utenti di social media ed i cittadini, che sono una parte fondamentale della catena del valore Secure!.
Per poter garantire un forte impatto dei risultati del progetto all'interno del territorio toscano è necessario raggiungere i seguenti obiettivi:
- attirare una massa critica che possa esprimere consenso verso gli obiettivi e le soluzioni proposte
- definire i vari settori di mercato che possono essere interessati all'acquisizione dalla piattaforma o anche di singoli componenti realizzati all'interno del progetto
- definire modelli di business innovativi che possano offrire un cambiamento, un 'innovazione allo scopo di ottenere un progresso socio-economico del territorio.
Attirare una massa critica:
A tal fine le attività specifiche verranno dedicate alla promozione e alla diffusione dei risultati le cui attività sono previste sin dall'inizio.
- Incontri da realizzare durante la prima fase del progetto finalizzati alla diffusione della metodologia Secure! e alla creazione di una massa critica che possa contribuire alla realizzazione e il popolamento del sistema e allo sviluppo dei dimostratori.
- Seminari, finalizzati al trasferimento dei risultati a tutti i potenziali beneficiari di Secure!, (comuni e altre amministrazioni provinciali e regionali, imprese e cittadini). Tali seminari hanno l'obiettivo di: illustrare lo stato dei lavori attraverso azioni dimostrative; di stimolare le interazioni tra i partecipanti e i potenziali soggetti interessati e di accrescere il livello di consenso sugli obiettivi del progetto.
- Iniziative specifiche promosse dalla Regione Toscana, per diffondere i risultati raggiunti ed illustrare i dimostratori identificati.
- Incontri con altre partnership regionali interessate allo sviluppo di iniziative congiunte o di azioni di supporto nell'ambito della priorità dei Distretti ICT e Poli di Innovazione con l'intento di estendere la rete di relazioni e di servizi per i cittadini e le imprese..
Definizione dei settori di mercato
Questa attività sarà focalizzata alla definizione dei vari settori di mercato potenzialmente interessati all'adozione del sistema Secure! Verranno analizzati specifici scenari che potranno essere utilizzati per verificare l'interesse del mercato di riferimento. L'analisi del mercato sarà fondamentale per poter definire i vari modelli di business.
Definizione di modelli di business innovativi: Open Innovation
Per Secure! adottare un paradigma di Open Innovation comporta che l'ambizione del progetto è quella di realizzare una piattaforma che impatti sull'ecosistema di business nella filiera di riferimento, facendo passare gli attori coinvolti da una logica della catena del valore a quella dell'ecosistema, dove gli stakeholder a volte competono, a volte collaborano ma in ogni caso creano valore per gli utenti, i clienti e per il territorio dove operano. Ciò vuole dire creare un ambiente aperto, da utilizzare per la realizzazione di applicazioni dedicate alla gestione delle emergenze e alla sicurezza del territorio, attraverso l'uso di tecnologie avanzate e innovative.
Pertanto questa attività analizzerà e produrrà nuovi modelli di business basati sul concetto di Open Innovation.

Strumenti/attrezzature

Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Non è prevista l'acquisizione di strumenti e attrezzature specifiche.
Saranno utilizzati strumenti e attrezzature ICT già presenti nelle sedi operativi di svolgimento del progetto di ciascuno dei proponenti, senza onere per la finanza di progetto.

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività
Le professionalità necessarie saranno espresse dai diversi partner secondo le indicazioni riassunte nelle cornici economiche di ciascuno.
I mesi uomo complessivi possono esser stimati coerentemente, tenendo conto dei costi medi di ciascun partner parimenti espressi.
Questa stima è pari a circa 30.1 mesi uomo.

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività
Non prevista.

Risultati Attesi: deliverable e milestones
Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.
Nell'ambito della presente attività, è previsto il seguente risultato misurabile e verificabile (deliverable):
- D5.6 - Report delle attività e risultati della comunicazione (Mese 24)
- D5.7 - Modelli e piano di Business (Mese 24)

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Costo totale dell'attività

Indicare il costo complessivo dell'attività
Costo totale dell'attività: 152.810,97

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato
Upload: Nessun file Caricato
Upload: Nessun file Caricato

ATTIVITÀ N. 5.5

Denominazione:

Descrizione singola attività

Strumenti/attrezzature
Definire quali sono gli strumenti e le attrezzature che si intendono utilizzare per la realizzazione delle attività

Risorse umane
Specificare le professionalità e i rispettivi tempi (mesi uomo) necessari alla realizzazione delle attività

Subcontratti
Individuare l'eventuale necessità di acquisire competenze tecniche specifiche o brevetti per la realizzazione delle attività

Risultati Attesi: deliverable e milestones

Illustrare i risultati attesi nel corso dell'obiettivo operativo, specificando se sono previsti specifici deliverable e milestone per l'attuazione del progetto.

Tempistica

indicare i mesi nel corso dei quali verrà realizzato l'Attività

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Costo totale dell'attività

Indicare il costo complessivo dell'attività

Costo totale dell'attività:

Eventuale documentazione Aggiuntiva

Upload: Nessun file Caricato

Upload: Nessun file Caricato

Upload: Nessun file Caricato

CRONOPROGRAMMA

OBIETTIVI / MESI

Obiettivo	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Obbiettivo 1	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#
Attivita' 1.1	#	#	#	#	#	#																		
Attivita' 1.2				#	#	#	#	#	#	#	#	#												
Attivita' 1.3				#	#	#	#	#	#	#	#	#	#	#	#									
Attivita' 1.4							#	#	#	#	#	#	#	#	#	#	#	#	#	#	#			
Attivita' 1.5							#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#
Obbiettivo 2	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#						
Attivita' 2.1	#	#	#	#	#	#																		
Attivita' 2.2				#	#	#	#	#	#	#	#	#												
Attivita' 2.3				#	#	#	#	#	#	#	#	#	#	#	#	#	#	#						
Attivita' 2.4				#	#	#	#	#	#	#	#	#	#	#	#									
Attivita' 2.5				#	#	#	#	#	#	#	#	#	#	#	#									
Obbiettivo 3	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#									
Attivita' 3.1	#	#	#																					
Attivita' 3.2	#	#	#	#	#	#	#	#	#	#	#	#												
Attivita' 3.3				#	#	#	#	#	#	#	#	#	#	#	#									
Attivita' 3.4				#	#	#	#	#	#	#	#	#	#	#	#									
Attivita' 3.5																								
Obbiettivo 4				#	#	#	#	#	#	#	#	#	#	#	#	#	#	#						
Attivita' 4.1				#	#	#	#	#	#	#	#	#												
Attivita' 4.2				#	#	#	#	#	#	#	#	#	#	#	#	#	#	#						
Attivita' 4.3							#	#	#	#	#	#	#	#	#	#	#	#						
Attivita' 4.4							#	#	#	#	#	#	#	#	#	#	#	#						
Attivita' 4.5																								
Obbiettivo 5				#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#
Attivita' 5.1				#	#	#	#	#	#	#	#	#												
Attivita' 5.2							#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#
Attivita' 5.3							#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#
Attivita' 5.4															#	#	#	#	#	#	#	#	#	#
Attivita' 5.5																								

ELEMENTI PER LA VALUTAZIONE DEL PROGETTO

CRITERI DI SELEZIONE

A. Grado di innovazione

S.1 Prospettive di diffusione e trasferimento dei risultati attesi dalla realizzazione del progetto di ricerca e sviluppo tecnologico proposto ad altre imprese potenzialmente interessate.

