PIANO TRIENNALE DI REALIZZAZIONE 2022-24 - RICERCA DI SISTEMA ELETTRICO NAZIONALE
Progetti di ricerca di cui all'art. 10 comma 2, lettera a) del decreto 26 gennaio 2000

AFFIDATARIO ENEA

Tema 2.1 – Cybersecurity dei sistemi energetici

Durata: 36 Mesi

Semestre n. 6 – Periodo attività: 01/07/2024 – 31/12/2024

ABSTRACT ATTIVITA' SEMESTRALE:

Il presente documento descrive le attività di ricerca del progetto “Cybersecurity dei sistemi energetici” svolte da ENEA e dai propri co-beneficiari durante il sesto semestre di progetto.

Le attività di ricerca hanno riguardato le seguenti Linee di Attività:

- ENEA (affidatario del progetto) per LA1.6, LA2.7, LA3.4, LA3.7; LA3.8; LA3.13; LA4.5;
- UniPD-QTech (cobeneficiario del progetto) per LA1.7 e LA1.8;
- UNINA-FISICA (cobeneficiario del progetto) per LA1.9 e LA1.10;
- ROMA1-DIET (cobeneficiario del progetto) per la LA1.11;
- ROMA3-DICITA (cobeneficiario del progetto) per LA3.9;
- UNIBA (cobeneficiario del progetto) per LA3.10;
- DIG-UNISANNIO (cobeneficiario del progetto) per LA3.12.

AFFIDATARIO / COBENEFICIARIO	SINTESI DELLE ATTIVITÀ DI RICERCA SVOLTE E DEI RISULTATI CONSEGUITI
ENEA	<p>Nell'ambito del presente semestre, ENEA ha condotto attività di ricerca relativamente alle seguenti linee di attività: LA1.6, LA2.7, LA3.4, LA3.7; LA3.8; LA3.13; LA4.5.</p> <p>Con riferimento alla Linea di Attività LA1.6 “Valutazione della cyber-vulnerabilità di microreti elettriche dotate di apparati e tecnologie di comunicazione, monitoraggio, gestione e test degli interventi mitigativi”, nel semestre in corso sono stati eseguiti i penetration test (PET) su ciascun apparato precedentemente selezionato.</p> <p>Per ogni dispositivo sono stati condotti test di penetrazione, analizzati i risultati e formulate proposte di azioni mitigative. Al fine di sintetizzare i risultati sperimentali, sono stati definiti specifici KPI (Key Performance Indicators) e assegnato a ciascun apparato un valore numerico rappresentativo del livello di vulnerabilità.</p> <p>I risultati ottenuti hanno evidenziato che, sebbene la maggior parte dei dispositivi commerciali testati presenti una difesa strutturata contro gli</p>

attacchi cibernetici, permangono alcune vulnerabilità associate a vie di accesso non completamente protette. Tali varchi corrispondono a porte di comunicazione su cui operano servizi necessari allo scambio di dati con l'esterno. L'azione mitigativa proposta consiste nel contestualizzare l'impiego del dispositivo e valutare, nell'ambito dell'applicazione specifica, se sia effettivamente necessario mantenere attive tali porte. La loro apertura, infatti, comporta il posizionamento del dispositivo al di fuori di una trusted area. Qualora l'apertura risulti indispensabile, si suggerisce l'adozione di misure di protezione aggiuntive, come ad esempio l'implementazione di accessi crittografati.

L'intera attività si è svolta in conformità con quanto previsto dal capitolato, senza registrare scostamenti, e ha raggiunto tutti gli obiettivi prefissati.

Nel corso del semestre è stato redatto il rapporto tecnico relativo alle attività svolte nell'ambito della LA:

- *Rapporto Tecnico RdS_PTR22-24_PR 2.1_LA1.6_128 «Valutazione della cyber-vulnerabilità di microreti elettriche dotate di apparati e tecnologie di comunicazione, monitoraggio, gestione e test degli interventi mitigativi».*

Per ciò che concerne la **LA2.7 “Implementazione di uno schema di protezione e sviluppo di un prototipo per la mitigazione degli effetti connessi ai cyber-attacchi in ottica di incremento della cyber-resilienza delle reti e delle microreti elettriche”**, nel presente semestre sono stati eseguiti i test per la validazione sperimentale del prototipo sviluppato nell'ambito del quinto semestre.

