Programma Operativo Nazionale 2014-2020
Dottorati di ricerca su tematiche dell'innovazione e green
D.M. n. 1061 del 10 agosto 2021

Università degli Studi di Napoli Federico II
Dottorato di Ricerca in Information Technology and Electrical Engineering
XXXVII CICLO
TEMATICHE GREEN (AZIONE IV.5)

BORSA N. 4 - Dottorando FRANCESCO CAPUTO

Titolo del progetto:

"Cybersecurity nelle reti di trasduttori in ambito *smart farm*"

SETTORE SNSI: Industria intelligente e sostenibile, energia e ambiente

SETTORE PNR: Prodotti Alimentari, Bioeconomia, Risorse Naturali, Agricoltura, Ambiente

a. Motivazioni

Spesso si parla di sicurezza nel momento in cui ci siano dati sensibili da proteggere. Tuttavia, quali siano questi dati sensibili in oggetto è legato a specifiche scelte progettuali. In questo percorso dottorale si vuole porre l'attenzione sulla cybersecurity in ambito "Agrifood" del PNR ed "Industria Intelligente" ed "Alimentazione" del programma SNSI, in quanto ci si muove verso un mondo sempre più connesso che sta recentemente investendo anche nel settore agricolo maggiori energie e risorse.

Sono sempre più diffusi infatti i sistemi gestiti di coltivazione, che fanno uso di una classe di trasduttori, attuatori e sistemi di gestione connessi tra loro in modo da poter migliorare coltivazioni agricole in maniera naturale, pulita ed ecosostenibile.

In virtù del fatto che le componenti di questi sistemi di gestione sono connessi, questi componenti comunicano tra loro dati fondamentali per il corretto funzionamento di tutto il sistema. Molte volte, erroneamente, si pensa che questi dati (es. temperature, umidità di un terreno, luminosità, raggi UV, ecc.) non siano sensibili ed in quanto tali non vadano tenuti in sicurezza. Esiste tuttavia la possibilità, non così remota, che questi dati siano alterati da componenti esterni malevoli, che portano ad alterazioni del comportamento del sistema complessivo, con l'inevitabile epilogo della perdita di qualità di un raccolto o anche la perdita del raccolto stesso.

La possibilità di cyber-attacchi diretti a sistemi utilizzati nell'ambito agrifood è ancora più concreta in un contesto di libero mercato, dove la concorrenza è l'elemento fondamentale, e vi è un alto rischio di servirsi di una pratica illecita, quale la compromissione malevola di un sistema di coltivazione.

Complici i cambiamenti climatici, infine, sono altresì sempre più diffusi i sistemi di controllo e gestione di impianti di coltivazione *indoor* (*smart farm* o serre idroponiche), dove i sistemi diventano ancor più complessi, e dove, ancora una volta, la modifica illecita del comportamento della stessa può significare anche il fallimento di un produttore o anche il rovescio di un intero mercato a favore di altri.

È evidente che è necessario portare l'attenzione su ciò che non solo riguarda la realizzazione di sistemi di coltivazione ecosostenibile, ma anche alla sicurezza degli stessi. Ricorrere a sistemi di controllo e monitoraggio è una pratica sempre più diffusa, ma ad oggi non si pone il giusto grado di importanza alla sicurezza dei dati scambiati, mentre essa sarà certamente necessaria nell'immediato futuro.

La proposta di percorso dottorale è finalizzata dunque alla prototipazione ed alla validazione di strategie di contrasto di cyber-attacchi mirati ad alterare il funzionamento di sistemi di coltivazione intelligenti, favorendo quindi l'inserimento degli stessi nel settore agricolo in maniera sempre più affidabile.