Il successo dell'iniziativa Secure! dipende, in buona parte, dalle attività di promozione e diffusione dei risultati che i partner sapranno attuare sin dalle fasi iniziali del progetto. È, infatti, fondamentale creare un consenso diffuso presso amministrazioni provinciali e comunali, verso le imprese che possono essere interessate all'utilizzo dei servizi Secure! e non ultimo presso gli utenti di social media, i cittadini, che sono una parte fondamentale della catena del valore Secure!.

Per poter garantire un forte impatto dei risultati del progetto all'interno del territorio toscano Secure! si propone di raggiungere i seguenti obiettivi:

- attirare una massa critica che possa esprimere consenso verso le soluzioni proposte

- definire i vari settori di mercato che possono essere interessati all'acquisizione dalla piattaforma o

anche di singoli componenti realizzati all'interno del progetto
- definire modelli di business innovativi che possano offrire un cambiamento, un 'innovazione nel'utilizzo dei vari servizi per ottenere un progresso socio-economico del territorio.
Nello specifico verranno effettuate le seguenti attività:
• Incontri da realizzare durante la prima fase del progetto finalizzati alla diffusione della metodologia Secure! e alla creazione di una massa critica che possa contribuire alla realizzazione e il popolamento del sistema e allo sviluppo dei dimostratori.
• Seminari, finalizzati al trasferimento dei risultati a tutti i potenziali beneficiari di Secure!, (, comuni e altre amministrazioni provinciali e regionali, imprese e cittadini). Tali seminari hanno l'obiettivo di: illustrare lo stato dei lavori attraverso azioni dimostrative; di stimolare le interazioni tra i partecipanti e i potenziali soggetti interessati e di accrescere il livello di consenso sugli obiettivi del progetto.
• Iniziative specifiche promosse dalla Regione Toscana, per diffondere i risultati raggiunti ed illustrare i dimostratori identificati.
• Incontri con altre partnership regionali interessate allo sviluppo di iniziative congiunte o di azioni di supporto nell'ambito della priorità dei Distretti ICT e Poli di Innovazione con l'intento di estendere la rete di relazioni e di servizi per i cittadini e le imprese.

S.2 - Contributo del progetto di ricerca e sviluppo tecnologico proposto all'avanzamento delle conoscenze,delle competenze e delle tecnologie nello specifico settore produttivo o ambito applicativo di interesse.
Il progetto si inserisce a pieno titolo in uno Stato dell'arte estremamente dinamico ed interessante, che a costo di una certa lunghezza è stato dettagliatamente illustrato nella apposita sezione.
Gli avanzamenti dello stato dell'arte proposti dal progetto vanno nelle cinque direzioni presentate nella sezione "Stato dell'arte", di seguito riportate:
1. il crowdsourcing e il crowdsensing applicati alla prevenzione, anticipazione e gestione di situazioni di emergenza/crisi, di sicurezza pubblica e di protezione civile;
2. l'acquisizione e la raccolta di dati da sorgenti multiple;
3. l'integrazione e l'analisi di informazioni, soprattutto raccolte dai social media;
4. situation awareness, early warning system e supporto decisionale;.
5. sicurezza, trust, privacy ed affidabilità delle informazioni raccolte e gestite.
Il primo tema è sia tecnologico che applicativo e di integrazione, laddove tutti gli altri sono più scientifico-tecnologici e presentano avanzamenti sia in termini generali, che nell'applicazione al problema specifico considerato nel progetto.
Nella sezione "Stato dell'arte del progetto" sono discussi e riportati in dettaglio le conoscenze, le competenze e le tecnologie avanzate dal progetto rispetto allo stato dell'arte. Se ne riportano qui per comodità gli elementi principali:
1. Applicazione del crowdsourcing e il crowdsensing alla prevenzione, anticipazione e gestione di situazioni di emergenza/crisi, di sicurezza pubblica e di protezione civile. Partendo dallo stato attuale non maturo, dal punto di vista teorico, tecnologico e organizzativo, il progetto introduce i seguenti avanzamenti: capacità di elaborare, integrare e correlare opportunamente le informazioni al fine di avere una migliore situation awareness; maggiore flessibilità, dinamicità ed efficacia nel coordinamento degli interventi orientato al raggiungimento di certi obiettivi; migliore collegamento logico-informativo tra tutti gli attori coinvolti; integrazione logica e tecnologica dei vari social media; verifica e la valutazione della veridicità e dell'attendibilità delle informazioni fornite dagli utenti; la capacità di selezionare informazioni realmente utili e rilevanti tra tutte quelle ricevute dalla folla o inserite nei social media;
2. Acquisizione e la raccolta di dati da sorgenti multiple. L'eterogeneità e la mole dei dati gestiti in Secure! porterà alla definizione di procedure e soluzioni apposite per la loro integrazione e gestione, è per la rapida scalabilità verso nuove tipologie di dati e sorgenti. Verranno definite ed implementate anche una serie di politiche per la valutazione delle sorgenti e la loro rilevanza, e per la differenziazione dell'analisi effettuabile a seconda della sorgente. Si adotteranno tecnologie state-of-the-art per la gestione di grandi moli di dati, sia online che offline, sulle quali verranno definiti e realizzati componenti, servizi e soluzioni ad-hoc per il loro filtraggio, integrazione, trasformazione e analisi per soddisfare i requisiti sfidanti imposti dal problema applicativo affrontato nel progetto.
3. Integrazione ed analisi di informazioni (soprattutto provenienti dai social media). Nuove tecniche di Entity Linking specifiche per l'analisi di contenuti testuali provenienti da Social Media (testi molto brevi, uso di un linguaggio informale, e dall'uso di costruzioni sintattiche specifiche, come "hashtags"), che superano lo stato dell'arte dell'analisi di contenuti testuali "tradizionali". Nuove tecniche di analisi aggregata di molteplici sorgenti di informazione con lo scopo di individuare topic emergenti di interesse nel tempo più breve possibile. Nuove tecniche di analisi delle immagini che permettono di allargare la tipologia di soggetti e situazioni che possono essere riconosciute automaticamente.
4. Situation awareness, early warning system e supporto decisionale. Sistema di ragionamento pratico che gestirà in maniera olistica la costruzione della situation awareness, la determinazione degli early warning e la relativa gestione dei piani di intervento e delle azioni necessarie. Questo permetterà di supportare e gestire le continue esigenze che emergono, dall'emergenza di nuove opportunità di sorgenti informative, dalla consapevolezza che lo stato della situazione "ricostruito" sarà una prospettiva della