La verifica del corretto funzionamento del dispositivo è stata effettuata mediante la configurazione del test-bed definito nell'ambito della Linea di Attività LA1.2 e implementato presso il laboratorio SGRE del Centro Ricerche ENEA di Portici. Per consentire la connessione del test-bed a reti sintetiche, sia di tipo radiale che con topologia ad anello, è stato utilizzato un sistema Hardware In the Loop (HIL). Le connessioni degli apparati inclusi nel test-bed, variabili di volta in volta, ai bus disponibili nel laboratorio SGRE sono state configurate tramite il tool Powerlab, strumento software dedicato alla gestione degli apparati sperimentali.

L'intera attività si è svolta in conformità con quanto previsto dal capitolato, senza registrare scostamenti, e ha raggiunto tutti gli obiettivi prefissati.

Nel corso del semestre sono stati redatti sia il rapporto tecnico sulle attività svolte nell'ambito della LA, sia quello descrittivo relativo al prototipo elettrico-cibernetico realizzato:

- *Rapporto Tecnico RdS_PTR22-24_PR 2.1_LA2.7_136 «Implementazione di uno schema di protezione per la mitigazione degli effetti connessi ai cyber-attacchi in ottica di incremento della cyber-resilienza delle reti e delle microreti elettriche».*
- *Prototipo RdS_PTR22-24_PR 2.1_LA2.7_137*

Con riferimento alla Linea di Attività **LA3.4 “Implementazione di un'infrastruttura di calcolo a basso consumo per il controllo informatico delle reti elettriche intelligenti cyber-resilienti”**, nel sesto semestre è stata

effettuata l'installazione e configurazione di un nodo Elasticsearch, finalizzata a garantire una rapida ed efficace indicizzazione dei dati, nonché la loro storicizzazione. Parallelamente, è stato fornito supporto alla definizione del framework privacy, volto ad assicurare la conformità del processo di elaborazione dei dati di traffico alle normative europee vigenti in materia di protezione dei dati personali. La raccolta e la successiva post-elaborazione dei dati di traffico provenienti dalle reti informatiche dei Centri ENEA di Casaccia e Portici ha evidenziato la necessità di affrontare con attenzione le implicazioni legate alla riservatezza delle informazioni. Per rispondere a questa esigenza, in collaborazione con il Data Protection Officer dell'ENEA, è stata condotta un'analisi approfondita degli impatti privacy, accompagnata dalla redazione del documento di Data Protection Impact Assessment (DPIA) e del relativo allegato tecnico. Questa attività riveste un'importanza strategica non solo per garantire la conformità normativa, ma anche per rafforzare la fiducia degli stakeholder e assicurare la sostenibilità etica e legale delle soluzioni tecnologiche adottate. La corretta gestione dei dati sensibili, infatti, rappresenta un elemento chiave per l'adozione su larga scala di infrastrutture digitali nelle reti elettriche intelligenti.

L'intera attività si è svolta in conformità con quanto previsto dal capitolato, senza registrare scostamenti, e ha raggiunto tutti gli obiettivi prefissati.

Nel corso del semestre è stato infine redatto il rapporto tecnico relativo alle attività svolte nell'ambito della LA:

- *Rapporto Tecnico RdS_PTR22-24_PR2.1_LA3.4_138 «Implementazione di una infrastruttura di calcolo a basso consumo per il controllo informatico delle reti elettriche intelligenti cyber-resilienti».*

Con riferimento alla Linea di Attività **LA3.7 "Realizzazione e implementazione su un caso d'uso di una piattaforma di stream analytics e implementazione delle logiche di training e inference dei modelli di Machine Learning e Artificial Intelligence su acceleratori di varia natura (FPGA/GPU)"**, nel semestre in esame le attività si sono concentrate sull'individuazione di una dashboard con interfaccia grafica semplice e intuitiva, in grado di gestire efficacemente i singoli componenti del sistema e di garantirne scalabilità e replicabilità.

La dashboard di monitoraggio e gestione rappresenta un elemento chiave per la visualizzazione e il controllo del cluster Kubernetes, semplificando operazioni che - se eseguite da riga di comando - risulterebbero più complesse e meno accessibili. A tal fine, è stato adottato Lens, un'interfaccia grafica open-source progettata per offrire una visione chiara e dettagliata delle risorse, delle configurazioni e dello stato delle applicazioni attive nel cluster. Tramite Lens è possibile esplorare il cluster, visualizzare i dettagli dei pod, configurare le applicazioni in esecuzione, risolvere eventuali problemi e monitorare le prestazioni dei singoli componenti.