b. Obiettivi

L'attività di ricerca proposta consiste nello sviluppo e validazione di contromisure ad attacchi digitali in ambito agrifood, con particolare riferimento ai sistemi di coltivazione intelligenti e alla sicurezza ed affidabilità degli stessi, nell'ottica di tecnologie a stato dell'arte per un mercato high-tech dell'industria agroalimentare.
Saranno prese in considerazione la vulnerabilità di trasduttori per l'internet of things (IoT) impiegati nell'ambito agricolo, la vulnerabilità degli algoritmi di crittografia utilizzati per trasmettere i dati acquisiti nel monitoraggio dei processi della filiera agricola, le tecniche utilizzate per ottenere in modo malevolo le chiavi di cifratura degli algoritmi di crittografia e le tecniche utilizzate per attaccare, intercettare e sostituire i dati scambiati.
Ci si propone di studiare le pratiche di attacco comunemente utilizzate per attaccare sistemi di natura diversa da quella agroalimentare per contestualizzarle poi all'ambito di ricerca. Un'attenzione particolare sarà devoluta ai cosiddetti "side-channel attacks", che si basano sulla perdita collaterale di informazioni correlate all'operazione del dispositivo, come ad esempio consumo di energia e dissipazione di calore, per poter accedere alle informazioni sensibili che dovrebbero essere protette. Si valuteranno quindi appropriate contromisure per favorire la libera crescita ed esercizio in sicurezza dei sistemi agricoli, garantendo un libero mercato ed una concorrenza sana.
Ci si pone, quindi, come principale obbiettivo la prototipazione e la validazione di strategie di contrasto ai cyber-attacchi rivolti a sistemi di coltivazione connessi, alla perdita di dati ed al perfezionamento dei sistemi di crittografia utilizzati, migliorando quindi la sicurezza nella comunicazione di dispositivi IoT utilizzati nell'agricoltura di precisione. La sensibilizzazione all'argomento cyber-security sarà anche di fondamentale importanza in ambito delle coltivazioni intelligenti, favorendo al contempo il piano regionale "Industria intelligente ecosostenibile, energia e ambiente" del programma SNSI ed in accordo con il settore "Prodotti Alimentari, Bioeconomia, Risorse Naturali, Agricoltura, Ambiente" del PNR.
Infine, nel raggiungimento di tali obbiettivi, il candidato acquisirà conoscenze sia specialistiche che trasversali con riferimento principale agli ambiti agrifood, intelligenza artificiale, cybersecurity, e metrologia, così da formare una figura professionale che partendo dall'ambito di ricerca sarà in grado di trasferire il know-how acquisito e contribuire all'innovazione nel settore.

c. Cronoprogramma

L'attività di formazione e ricerca associata alla presente proposta di percorso dottorale è strutturata in diverse parti, talvolta consecutive ed altre volte concomitanti, dettagliate qui di seguito. Si elencano anzitutto le attività raggruppate in "work package" proponendone una pianificazione temporale delle stesse all'interno del triennio. Successivamente, si riportano i risultati attesi anno per anno.

WP1 [mesi 1-9]: Analisi dello stato dell'arte su "side-channel attacks".
Queste attività riguarderanno lo studio della letteratura riguardante l'attacco a dispositivi per l'acquisizione e lo scambio di dati di monitoraggio, tipicamente dotati di microcontrollore e con implementati algoritmi di criptaggio delle informazioni. Il focus sarà sulla misurazione di nano-correnti associate al consumo di potenza dei dispositivi e alle tecniche a stato dell'arte per l'analisi

statistica di tali tracce di potenza ai fini di evidenziare una correlazione con le operazioni in corso sui dispositivi stessi.

WP2 [mesi 1-18]: Studio delle recenti tecniche di "machine learning"
Queste attività comprenderanno lo studio teorico e l'applicazione pratica delle recenti tecniche di intelligenza artificiale con possibilità di apprendimento automatico. La base dello studio sarà di stampo statistico, ma si considereranno i framework di apprendimento automatico più avanzati, con riferimento a librerie sviluppate nel comune linguaggio python.

WP3 [mesi 7-12]: Stesura dei requisiti per l'ambito applicativo "agrifood"
Saranno definiti i requisiti di sicurezza per un sistema di trasduttori interconnessi atti al monitoraggio di un sistema agroalimentare, considerando lo stato dell'arte e i desiderata del mercato, e quindi interfacciandosi con i diversi stakeholders della filiera.

WP4 [mesi 10-18]: Progettazione concettuale di un sistema sicuro di trasduttori smart
Si progetterà un sistema di trasduttori intelligenti interconnessi con implementate misure di sicurezza, ovvero contromisure ai side-channel attacks, in accordo con lo stato dell'arte ed i requisiti definiti in precedenza, nonché facendo uso di tecniche avanzate di machine learning.

WP5 [mesi 15-28]: Progettazione fisica di un sistema sicuro di trasduttori smart
Si svilupperà un sistema di trasduttori intelligenti interconnessi con implementate misure di sicurezza, facendo uso di tecniche avanzate di machine learning in accordo con la progettazione concettuale dello stesso, e dunque con lo stato dell'arte ed i requisiti definiti.

WP6 [mesi 25-30]: Quantificazione delle prestazioni
Le diverse componenti del sistema progettato concettualmente e poi fisicamente saranno testate anzitutto singolarmente per valutarne la funzionalità, dopodiché il sistema nel suo complesso sarà caratterizzato metrologicamente per ottenere una quantificazione rigorosa delle prestazioni e verificarne l'aderenza ai requisiti. Laddove necessario, si tornerà alla fase di progettazione per raffinare in sistema in modo da rispettare i requisiti.

WP7[27-36]: Validazione sul campo
Il sistema sarà infine testato sul campo per verificarne l'utilità e l'accettabilità nell'ambito agrifood. Una campagna sperimentale apposita sarà definita e condotta in accordo con esperti del settore e *stakeholders*.

d. Risultati attesi

In accordo con i WP definiti in precedenza, i risultati attesi anno per anno sono riportati di seguito.