situazione "reale", dalla necessità di gestire ed integrare informazioni a volte contrastanti tra di loro ed infine dalla necessità di dover perseguire degli obiettivi (di conoscenza, ma anche di performance), a volte anche di dover scegliere tra più opzioni o di determinare un trade-off opportunistico. La determinazione e la consapevolezza della situazione saranno il risultato della fusione di due approcci: uno bottom-up (reattivo), con le informazioni provenienti in maniera spontanea dall'ambiente osservato e da sorgenti informative geospaziali; l'altro top-down, fatto da un insieme "intenzionale" e "pianificato" di azioni informative (atte a raccogliere, estrarre, correlare, integrare, approfondire, ecc. dati ed informazioni). Il sistema, grazie al modello computazionale ed alle caratteristiche di goal-orientation di PRACTIONIST, sarà dotato della capacità di adattamento dei piani di risposta ai fattori di contingenza che possono emergere durante l'emergenza, supportando così le capacità di riconfigurazione e di rideterminazione degli obiettivi e delle azioni. Infine, un altro elemento di innovazione introdotto dal progetto è la definizione e lo sviluppo di un set di servizi di analisi off-line (Secure! Analtytics).
5. Sicurezza, trust, privacy ed affidabilità. Migliorare le tecnologie per la protezione dei servizi, dei dispositivi mobili e dei dati, con particolare attenzione agli aspetti di privacy, attraverso meccanismi per garantire la sicurezza e l'affidabilità del servizio, anche in contesti ad elevata criticità, e per la protezione di dispositivi mobili cosi come rendere affidabili le comunicazioni. Meccanismi per garantire gli accessi ai servizi in maniera appropriata attraverso i dispositivi personali mobili, in base al livello di sicurezza dettati dal contesto ed il rischio della emergenza in esame: applicazioni sui cellulari dei linguaggi di controllo accessi e delega di diritti, che sono per il momento usati solo su sistemi desktop. Meccanismi per protocolli di comunicazione anonima ove richiesto dalle politiche di privacy del utente. Meccanismi per mediare i conflitti che nascono dalla gestione condivisa dei dati. Meccanismi di valutazione della credibilità dei dati raccolti, della robustezza del sistema di raccomandazione e conseguentemente di gestione della fiducia. Soluzioni per la protezione delle informazioni personali.

B. Validità tecnica

S.3 - Livello di chiarezza e dettaglio della proposta progettuale, con particolare riferimento alle attività previste, ai tempi, agli obiettivi, ai risultati e al ruolo che i vari portatori di interessi hanno nel progetto stesso.
Nella sezione "Idea alla base del progetto", oltre a presentare le motivazioni del progetto, viene accennato l'obiettivo dello stesso e quali problematiche occorre affrontare per raggiungere tale obiettivo. Queste problematiche sono poi ampiamente discusse nella sezione "Stato dell'arte", la quale riporta un'introduzione su sistemi, approcci, soluzioni e progetti che affrontano il problema della gestione delle crisi e delle situazioni di emergenza. La sezione è poi articolata in cinque sezioni, una per ogni macro-tema di ricerca e sviluppo da affrontare nel progetto. Il primo tema (applicazione del crowdsourcing e il crowdsensing alla prevenzione, anticipazione e gestione di situazioni di emergenza/ crisi, di sicurezza pubblica e di protezione civile) è sia tecnologico che applicativo e di integrazione, mentre gli altri quattro sono più scientifico-tecnologici e presentano avanzamenti sia in termini generali, che nell'applicazione al problema specifico considerato nel progetto.
La sezione "Obiettivo generale" include , oltre alla presentazione dell'obiettivo generale del progetto Secure! (anche riportando l'architettura del Secure! Framework ed il suo ruolo nella costruzione di sistemi specifici, cfr. Figura 1), anche le seguenti informazioni aggiuntive, che mirano a fornire un quadro più chiaro della proposta e dell'approccio chr si vuole seguire:
? viene presentato il flusso e le trasformazioni che le varie tipologie ed i vari livelli di informazione considerati nel modello previsto per Secure! (cfr. Figura 2);
? vengono introdotti gli obiettivi operativi in cui l'obiettivo generale è articolato, fornendone anche una immagine con la relativa breve discussione delle relazioni tra gli stessi (cfr. Figura 3);
? viene introdotto il diagramma temporale delle attività del progetto e della notazione utilizzata nel relativo file allegato;
? viene descritto brevemente il ciclo di vita previsto per il progetto;
? vengono presentati i due piloti in cui i risultati del progetto saranno sperimentati e validati;
? viene presentato un possibile altro scenario applicativo degli stessi risultati;
? viene presentato l'impatto previsto per il progetto ed i risultati attesi;
? viene brevemente descritta la compagine dei partner ed il loro ruolo nel progetto.

S.4 - Livello di appropriatezza della definizione e motivazione della proposta di miglioramento e dei parametri di performance connessi al progetto inclusa la loro misurazione.

C. Validità economica

S.5 - Pertinenza e congruità delle spese previste in relazione ai risultati da raggiungere
Il piano economico della proposta Secure! è stato elaborato tenendo conto per ogni obiettivo della coerenza fra i risultati prodotti e il relativo costo. I dati che riportiamo qui di seguito servono a dare un quadro di insieme che evidenzia e giustifica il rapporto della stima economica rispetto ai risultati attesi.
Obiettivo 1 Secure! Framework
I risultati attesi da questo obiettivo sono:

- Specifica dei requisiti (€188.196)
- Architettura orientata ai servizi del Secure! Framework (€507.802)
- Specifica dell'infrastruttura di integrazione (€264.181)
- Servizi ed applicazioni di crowsourcing, situation-awareness ed analytics (€264.181)
- Secure! Framework (€523.902)
Il risultato finale sarà il Framework Secure! che verrà utilizzato per la sperimentazione.
Il costo stimato per il risultato finale è di €1.748.262 che ammonta al 28% del costo totale del progetto.
Tale costo è suddiviso:
Ricerca Industriale: €1.419.094 (81%)
Sviluppo Sperimentale: €329.168 (19%)
Obiettivo 2 Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy
I risultati attesi da questo obiettivo sono:
- Requisiti di affidabilità, sicurezza, fiducia e privacy per l'infrastruttura (€77.145)
- Architettura della infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy (€168.449)
- Realizzazione delle componenti della infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy (€289.644)
- Modelli ed algoritmi per la gestione degli aspetti di privacy (€74.797)
- Modelli ed algoritmi per la gestione della fiducia in resti sociali e della credibilità dell'informazione (€78.166)
Il risultato finale dell'obiettivo 2 sarà la progettazione e la realizzazione di architetture, metodologie, tecniche, protocolli e algoritmi per garantire la sicurezza, la privacy, l'affidabilità dell'infrastruttura del progetto Secure!
Il costo stimato è di €688.201 che ammonta al 11% del costo totale del progetto.
Tale costo è suddiviso:
Ricerca Industriale: €644.723 (94%)
Sviluppo Sperimentale: €43.478 (6%)
Obiettivo 3 Tecniche e componenti innovative di Crowd-sensing e crowd-sourcing
I risultati attesi da questo obiettivo sono:
- Rapporto di ricerca sulle tecniche di crowd-sensing e crowd-sourcing (€242.459)
- Rapporto di ricerca sulle tecniche, e componenti sw per la raccolta dati (€232.039)
- Rapporto di ricerche sulle tecniche, e componenti sw per l'estrazione di informazioni e modalità di integrazione. (€577.997)
- Rapporto di ricerca sulle modalità di integrazione dell'informazione. (€426.592)
Il risultato finale dell'obiettivo 3 sarà lo studio delle tecniche di crowd-sensing e crowd-sourcing e il delivery dei componenti sw all'interno della piattaforma Secure!.
Il costo stimato è di €1.479.087 che ammonta al 24% del costo totale del progetto.
Tale costo è suddiviso:
Ricerca Industriale: € 1.344.031 (91%)
Sviluppo Sperimentale: € 135.056 (9%)
Obiettivo 4 Tecniche e componenti innovativi per il supporto decisionale
I risultati attesi da questo obiettivo sono:
- Modelli di gestione dei contenuti e delle decisioni (€251.208)
- Tecniche e servizi di elaborazione ed analisi in tempo reale (situation awareness) (€156.063)
- Servizi e meccanismi decisionali (€236.576)
- Tecniche e servizi per l'analisi off-line (Secure! Analytics) (€318.160)
Il risultato finale dell'obiettivo 4 sarà l'implementazione del sistema di gestione delle azioni e di supporto decisionale (Decisional Support System, DSS).
Il costo stimato è di € 962.007che ammonta al 15% del costo totale del progetto.
Tale costo è suddiviso:
Ricerca Industriale: € 920.087 (96%)
Sviluppo Sperimentale: € 41.920 (4%)
Obiettivo 5 Applicazione e validazione in contesti reali
I risultati attesi da questo obiettivo sono:
- Specifica degli scenari applicativi del dimostratore e piano di sperimentazione (€171.241)
- Dimostratore utilizzato per la realizzazione dei piloti (€633.069)
- Validazione analitica e simulativa del sistema Secure! (€207.289)
- Validazione sperimentale (testing) (€207.289)
- Realizzazione di attività per la valorizzazione e promozione dei risultati del progetto (€50.937)
- Modelli e piano di Business (€101.874)
Il risultato finale dell'obiettivo 5 sarà l'implementazione del sistema di gestione delle azioni e di supporto decisionale (Decisional Support System, DSS).
Il costo stimato è di € 1.371.700che ammonta al 22% del costo totale del progetto.
Tale costo è suddiviso:
Ricerca Industriale: € 786.559 (57%)

Sviluppo Sperimentale: € 585.141 (43%)
Il costo totale del progetto, che ha come scopo la realizzazione di un sistema per la fornitura di strumenti di supporto per la gestione di scenari di sicurezza pubblica e privata e di protezione civile (prima, durante e dopo), è di € 6.249.257,19 con un finanziamento della Regione Toscana di €2.752.343,96 (44,04% del costo totale).

D. Rilevanza aziendale

S.6 - Prospettive di mercato in termini di miglioramento dei processi di produzione e di definizione di nuovi prodotti/servizi derivanti dalla realizzazione del Progetto di R&S