Durante la fase di realizzazione del progetto si sono verificati alcuni scostamenti tecnici. In particolare, non è stato possibile formalizzare una consulenza esterna per lo sviluppo della dashboard, a causa di vincoli organizzativi e delle tempistiche ristrette. Questo ha comportato una riorganizzazione del lavoro, con un ricorso prevalente a software open-source

per la realizzazione dei componenti e l'installazione di un orchestratore di container, utile a facilitare la comunicazione tra i vari elementi del sistema. La soluzione adottata ha permesso di ottenere un sistema IT scalabile e replicabile, capace di analizzare i dati provenienti dalle sorgenti di rete con semplicità ed efficienza. Un ulteriore scostamento tecnico ha riguardato la scelta di non utilizzare acceleratori hardware specializzati (GPU/FPGA) per il training dei modelli. I test condotti hanno infatti evidenziato che tali risorse non offrivano vantaggi significativi in termini di prestazioni sugli algoritmi considerati. Di conseguenza, si è optato per escludere temporaneamente questi acceleratori, favorendo una maggiore semplicità di replica e scalabilità del sistema.

Questa attività ha contribuito alla realizzazione di un'infrastruttura flessibile e adattabile, capace di supportare l'analisi in tempo reale dei dati di rete e l'implementazione di modelli intelligenti, pur mantenendo contenuti i costi e la complessità operativa. Le soluzioni tecniche adottate hanno consentito di superare gli scostamenti iniziali senza compromettere il raggiungimento degli obiettivi previsti dalla Linea di Attività, tutti pienamente conseguiti.

Nel corso del semestre è stato infine redatto il rapporto tecnico relativo alle attività svolte nell'ambito della LA:

- *Rapporto Tecnico RdS_PTR22-24_PR2.1_LA3.7 «Realizzazione e implementazione su un caso d'uso di una piattaforma di stream analytics e implementazione delle logiche di training e inference dei modelli di ML e Artificial Intelligence su acceleratori di varia natura».*

Nell'ambito della **LA3.8 "Test dell'infrastruttura di calcolo a basso consumo per il controllo informatico smart di reti cyber-resilienti"** il sesto semestre è stato focalizzato sulla implementazione di procedure di test per misurare le bande di comunicazione e le latenze nel server di calcolo.

A tal fine, ci si è concentrati sulla velocità di trasferimento dei dati all'interno del sistema, misurando la banda di comunicazione ([B/s]) e le latenze ([s]) nei diversi percorsi di accesso ai dati. In particolare, sono state analizzate le seguenti configurazioni dell'infrastruttura di calcolo HPC a basso consumo per il controllo informatico smart di reti cyber-resilienti del processore ai dati:

- Trasferimento tra processore e i vari livelli della gerarchia di memoria: lettura/scrittura verso dati residenti in L1, L2, L3 o nella memoria DDR del nodo host. Per questa misura è stato sviluppato del codice ad hoc.
- Trasferimento tra memoria host e scheda FPGA: lettura/scrittura dalla memoria DDR del processore verso i dati situati nella memoria (HBM o DDR) delle schede acceleratrici FPGA. Per i valori di banda si è utilizzata la funzionalità "xbutil examine" fornita da Amd; per la misura delle latenze si è sviluppato un codice dedicato
- Accesso dalla FPGA ai suoi banchi di memoria (DDR/HBM): lettura/scrittura verso i banchi di memoria HBM o DDR presenti sulla scheda FPGA. Per i valori di banda si è utilizzata la funzionalità "xbutil examine" fornita da Amd; per la misura delle latenze si è sviluppato un codice dedicato, implementando opportuni kernel su FPGA

Infine, nel presente semestre è stato eseguito il test del cavo crittato realizzato nella LA1.11 dalla Sapienza Università di Roma, mediante comunicazioni tra il

server di calcolo SuperMicro, situato presso il centro ENEA di Casaccia, e un nodo di calcolo nella rete di Portici. Le comunicazioni sono state cifrate utilizzando l'algoritmo QP-DYN, implementato su FPGA.