Primo anno

- approfondita conoscenza dello stato dell'arte relativo ad attacchi "side-channel";
- padronanza di tecniche avanzate di analisi delle serie temporali basate su "machine learning";
- documento di requisiti del sistema sicuro di trasduttori smart per agrifood;

Secondo anno

- proof of concept del sistema di trasduttori smart;
- valutazione preliminare della funzionalità del sistema;
- pubblicazione a rivista relativa al proof of concept del sistema di trasduttori smart;

Terzo anno

- sistema finale di trasduttori smart con protezione dai cyber-attacchi;
- documento dichiarativo delle prestazioni del sistema;
- sistema validato sul campo con evidenziati i limiti di utilizzo;
- pubblicazione a rivista: sistema di trasduttori utilizzato in ambito agrifood;
- pubblicazione a rivista: caratterizzazione performance metrologiche del sistema.

L'attività di ricerca sarà scandita da periodici traguardi scientifici che consisteranno prevalentemente nella stesura di articoli scientifici indirizzati a riviste di settore. Si prevede un'attività di pubblicazione minima durante il primo anno (dedicato maggiormente alla formazione del candidato), e via via crescente nel raggiungimento del terzo anno del percorso dottorale. Il numero minimo di pubblicazioni a rivista previste nel triennio è pari a tre. Le riviste destinatarie saranno scelte con riferimento agli indici bibliometrici SJR (Scimago Journal Ranking) ed IF (Impact Factor). Saranno inoltre considerate prevalentemente riviste nel primo quartile (Q1) per ambiti quali "Instrumentation", "Computer Science Applications", "Computer Networks and Communications", "Signal processing", "Artificial Intelligence", "Food science" ed affini.
In aggiunta alle pubblicazioni a riviste, si prevedono pubblicazioni in atti di congresso associate alle attività di comunicazione descritte nel seguito, e quantificabile nella partecipazione a circa due congressi per anno.
Non è attualmente prevista una attività brevettuale. Si prevede invece la partecipazione a bandi nazionali e/o europei perché i prototipi di sistemi ed algoritmi sviluppati come prodotti della ricerca possano essere portati ad un livello di sviluppo più alto grazie a maggiori risorse umane ed economiche.

e. Impresa

Durante l'attività di dottorato è previsto un periodo in azienda di circa sei mesi, presso Officina Elettronica, con sede operativa presso il palazzo ICE-SNEI di via Diocleziano, 107, scala B, int 506, 80125 Napoli. Alcune delle attività di tale impresa comprendono l'impiego di microprocessori e microcontrollori in diversi settori dell'elettronica, la raccolta e memorizzazione locale o remota di dati tramite terminali di rete con possibilità di accesso via web, e la progettazione, realizzazione e manutenzione di reti di telecomunicazione.
Durante tale periodo sarà dunque progettato, prima concettualmente e poi fisicamente, il sistema sicuro di trasduttori *smart* nel rispetto delle specifiche di sistema definite in precedenza. In accordo con il cronoprogramma definito per il progetto presente, il periodo in azienda sarà da svolgersi tra i mesi 13 e 18 nel triennio del percorso dottorale.

f. Istituzione ospitante all'estero

Facoltativamente sarà possibile svolgere un'attività estera per il raffinamento della formazione del candidato e lo svolgimento di un'attività di ricerca in ambiente internazionale. Tale attività avrebbe una durata orientativa di circa 6 mesi e verrebbe svolta presso la School of Computing and Information Technology dell'Università di Wollongong (Australia) di comune accordo con il prof. Willy Susilo, esperto di crittografia, cybersecurity e sicurezza delle reti.

g. Prodotti misurabili della ricerca, comunicazione e disseminazione

La comunicazione dell'attività di ricerca inerente al percorso dottorale sarà opportunamente divulgata, in aggiunta alle pubblicazioni scientifiche su riviste di settore, con presentazioni a congressi e seminari. Si prevede la partecipazione a circa due congressi all'anno, di cui un congresso di stampo generalista (come ad esempio la "IEEE International Instrumentation and

Measurement Technology Conference" come conferenza di punta in campo metrologico) ed un congresso specializzato in ambito cybersecurity e/o agrifood.
Questo permetterà la divulgazione dei risultati nei vari ambiti di interesse, ovvero all'interno della comunità metrologica, nell'ambito cybersecurity, tra i gruppi di ricerca in applicazioni di intelligenza artificiale, nonché nella ricerca associata al settore agroalimentare. La partecipazione a congressi e seminari favorirà anche la discussione con esperti dei vari settori interessati ai fini di una condivisione di conoscenze, metodi, strumenti, e soluzioni.
Sarà infine considerata la divulgazione dei risultati della ricerca sulle comuni piattaforme di social networking ai fini di diffondere una maggiore consapevolezza sulla tematica ad un pubblico più vasto.