L'obiettivo del progetto SECURE!, da un punto di vista industriale è sostanzialmente quello di realizzare una importante innovazione di prodotto, cui si accompagneranno innovazioni di processo nei "clienti" che l'adotteranno all'atto della sua applicazione.
Limitiamoci per ora ad analizzare i benefici "interni" che questa innovazione di prodotto porterebbe ai proponenti.
Le aziende che propongono SECURE! sono tutte aziende del settore ICT.
Esse quindi, sia pure con profili diversi tra loro dovute alle ovvie differenze che esse hanno, ad esempio sotto il semplice profilo della dimensione dell'azienda, devono comunque confrontarsi con alcune dinamiche fondamentali di evoluzione del settore.
Il settore dell'ICT, per le imprese europee e per quelle nazionali in particolare, presenta una sfida competitiva principale: troppi operatori storicamente si sono posti sul mercato solo con un approccio da System Integrator o "peggio" con un approccio da fornitore di risorse di progettazione/programmazione da inserire in progetti di System Integration di responsabilità di altri.
Ora tali due modelli di business, pur se importanti e rispettabili, presentano entrambi un rischio di compressione del ruolo dell'azienda nella catena del valore, e quindi, dei margini ottenibili.
Questo rischio deriva da un duplice fenomeno:
A) Da un lato vi è un continuo innalzarsi delle prestazioni e delle funzionalità delle piattaforme e dei prodotti software "di base", quindi realizzare sistemi complessi richiede progressivamente minori attività;
B) dall'altro per svolgere tali attività d'integrazione e personalizzazione dei sistemi, sta progressivamente crescendo la concorrenza internazionale di System Integrator basati nei Paesi emergenti (in paesi come l'India, il Brasile, alcuni paesi dell'est europeo), che possono girare al cliente una parte del vantaggio di costo di cui godono nell'accesso a risorse professionali di basso costo e ottima preparazione (in un fenomeno noto come offshoring).
Citando ad esempio i dati riportati nello studio UNCTAD Information Economy Report 2010 il mercato globale per l'outsourcing dei servizi ammonterebbe a un importo compreso tra 785 e 805 miliardi di dollari nel 2009, del quale il 12 % internazionale (offshore sourcing).
Ben due terzi di questo mercato sono legati all'IT (servizi di programmazione, systems integration, test e supporto) e solo un terzo all'outsourcing di processi di business (come il customer care). Il fenomeno è in espansione, specie in termini di nazioni che si propongono come fornitori a basso costo. Vale la pena notare che nella crisi l'andamento di questo trend non ha mostrato segni apprezzabili di flessione, proprio perché risponde a razionali di risparmio ed efficienza economica.
In sintesi in questa situazione molte aziende IT europee, che finora sono stati a vari livelli e con vari profili dei System Integrators corrono il rischio di una sostanziale erosione della propria competitività, schiacciati da una dinamica competitiva che vede da un lato giganti mondiali come Google, Microsoft o Oracle che possono far leva su loro prodotti software, dall'altro dalla concorrenza di Paesi come l'India, la Cina o il Brasile.
È fondamentale superare questa rischio; fortunatamente negli ultimi anni insieme a questi rischi si stanno aprendo nuove opportunità in contesti di mercato che fino a qualche anno fa sembravano completamente bloccati. Un esempio tipico è costituito dall'informatica ad uso "consumer". Qualche anno fa questo mercato era largamente dominato dai produttori di package applicativi importanti che richiedevano enormi investimenti e potavano contare su una posizione di leadership del mercato fortissima. L'esempio più tipico si poteva trovare nel pacchetto di applicazioni di produttività personale "Office" di Microsoft, ma più in generale il fenomeno del predominio di alcuni produttori e delle elevatissime barriere all'ingresso si verificava anche per moltissimi altri prodotti software consumer.
Negli ultimi anni invece alcuni fenomeni tra cui una sempre più efficace declinazione del modello Open Source, e il connesso crescere del ruolo degli standard aperti, de jure o de facto, e delle tecnologie di interoperabilità, ma soprattutto l'enorme successo dei due fenomeni del Social Networking e del Mobile Computing con smartphones e laptops hanno cambiato radicalmente queste prospettive.
In questo contesto, infatti, è stato riscoperto e ridefinito il ruolo del "prodotto" software, che è diventato un concetto molto più agile, focalizzato e di nicchia, e che può essere definito e realizzato con livelli di investimento ragionevoli anche per operatori IT che prima non avevano altra scelta che proporsi al mercato come "System Integrators".
Basti ad esempio pensare all'enorme numero di apps che sono state prodotte e messe sul mercato (Apple Store o Android Market – proprio in questi giorni l'Apple Store ha raggiunto 25 miliardi di applicazioni scaricate in soli quattro anni) o anche alle applicazioni disponibili su piattaforme sociali quali Facebook

(l'esempio più tipico essendo quello dei giochi, che però non è il solo).
In questo nuovo contesto diventa quindi in definitiva al contempo possibile ed indispensabile difendere la competitività e la redditività aziendale ideando opportuni "prodotti" software di nicchia.
E' chiaro quindi che il progetto SECURE! risponde pienamente a questa esigenza.
Esso consentirà di inserirsi nei fenomeni del Mobile Computing e del Social Networking, sempre più centrali al settore ICT, con una finalizzazione che coniugherà all'indubbio e crescente appeal di questi paradigmi una destinazione di utilizzo, quella della sicurezza, che è in se stessa, di estrema importanza e di valore economico potenziale rilevantissimo.

E. Competenze ed esperienze del Gruppo di Lavoro proposto

S.7 - Esperienze e competenze delle imprese partecipanti al Progetto di R&S in attività di ricerca industriale e sviluppo sperimentale

ENGINEERING è un player globale e il primo gruppo di system integration in Italia, leader nell'offerta integrata e completa lungo l'intera catena del valore del software: progettazione, sviluppo, servizi di outsourcing, prodotti e soluzioni verticali proprietarie, consulenza IT e strategica, su misura per i modelli di business dei clienti su tutti i mercati. L'azienda conta 6.300 dipendenti, 37 sedi con una distribuzione capillare nelle Regioni italiane, presenza commerciale diretta nell'UE, in Irlanda e in Belgio, ed extra-UE in Brasile e area America latina. Grazie al piano di acquisizioni e alla capacità di apertura di nuovi mercati, il Gruppo dispone di una capacità produttiva globale in 40 diversi Paesi.
Con un valore della produzione di oltre 700 milioni di euro ed un market share del 7%, il gruppo ENGINEERING opera con 7 business unit: Finance, Pubblica Amministrazione Centrale, Pubblica Amministrazione Locale e Sanità, Oil & Services, Energy & Utility, Industry e Telecom, supportate da 5 centri competenza trasversali rispetto alle business unit e ad elevata specializzazione e dalla Divisione Ricerca & Innovazione che ha il doppio ruolo di promuovere la ricerca sul software a livello internazionale e trasferire l'innovazione al ciclo produttivo delle strutture di business.
ENGINEERING è partner e socio fondatore della piattaforma di software e servizi NESSI che ha già ricevuto 200 milioni di investimenti per progetti da sviluppare in ambito UE. ENGINEERING ha partecipato e partecipa costantemente a progetti di ricerca europei e nazionali, insieme ai principali player ICT, università e centri di ricerca.
Il progetto Secure! sarà prevalentemente realizzato nell'ambito dell'unità di ricerca "Intelligent Systems". Un risultato di tale ricerca è la suite di sviluppo PRACTIONIST (www.practionist.org), che sarà estesa ed utilizzata nel presente progetto, soprattutto per il supporto ai processi decisionali.
Inoltre l'unità "Intelligent Systems" ha maturato negli anni competenze e risultati nei ambiti rilevanti per il progetto Secure!: sistemi intelligenti, interfacce intelligenti, sistemi di ragionamento pratico, infrastrutture autonomiche di erogazione di servizi, goal-oriented business process management, servizi ubiquitous, user profiling e social network analysis.
L'Università degli Studi di Firenze è una Università con circa 25000 studenti, e che svolge attività di ricerca in svariati domini, dall'ingegneria alle scienze umane, architettura, medicina o informatica. Il gruppo di ricerca RCL (Resilient Computing Lab) presso il Dipartimento di Sistemi e Informatica ha il suo obiettivo centrale nella ricerca e sperimentazione di architetture e sistemi resilienti e sicuri. Il gruppo è attualmente coinvolto nella ricerca in due macro-aree: i) architetture e tecniche per i sistemi fault tolerant, infrastrutture e reti, e ii) validazione della dependability, trust e Qualità del Servizio (QoS) di sistemi informatici, attraverso tecniche analitiche, simulative e sperimentali. Membri del gruppo sono stati coinvolti in molti progetti cooperativi, inclusi progetti Nazionali e finanziati dalla Comunità Europea dal Framework 2 al Framework 7. Attualmente il gruppo è coinvolto nei progetti Europei FP7-SST-2008-234088 ALARP (A railway automatic track warning system based on distributed personal mobile terminals) ed ARTEMIS-JU-100022 CHESS, nel progetto Nazionale MIUR-PRIN DOTS-LCCI - - Dependable Off-The-Shelf based middleware systems for Large-scale Complex Critical Infrastructures", e nel Progetto Regionale Bando Unico R&S 2008-POR CREO attività 1.5 "SILFI - Sistema Intelligente per la Lotta al Fuoco Integrata".
Resiltech è una giovane Società a Responsabilità Limitata, nata nel Settembre del 2007, che integra l'esperienza di ricerca accademica con competenze di verifica e validazione e di sviluppo nell'ambito dei sistemi resilienti. Il team fondatore di Resiltech è infatti composto da personale con Dottorato di Ricerca nell'ambito della progettazione e validazione sistemi critici, e da personale con ampia esperienza industriale nella medesima area. L'ampia esperienza di Resiltech nell'ambito della Verifica e Validazione la qualificano come un importante consulente per la certificazione di prodotti critici, principalmente nell'ambito ferroviario e dell'automotive, dove Resiltech offre il suo supporto a molte compagnie sia di piccole che di grandi dimensioni. Resiltech vanta importanti esperienze nell'ambito della ricerca e tecnologia ICT, in particolare nel campo della teoria e pratica dei sistemi resilienti. Resiltech è stata coinvolta nel progetto Europeo FP7-ICT-CA-216295 AMBER Coordination Action ed è attualmente coinvolta nel progetto Europeo FP7-SST-2008-234088 ALARP (A railway automatic track warning system based on distributed personal mobile terminals) e nel Progetto Regionale Bando Unico R&S 2008-POR CREO attività 1.5 "SILFI - Sistema Intelligente per la Lotta al Fuoco Integrata". Resiltech attualmente contribuisce alla definizione dello standard ISO26262 ed in AUTOSAR (principalmente nel settore WP1.3 Safety).