Durante la fase realizzativa del progetto si sono verificati alcuni scostamenti tecnici rispetto a quanto inizialmente pianificato. In particolare, tra i criteri stabiliti per valutare il conseguimento degli obiettivi, era previsto che il Rapporto Tecnico includesse una descrizione dettagliata dei test condotti per verificare la funzionalità di tutti i componenti dell'infrastruttura digitale realizzata. Tali test avrebbero dovuto comprendere prove specifiche sulle procedure di comunicazione, sui singoli moduli hardware e software, sulle interdipendenze tra i componenti e sull'infrastruttura nel suo complesso, oltre ai risultati delle misure effettuate. Tuttavia, nel corso dell'implementazione si è scelto di adottare un approccio differente, privilegiando l'utilizzo di test funzionali complessivi dell'architettura, secondo un modello di tipo black-box. In tal senso, la verifica del corretto funzionamento dell'infrastruttura hardware/software è stata basata sull'analisi dei risultati prodotti, piuttosto che sull'esame interno dei singoli componenti e delle loro interazioni. La scelta di non implementare "unit test" è derivata dalla constatazione che molte delle funzionalità risultano già integrate nei software utilizzati, rendendo poco praticabile l'utilizzo di test unitari. Le soluzioni tecniche adottate hanno comunque permesso di superare gli scostamenti iniziali, senza compromettere il raggiungimento degli obiettivi previsti dalla Linea di Attività, che sono stati tutti pienamente conseguiti.

Nel corso del semestre è stato infine redatto il rapporto tecnico relativo alle attività svolte nell'ambito della LA:

- *Rapporto Tecnico Rds_PTR22-24_PR2.1_LA3.8_142 «Test dell'infrastruttura di calcolo HPC a basso consumo per il controllo informatico smart di reti cyber-resilienti».*

La **LA3.13 "Validazione ed Integrazione in piattaforma di un toolset di rivelazione attacchi nel contesto delle microreti elettriche"**, nel sesto semestre, l'attività si è concentrata sulla validazione dei componenti progettati per l'integrazione nella piattaforma di analisi degli stream di dati misurati. Tale validazione è stata condotta all'interno di un ambiente dedicato, definito e segregato funzionalmente rispetto alla piattaforma operativa, al fine di garantire affidabilità e riproducibilità dei test. L'ambiente di test è stato caratterizzato dal deployment di circa 100 smart meter commerciali, installati presso il Centro Ricerche ENEA di Portici, utilizzati per la misura delle grandezze elettriche dei sistemi monitorati. L'acquisizione dei dati è stata strutturata in modalità centralizzata, con un dispositivo edge configurato come nodo di raccolta principale. Per supportare il flusso dati, è stato disegnato e implementato un sistema di relay che consente l'acquisizione, tramite broker MQTT, dei dati provenienti dagli smart meter, rendendoli disponibili per l'elaborazione e l'analisi all'interno della piattaforma.

La validazione ha riguardato sia la correttezza funzionale dei componenti sviluppati sia la robustezza del sistema di acquisizione.

L'intera attività si è svolta in conformità con quanto previsto dal capitolato, senza registrare scostamenti, e ha raggiunto tutti gli obiettivi prefissati. Nel corso del semestre sono stati redatti anche i due rapporti tecnici di sintesi delle attività svolte nella LA:

- *Rapporto Tecnico RdS_PTR22-24_PR2.1_LA3.13_149 «Componenti per il sistema integrato di rilevazione delle anomalie gerarchiche».*
- *Rapporto Tecnico RdS_PTR22-24_PR2.1_LA3.13_150 «Validazione ed integrazione in piattaforma di un toolset di rivelazione attacchi nel contesto delle microreti elettriche».*

Insieme ai due rapporti tecnici è stato altresì rilasciato il software sviluppato (Componenti per il sistema integrato di rilevazione delle anomalie gerarchiche).

- *Software: «Componenti per il sistema integrato di rilevazione delle anomalie gerarchiche».*

La **LA4.5 “Attività di diffusione II SAL”** ha come obiettivo la divulgazione dei risultati di progetto conseguiti da ENEA e dai relativi co-beneficiari. Nel sesto semestre, in particolare, sono proseguite le iniziative di divulgazione scientifica e confronto con la comunità di esperti, con l'obiettivo di promuovere i risultati del Progetto 2.1 e rafforzarne l'impatto nel contesto della cybersecurity applicata al settore energetico. Più nello specifico:

- **Ottobre 2024:** le attività condotte da ENEA sono state presentate durante la Sessione sulla Cyber Security nel settore energetico, organizzata dal CNR in occasione del Cybersecurity Day. La sessione, strutturata come dibattito aperto e interattivo, ha rappresentato un'importante occasione di confronto con esperti del settore, istituzioni e stakeholder. L'approccio dialogico ha permesso di illustrare i principali risultati e obiettivi del progetto, raccogliendo al contempo feedback preziosi da parte del pubblico, utili per orientare le attività future e rafforzare l'efficacia delle soluzioni proposte. Il confronto ha evidenziato un interesse crescente verso le tematiche di sicurezza informatica applicata all'energia, confermando la rilevanza strategica del progetto nel quadro della transizione digitale del settore.
- **Settembre 2024:** i risultati del Progetto 2.1 sono stati divulgati nella sessione tematica “Novel methodologies, models, and solutions for secure and cyber-resilient smart grids and multi-carrier energy systems”, organizzata da ENEA all'interno della conferenza NanoInnovation 2024, svoltasi dal 9 al 13 settembre presso la Sapienza Università di Roma. Durante la sessione, la ricercatrice Giovanna Adinolfi ha presentato il contributo “Innovative Devices for Electric and Cyber Security in Distribution Grids”, focalizzato sullo sviluppo di un prototipo innovativo per la protezione cibernetica delle reti di distribuzione elettrica. Il dispositivo integra soluzioni avanzate per la sicurezza elettrica e informatica, con l'obiettivo di aumentare la cyber-resilienza delle infrastrutture energetiche in scenari sempre più digitalizzati e interconnessi. La presentazione ha suscitato notevole interesse tra i partecipanti, grazie all'approccio multidisciplinare adottato e alle potenzialità applicative del prototipo, confermando il ruolo strategico

	<p>della ricerca pubblica nello sviluppo di tecnologie per la cybersecurity energetica.</p> <ul style="list-style-type: none"> • 6 dicembre 2024: presso l’Auditorium del GSE a Roma, si è tenuto il workshop “La cybersecurity dei sistemi energetici”, organizzato nell’ambito della Ricerca di Sistema Elettrico, con il coinvolgimento di RSE (coordinatore), ENEA e CNR. Il workshop ha rappresentato un’importante occasione di confronto tra enti di ricerca, istituzioni e stakeholder del settore energetico, finalizzata alla presentazione dei risultati del Progetto Integrato Cybersecurity dei Sistemi Energetici e alla promozione delle soluzioni innovative per la protezione delle infrastrutture critiche sviluppate nell’ambito del progetto. ENEA, insieme ai propri co-beneficiari, ha contribuito con sette presentazioni tematiche, oltre a una presentazione di inquadramento generale delle attività svolte nel contesto del progetto. <p>In parallelo, sono proseguite le attività di disseminazione scientifica attraverso la pubblicazione di articoli, contribuendo alla valorizzazione dei risultati ottenuti e al rafforzamento del ruolo strategico del progetto nella ricerca sulla cybersecurity in ambito energetico. Nel corso del triennio, ENEA e i propri co-beneficiari hanno pubblicato complessivamente dieci articoli scientifici.</p> <p>L’intera attività si è svolta in conformità con quanto previsto dal capitolato, senza registrare scostamenti, e ha raggiunto tutti gli obiettivi prefissati.</p> <p>Nel corso del semestre è stato redatto il rapporto tecnico di sintesi delle attività svolte nella LA:</p> <ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR 22-24_PR 2.1_LA4.5_152 «Resoconto delle attività di diffusione relative al SAL 2)».</i>
<p>UniPD-QTech</p>	<p>Nel periodo di riferimento, UniPD-QTech è stata impegnata nelle attività relative a LA1.7 e LA1.8.</p> <p>Con riferimento alla linea di attività LA1.7, “Definizione e implementazione sperimentale di un protocollo quantistico di autenticazione di un comando a distanza con l’obiettivo di incremento della cyber-sicurezza delle reti energetiche”, nel sesto semestre sono stati condotti test pratici utilizzando il sistema IDQ Clavis XGR, finalizzati alla verifica della soglia di Quantum Bit Error Rate (QBER).</p> <p>Le attività hanno previsto la simulazione della risposta della rete in presenza di tentativi di compromissione, verificando l’efficacia del meccanismo di blocco automatico della generazione delle chiavi, a tutela dell’integrità del sistema. Quale metrica per la valutazione sperimentale di robustezza dei dispositivi QKD agli attacchi è stato usato il Quantum Bit Error Rate (QBER). In particolare, è stata impostata una soglia di QBER pari all’1%, al fine di facilitare l’identificazione di eventuali tentativi di attacco. I test condotti hanno confermato l’efficacia in termini di sicurezza della trasmissione delle chiavi.</p> <p>Nel corso dell’attività LA1.7 sono emersi alcuni scostamenti, di seguito evidenziati. Durante la fase di realizzazione del progetto, sono stati acquisiti dispositivi commerciali per la Quantum Key Distribution (QKD), che hanno fornito una solida base protocollare su cui costruire il framework previsto dalla linea LA1.7. Di conseguenza, non è stato necessario sviluppare un protocollo</p>