Il Laboratorio Comunicazioni e Immagini (LCI) (http://lci.micc.unifi.it/labd/) è uno dei laboratori del Centro di Eccellenza MICC (Centro per la Comunicazione e l'Integrazione dei Media) dell'Università degli Studi di Firenze. LCI svolge attività di ricerca di base e azione di trasferimento tecnologico verso le imprese e gli enti pubblici. L'attività di ricerca si colloca nell'ambito dell'Ingegneria dell'Informazione e della Multimedialità, qui di seguito sono elencati i principali settori di interesse.
Multimedia Forensics. Il gruppo di lavoro ha sviluppato metodologie per l'identificazione della sorgente di acquisizione (ad esempio marca e modello di fotocamere digitali) che esplorino le varie fasi di acquisizione di una fotocamera digitale cercando imperfezioni nel sensore di acquisizione (CCD) o sono volti a rintracciare il tipo di interpolazione cromatica nelle fotocamere dotate di Color Filter Array (CFA). Vengono sviluppate applicazioni e metodi indirizzati a identificare le operazioni di post-processing sull'immagine come la compressione (doppio JPEG), le trasformazioni affini (rotazioni, ridimensionamento), il cloning (regioni duplicate nell'immagine) e fotomontaggi volti a individuare regioni contraffatte all'interno dell'immagine sotto osservazione.
Television e Digitale Terrestre (DTT) e Applicazione MHP. Il gruppo di lavoro ha progettato e sviluppato applicazioni standard MHP per la DTT mediante l'utilizzo di software dedicati (authoring tool specifici) o direttamente in linguaggio Java. Il risultato di tale lavoro ha portato alla realizzazione di applicazioni di servizio di tipo sia statico che interattivo.
Il laboratorio è stato partner del Centro di Competenza sulla Televisione Digitale Terrestre (DTT-Toscana Lab).
Applicazioni Multimediali per i Beni Culturali. Le attività del laboratorio concernono anche la progettazione e lo sviluppo di applicazioni multimediali dedicate alla messa in rete di contenuti digitali e alla loro protezione con tecniche opportunamente sviluppate. Quest'ambito di ricerca tipicamente multidisciplinare coinvolge diverse esperienze e professionalità tra cui: programmazione Java, gestione di database e banche dati. Attualmente vengono realizzate applicazioni dedicate alla esposizione web di database di immagini e metadati di interesse culturale, messi a disposizione dalla Direzione Regionale per i Beni Culturali e Paesaggistici della Toscana.
Gli apporti tecnici che il gruppo LCI può fornire nell'ambito del progetto SECURE! sono inerenti alla definizione e accrescimento della sicurezza (obiettivi operativi 1 e 2), all'attività forense relativa ai media digitali (obiettivo operativo 3) e all'acquisizione di dati multicanale, con particolare riferimento al canale DTT, Televisione Digitale Terrestre, (obiettivo operativo 3). Un contributo è altresì fornito nell'ambito dell'attività di validazione del sistema tramite approcci analitici, simulativi e sperimentali (obiettivo operativo 5), nonché nella disseminazione dei risultati del progetto tramite presentazioni e partecipazioni a convegni di rilevanza Internazionale.
Il Consiglio Nazionale delle Ricerche (CNR) è un Ente pubblico nazionale con il compito di svolgere, promuovere, diffondere, trasferire e valorizzare attività di ricerca nei principali settori di sviluppo delle conoscenze e delle loro applicazioni per lo sviluppo scientifico, tecnologico, economico e sociale del Paese. Gli istituti del CNR sono le unità che svolgono le attività di ricerca e si caratterizzano per le competenze, le attrezzature sperimentali e l'eccellenza dei ricercatori. Successivamente all'entrata in vigore del DL di riordino del CNR nel giugno 2003, il CNR è organizzato in una rete di 107 istituti, tra questi lo IIT e L'ISTI sono all'interno dell'area della ricerca di Pisa, la più grande della rete scientifica del CNR.
L'unità di ricerca CNR (Pisa) che partecipa al progetto Secure! si avvale della competenza di 3 gruppi di ricerca: Sicurezza (SEC), High performance Computing (HPC) e multimedia (NeMIS) di seguito descritti.
Il gruppo sicurezza (SEC) ha maturato una notevole esperienza nel settore della sicurezza, inclusi aspetti di cyber-security. Le tematiche principali di ricerca vertono sulla sicurezza di servizi web e cloud e di devices mobili, sull'analisi di sistemi critici, su sistemi di trust (fiducia) e risk management ed sulla sicurezza di social networks/dynamic coalitions. Il gruppo di ricerca, composto da circa 20 persone, è attivamente coinvolto in diversi importanti progetti europei in corso di svolgimento, tra cui Contrail, CONNECT, SESAMO, ANIKETOS, ed ha lavorato sul progetto regionale VISITOTuscany. Il gruppo coordina attualmente il progetto Europeo NESSoS, una rete di eccellenza per la sicurezza dell'Internet del Futuro. Il gruppo e' anche attivo nel coordinamento della piattaforma tecnologica italiana SERIT (Security Research in ITaly).
La ricerca svolta dal Laboratorio di High Performance (HPC) è finalizzata alla ricerca, progettazione e sviluppo di sistemi e soluzioni per problemi complessi, utilizzando tecniche di calcolo ad alte prestazioni. Settori principali di ricerca sono: Data and Web Mining, Information Retrieval, Distributed Search Engines, Service-Oriented Architectures, Cloud and Peer-to-Peer Systems. L'enfasi è posta sui requisiti di alte prestazioni, sia dei servizi offerti che delle applicazioni finali. Il gruppo di ricerca, composto da circa 20 persone, è attivamente coinvolto in diversi importanti progetti europei in corso di svolgimento, tra cui S-Cube, Contrail, Assets, IngeoClouds.
Il gruppo NeMIS ha maturato una lunga esperienza sullo studio e realizzazione di tecniche di image searching e content recognition. In particolare, le tecniche sviluppate, oltre ad offrire un alto grado di accuratezza, sono altamente scalabili e permettono di gestire sull'ordine delle centinaia di milioni di immagini. Il gruppo ha una lunga esperienza nella gestione di progetti di ricerca europei e finanziati da fondi strutturali. Il gruppo e' stato anche recentemente coordinatore del progetto regionale

VISITOTuscany.
Crowd è un'azienda che ha innovato il modo di collaborare su Internet mediante l'applicazione del crowdsourcing ai processi di business. Crowd svolge tutta la ricerca e sviluppo tra le sedi di Pisa e di Catania, sedi nelle quali impiega una quindicina di persone altamente specializzate e votate all'innovazione tecnologica e di processo. Crowd ha una presenza diretta oltre che in Italia in altri paesi europei quali Francia, Inghilterra, Germania e Spagna, e extra europei come gli Stati Uniti attraverso la controlla CrowdEngineering.
Crowd si è già distinta nell'innovazione sul crowdsourcing meritando dei riconoscimenti quale il titolo di "Cool Vendor in Social Software and Collaboration" di Gartner, "Company to watch in Social CRM" di Altimiter.
La piattaforma CrowdForce, prodotto di punta della Crowd, fornisce una soluzione completa per chi deve sviluppare delle applicazioni di crowdsourcing pienamente integrate con i sistemi aziendali e tutta la galassia Social Media. Esperienze attive nel mondo delle Telecomunicazioni, della Finanza, della Pubblica Amministrazione, della Ricerca e dei Media dimostra una flessibilità e trasversalità che rende la collaborazione con le "folle Internet" una grande opportunità per diversi settori economici.

S.8 - Esperienze e competenze professionali dei singoli Componenti il Gruppo di Lavoro in relazione alle funzioni e alle attività assegnate nel Piano di Lavoro.
I partner partecipanti al progetto Secure! costituiscono una compagine ben affiatata (avendo già collaborato in a precedenti iniziative progettuali di ricerca e sviluppo) e che garantisce tutte le competenze richieste per il corretto svolgimento delle attività ed il pieno raggiungimento dell'obiettivo generale suddetto ed i relativi obiettivi operativi in cui lo stesso è decomposto.
In termini generali, la suddetta compagine consta di una grande azienda ICT (ENGINEERING Ingegneriai Informatica s.p.a.), due PMI ICT (Crowd e Resiltech) e tre organismi di ricerca (Università di Firenze, Centro per la Comunicazione e l'Integrazione dei Media dell'Università degli Studi di Firenze, il Consiglio Nazionale delle Ricerche di Pisa). Questo equilibrio tra mondo della ricerca accademica e mondo della ricerca industriale, a nostro avviso, costituisce la giusta miscela per garantire un elevato grado di avanzamento dello stato dell'arte tecnologico-scientifico (come descritto nella relativa sezione) e l'effettiva applicazione dei risultati del progetto in contesti reali, come quelli degli scenari previsti per il progetto (descritti sopra) e scenari possibili (anch'essi brevemente accennati sopra).
Entrando più nel merito delle attività del progetto Secure!, in relazione alla partecipazione dei partner, si vuole rimarcare che la responsabilità obiettivi relativi di impostazione, integrazione (OO 1 - Secure! Framework) ed applicazione (OO 5: Applicazione e validazione in contesti reali) è affidata ad ENGINEERING, la quale ha anche la responsabilità delle componenti innovative per il supporto decisionale (obiettivo operativo 4). La responsabilità delle componenti innovative per il crowd-sensing è invece affidata a Crowd, laddove il CNR assume la responsabilità dell'obiettivo operativo 2 per la realizzazione dell'infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy. La seguente lista nostra le partecipazioni ed i ruoli dei partner nei vari obiettivi operativi:
• OO1 - Secure! Framework: ENGINEERING (responsabile), RESILTECH, Università di Firenze, MICC (partecipanti)
• OO2 - Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy: CNR (responsabile), RESILTECH, Università di Firenze, MICC, ENGINEERING (partecipanti)
• OO3 - Tecniche e componenti innovative di Crowd-sensing: CROWD (responsabile), MICC, ENGINEERING, CNR (partecipanti)
• OO4 - Tecniche e componenti innovative per il supporto decisionale: ENGINEERING (responsabile), RESILTECH, Università di Firenze, CNR (partecipanti)
• OO5 - Applicazione e validazione in contesti reali: ENGINEERING (responsabile), RESILTECH, Università di Firenze, MICC, CNR (partecipanti)
Ruoli dei partner all'interno del progetto Secure!.
ENGINEERING è il soggetto capofila dell'ATS e partecipa a quasi tutte le attività del progetto, ed è responsabile dell'obiettivo 1 e 5.
Università di Firenze –DSI. Le competenze apportate dal gruppo DSI nel progetto sono inerenti alla identificazione ed analisi dei requisiti critici per la sicurezza (obiettivo operativo 1 e 2), alla definizione di soluzioni architetturali e meccanismi per garantire la resilienza e sicurezza del sistema Secure! (obiettivo operativo 1 e 2), all'attività di validazione del sistema tramite approcci analitici, simulativi e sperimentali (obiettivo operativo 5), ed infine nella disseminazione dei risultati del progetto tramite presentazioni e partecipazioni a convegni di rilevanza Internazionale relativi all'ambito dei sistemi critici.
RESILTECH. Le competenze apportate da Resiltech nel progetto sono inerenti all'analisi dei requisiti, ed alla attività progettazione, sviluppo e validazione del sistema Secure! (obiettivo operativo 1), con attenzione agli aspetti critici, in particolare privacy e disponibilità (obiettivo operativo 2), riguardo ai quali Resiltech vanta ampia esperienza. Resiltech offre la possibilità di disseminazione dei risultati del progetto tramite presentazioni a corsi di formazione, partecipazioni a gruppi di lavoro, e convegni di rilevanza Internazionale.
Università di Firenze – MICC- LCI. Gli apporti tecnici che il gruppo LCI può fornire nell'ambito del progetto SECURE! sono inerenti alla definizione e accrescimento della sicurezza (obiettivi operativi 1 e