	<p>QKD ad hoc; l'attività si è invece concentrata sull'ottimizzazione dell'integrazione dei sistemi QKD all'interno della rete ENEA. Tale approccio non ha compromesso il raggiungimento degli obiettivi previsti dalla Linea di Attività, che sono stati tutti pienamente conseguiti.</p> <p>Nel corso del semestre è stato infine redatto il rapporto tecnico relativo alle attività svolte nell'ambito della LA:</p> <ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR22-24_PR2.1_LA1.7_129 «Definizione e implementazione sperimentale di un protocollo quantistico di autenticazione di un comando a distanza con l'obiettivo di incremento della cyber-sicurezza delle reti elettriche».</i> <p>Per ciò che concerne la LA1.8 "Individuazione dei modelli di rete QKD appropriati per servire le necessità più rilevanti per le architetture di sistemi energetici", nel presente semestre è stata studiata l'integrazione di protocolli QKD multiterminale al fine di superare le limitazioni della configurazione point-to-point adottata.</p> <p>In particolare, si è studiata la possibilità di introdurre switch ottici per permettere la distribuzione delle chiavi a più nodi in modo simultaneo. Questo approccio, sebbene promettente, non è stato ancora implementato a causa della complessità tecnica e della necessità di utilizzare sistemi QKD di diversi fornitori per garantire l'interoperabilità.</p> <p>Nel complesso, il progetto ha dimostrato la fattibilità dell'implementazione di una rete QKD per la protezione delle reti elettriche, fornendo specifiche dettagliate per la gestione delle chiavi crittografiche e le connessioni di scambio chiave. Le simulazioni e i test effettuati hanno confermato la validità dell'approccio scelto, evidenziando al tempo stesso le sfide legate alla scalabilità e all'ottimizzazione delle risorse. Le conoscenze acquisite in questa fase saranno fondamentali per futuri sviluppi del sistema, con particolare attenzione all'integrazione di soluzioni multiterminali più avanzate.</p> <p>L'attività non ha registrato scostamenti, e ha raggiunto tutti gli obiettivi prefissati.</p> <p>Nel corso del semestre è stato infine redatto il rapporto tecnico relativo alle attività svolte nell'ambito della LA:</p> <ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR 22-24_PR 2.1_LA1.8_131 «Studio e progettazione della tipologia di network di quantum key distribution finalizzato alla definizione di key-management-system e connessioni scambio chiave per l'ottimizzazione della cyber-sicurezza delle reti elettriche».</i>
<p>UNINA-FISICA</p>	<p>Nel periodo di riferimento, UNINA-FISICA è stata impegnata nelle attività relative a LA1.9 e LA1.10.</p> <p>Con riferimento alla LA1.9 "Progettazione e sviluppo di schemi di cyber difesa delle reti elettriche tramite Quantum Secure Direct Communication assistita da Quantum Machine Learning" nel presente semestre è stato completato lo sviluppo degli algoritmi avviato nel quinto semestre. In particolare, sono stati realizzati due algoritmi efficienti per l'apprendimento della classe, completamente generale, degli stati stabilizzatori t-doped. Questo risultato</p>