2), all'attività forense relativa ai media digitali (obiettivo operativo 3) e all'acquisizione di dati multicanale, con particolare riferimento al canale DTT, Televisione Digitale Terrestre, (obiettivo operativo 3). Un contributo è altresì fornito nell'ambito dell'attività di validazione del sistema tramite approcci analitici, simulativi e sperimentali (obiettivo operativo 5), nonché nella disseminazione dei risultati del progetto tramite presentazioni e partecipazioni a convegni di rilevanza Internazionale.
CNR. In Secure! il CNR è coinvolto in molte attività ed in tutti gli obiettivi operativi. Il CNR è responsabile dell'obiettivo operativo 2: Infrastruttura di gestione dell'affidabilità, sicurezza, fiducia e privacy.
CROWD. All'interno del progetto Crowd si occupa della ricerca e sviluppo delle tecnologie e modelli di corwdsourcing e di realizzazione di componenti innovativi di crowdsensing (nell'ambito dell'obiettivo operativo 3).

CRITERI DI PREMIALITA'

P.1 - Progetti proposti da imprese che aderiscono ai poli di innovazione e ai distretti tecnologici2 alla data di presentazione della domanda (nel caso di RTI/ATS tutte le imprese devono aderire ad un polo di innovazione o ad un distretto tecnologico)
Tutti i partecipanti sono affiliati a Poli e Distretti tecnologici della Regione TOscana. Nel Dettaglio:
Engineering Ingegneria Informatica è iscritta al Polo di Innovazione ICT - Robotica dal 9 marzo 2012
CrowdEngineering si è affiliato al Polo di Innovazione ICT Robotica in data 23 ottobre 2011
Resiltech : è affiliato al Polo di Innovazione ICT Robotica in data 14 marzo 2011
Rsiltech e' anche affiliata al DISTRETTO PER LE TECNOLOGIE FERROVIARIE, L'ALTA VELOCITA' E LA SICUREZZA DELLE RETI" dal 30/01/2012
Università di Firenze, CNR di Pisa fanno parte del Distretto Tecnologico ICT & Security dal 14 dicembre 2005
CNR è affiliata anche al Polo di Innovazione ICT Robotica dal 2 agosto 2011.
Le adesioni verranno presentate al momento della richiesta

P.2 - Progetti in aggregazione proposti da imprese appartenenti tutte ad una rete di imprese, formalizzata in contratto di rete ai sensi della L. 33/2009 alla data di presentazione della domanda
N/A

P.3 -Progetti presentati da un numero di imprese in aggregazione superiore al numero minimo di tre
Indicare il numero di imprese in RTI/ATS: *3*

P.4 - Progetti presentati da imprese giovanili e femminili (nel caso di RTI/ATS almeno un'impresa deve essere giovanile o femminile)[3]
N/A

P.5 - Progetti che assicurino occupazione aggiuntiva durante la realizzazione del progetto o entro la conclusione del progetto con effetti successivi (compilare la tabella successiva)
Per occupazione aggiuntiva si intende il numero espresso in Unità Lavorative Annuali di nuovi addetti inseriti nell'organico della sede operativa in cui si svolge il progetto di R&S a partire dalla data di presentazione della domanda d'aiuto)
N/A

1. **Per quanto riguarda i criteri da S.1 a S.8** il proponente ha la facoltà, ma non l'obbligo di compilare le sezioni. La compilazione dei punti è utile al fine di evidenziare e dare particolare rilievo ad elementi già descritti nelle precedenti schede del progetto, ma che si ritengono particolarmente importanti per l'attribuzione del punteggio in relazione allo specifico criterio. **Per quanto riguarda i criteri da P.1 a P.5** il proponente ha l'onere di compilare quelle sezioni nelle quali aspira ad ottenere il punteggio di premialità, dando evidenza, in particolare, agli elementi oggettivi che danno diritto a punteggio.
2. Poli di innovazione, come riconosciuti e ammessi a finanziamento nell'ambito del bando regionale attuativo della linea di attività 1.2 del POR Creo 2007-2013, approvato con decreto dirigenziale n.6377 del 21.12.2010 e distretti tecnologici di cui alla delibera GR 603/2010 e successive modifiche e integrazioni.
3. Si fa riferimento alla nozione di PMI giovanili, PMI femminili, come definite ai punti f, e g dell'art.1 del regolamento degli interventi previsti dalla Legge Regionale 21/2008, allegato A alla DGR 907 del 24 ottobre 2011. Ai fini del presente bando, il possesso del requisito di PMI femminile, giovanile o di lavoratori destinatari di ammortizzatori sociali, è dichiarato dal legale rappresentante ai sensi del DPR 445/00.

TABELLA RILEVAZIONE ULA

Ente	ULA alla data di presentazione	Occupazione aggiuntiva	Occupati di cantiere con termine contrattuale entro la	Occupati assunti prima della conclusione del progetto con effetti successivi alla conclusione dello stesso

		TOTALE	Tipologia	conclusione del progetto ULA	di cui Donne	contratto a tempo determinato ULA	di cui Donne	contratto a tempo indeterminato ULA	di cui Donne
Engineering Ingegneria Informatica S.p.A.	1	4		1	1	2	2	1	1
Engineering Ingegneria Informatica S.p.A.	0	0		0	0	0	0	0	0
Engineering Ingegneria Informatica S.p.A.	0	0		0	0	0	0	0	0
Engineering Ingegneria Informatica S.p.A.	0	0		0	0	0	0	0	0
Engineering Ingegneria Informatica S.p.A.	0	0		0	0	0	0	0	0
Engineering Ingegneria Informatica S.p.A.	0	0		0	0	0	0	0	0
		0	Ricercatore	0	0	0	0	0	0
		0	Assegnisti collaboratori	0	0	0	0	0	0
		0	Tecnici laureati	0	0	0	0	0	0
		0	Dirigenti	0	0	0	0	0	0
		0	Personale amm.vo	0	0	0	0	0	0
		0	Altro	0	0	0	0	0	0
TOTALE	1	4		1	1	2	2	1	1