	<p>consente di apprendere le mappe unitarie che generano tali stati, ovvero i circuiti unitari t-doped di tipo Clifford. I risultati ottenuti sono stati successivamente estesi per includere anche l'apprendimento di mappe dissipative e non unitarie, ampliando così il campo di applicazione degli algoritmi sviluppati.</p> <p>L'attività si è svolta secondo quanto pianificato, senza registrare scostamenti, e ha raggiunto tutti gli obiettivi prefissati. Nel semestre, è stato anche redatto il rapporto tecnico relativo alle attività svolte:</p> <ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR22-24_PR2.1_LA1.9_132 «Progettazione e sviluppo di schemi di cyber difesa di reti tramite quantum secure direct communication assistita da quantum machine learning».</i> <p>Per quanto riguarda la linea di attività LA1.10, "Emulazione e test degli schemi di cyber difesa delle reti elettriche tramite Quantum Secure Direct Communication assistita da Quantum Machine Learning", il semestre è stato principalmente dedicato all'analisi dei risultati delle misure sperimentali. I dati raccolti sono stati confrontati con i modelli teorici, evidenziando un'eccellente corrispondenza tra le previsioni e le osservazioni sperimentali.</p> <p>Durante lo svolgimento delle attività sono stati rilevati alcuni scostamenti rispetto al piano iniziale. In origine, era previsto il test dei modelli teorici su dispositivi NISQ commerciali, come Amazon Braket e IBM Quantum Falcon. Tuttavia, la disponibilità di un prototipo interno ha determinato una riorganizzazione delle risorse, orientando l'attività verso misure su singolo qubit. Questo approccio alternativo ha offerto vantaggi significativi in termini di accessibilità e controllo diretto sulle risorse computazionali, risultando particolarmente efficace per la validazione dei modelli teorici.</p> <p>Nonostante tali variazioni, tutti gli obiettivi previsti dalla linea di attività sono stati pienamente raggiunti. Nel semestre, è stato anche redatto il rapporto tecnico relativo alle attività svolte nell'ambito della LA:</p> <ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR 22-24_PR 2.1_LA1.10_133 «Emulazione e testing degli schemi di cyber difesa di reti tramite quantum secure direct communication assistita da quantum machine learning».</i>
<p>ROMA1-DIET</p>	<p>Nel periodo di riferimento, ROMA1-DIET è stata impegnata nelle attività relative alla LA1.11.</p> <p>Per quanto riguarda la linea di attività LA1.11, "Implementazione efficiente su logiche programmabili di primitive crittografiche per la sintesi di funzioni di cifratura a flusso e autenticazione", il semestre è stato dedicato allo sviluppo e alla sperimentazione della comunicazione sicura tra due utenti, basata su algoritmi crittografici implementati su logiche programmabili. L'attività ha previsto l'implementazione, in ambiente Xilinx Vivado, dell'algoritmo crittografico QP-Dyn, selezionato nel precedente semestre. Questo algoritmo si basa sull'interazione di due sistemi dinamici, MA e MB, combinati mediante operazione XOR. Parallelamente, è stato sviluppato in ambiente VITIS il sistema di comunicazione tra due utenti, che scambiano dati cifrati attraverso l'interfaccia AXI-Stream.</p>

	<p>Gli algoritmi e l'ambiente di comunicazione sono stati inizialmente testati su FPGA Xilinx XC7Z020. Successivamente, è stata realizzata una codifica e trasmissione tra due nodi della rete ENEA, utilizzando schede U280: il nodo codificatore è stato installato presso la sede di Casaccia, mentre il nodo decodificatore è stato configurato presso la sede di Portici.</p> <p>L'attività si è svolta in conformità con quanto previsto dal capitolato, senza registrare scostamenti, e ha portato al pieno raggiungimento degli obiettivi prefissati.</p> <p>Nel semestre sono stati redatti i rapporti tecnici di sintesi delle attività svolte:</p> <ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR22-24_PR 2.1_ LA1.11_134: «Preselezione degli algoritmi di cifratura ed autenticazione».</i> • <i>Rapporto Tecnico RdS_PTR22-24_PR 2.1_ LA1.11_135: «Implementazione efficiente su logiche programmabili di primitive crittografiche per la sintesi di funzioni di cifratura a flusso e autenticazione».</i>
<p>ROMA3-DICITA</p>	<p>Nel periodo di riferimento, ROMA3-DICITA è stata impegnata nelle attività relative alla LA3.9.</p> <p>Per ciò che concerne la LA3.9 “Progettazione e implementazione di un sistema di raccolta, conservazione e analisi di flussi di dati per la cybersicurezza delle reti di sensori”, nel presente semestre sono state svolte le seguenti attività:</p> <ul style="list-style-type: none"> • Formazione del modello: I dati, pre-elaborati nel precedente semestre, sono stati utilizzati per addestrare un modello autoencoder. L'architettura dell'autoencoder è stata progettata con strati densi, utilizzando la funzione di attivazione ReLU per gli strati intermedi e la sigmoid per lo strato di uscita. Durante l'addestramento, il modello ha imparato a rappresentare i normali modelli di traffico, minimizzando l'errore di ricostruzione tra i dati di ingresso e di uscita. • Rilevamento delle anomalie: Una volta addestrato, l'autoencoder è stato applicato a dati di prova contenenti traffico normale e dannoso. Calcolando gli errori di ricostruzione per ogni record, sono state identificate deviazioni significative dai modelli normali appresi come potenziali attacchi. È stata determinata una soglia utilizzando la curva ROC (Receiver Operating Characteristic), bilanciando i tassi di veri positivi e falsi positivi. • Valutazione delle prestazioni: Le prestazioni del modello sono state valutate utilizzando diverse metriche. La matrice di confusione ha fornito una ripartizione dettagliata dei risultati della classificazione, distinguendo tra veri positivi, veri negativi, falsi positivi e falsi negativi. Dalla matrice di confusione sono state ricavate altre metriche, come la precisione e il richiamo (recall). I rapporti di classificazione offrono un riepilogo completo delle principali metriche di prestazione del modello. <p>Il lavoro svolto ha evidenziato il potenziale del deep learning nel rafforzamento della cybersicurezza delle reti, dimostrando la capacità del modello sviluppato di rilevare in modo efficace le anomalie nel traffico di rete reale.</p>

	<p>La linea di attività LA3.9 ha registrato solo lievi scostamenti rispetto alla pianificazione iniziale. In particolare, non è stato approfondito l'utilizzo di un knowledge graph come supporto all'attività di apprendimento del modello di machine learning. Questo strumento, concepito per rappresentare in modo astratto e strutturato le componenti coinvolte nel processo di analisi, avrebbe potuto arricchire ulteriormente il contesto informativo del sistema. Tuttavia, l'assenza di tale componente non ha compromesso il raggiungimento degli obiettivi previsti. Al contrario, l'approccio basato esclusivamente sui dati ha prodotto risultati superiori alle aspettative in termini di efficienza del modello. Il knowledge graph rimane comunque un elemento di valore, soprattutto per la documentazione dell'applicazione, offrendo una rappresentazione di alto livello dei fattori che concorrono all'analisi dei fenomeni di intrusione informatica nel contesto applicativo del progetto.</p> <p>Nel semestre sono stati redatti i rapporti tecnici di sintesi delle attività svolte:</p> <ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR 22-24_PR 2.1_LA3.9_143: «Progettazione e implementazione di un sistema di raccolta, conservazione e analisi di flussi di dati per la cybersicurezza delle reti di sensori».</i> • <i>Rapporto Tecnico RdS_PTR 22-24_PR 2.1_LA3.9_144: «Sistema di raccolta, conservazione e analisi di flussi di dati per la cybersicurezza delle reti di sensori».</i> <p>Insieme ai due rapporti tecnici è stato altresì rilasciato il software sviluppato</p> <ul style="list-style-type: none"> • <i>RT_LA3.9_ENEA_C: Prototipo del sistema.</i>
<p>UNIBA</p>	<p>Nel periodo di riferimento, UNIBA è stata impegnata nelle attività relative alla LA3.10.</p> <p>Per quanto riguarda la linea di attività LA3.10, "Sviluppo ed implementazione di metodi di Machine Learning supervisionati e non supervisionati per lo studio delle anomalie", nel presente semestre sono stati sviluppati modelli di machine learning, sia supervisionati che non supervisionati, per l'analisi dei dati di traffico messi a disposizione. In particolare, sono stati realizzati due modelli supervisionati finalizzati all'identificazione di minacce di tipo DoS, simulate da ENEA e rilevate tramite il software di monitoraggio delle connessioni. I modelli si basano su tecniche di ensemble learning con alberi decisionali, utilizzando gli algoritmi Random Forest (RF) ed Extreme Gradient Boosting (XGBoost). Parallelamente, è stato sviluppato un modello non supervisionato basato sull'algoritmo DBSCAN, che consente di raggruppare eventi simili in cluster, sfruttando la densità dei dati nello spazio delle feature. I modelli sono stati integrati nei sistemi ENEA e implementati sulle macchine ENEA, contribuendo al sistema di rilevamento degli attacchi attraverso l'esecuzione di script sviluppati in linguaggio R.</p> <p>L'attività si è svolta in conformità con quanto previsto dal capitolato, senza registrare scostamenti e raggiungendo tutti gli obiettivi prefissati.</p> <p>Nel semestre sono stati redatti i rapporti tecnici di sintesi delle attività svolte:</p> <ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR 22-24_PR 2.1_LA3.10_146: «Sviluppo ed implementazione di metodi di Machine Learning supervisionati e non supervisionati per lo studio delle anomalie».</i>

	<ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR 22-24_PR 2.1_LA3.10_147: «Schema degli algoritmi di clustering da utilizzare per la protezione da cyber-minacce».</i>
<p>DIG-UNISANNIO</p>	<p>Nel periodo di riferimento, DIG-UNISANNIO è stata impegnata nelle attività relative alla LA3.12.</p> <p>Per ciò che concerne la LA3.12 “Sviluppo e confronto prestazionale di algoritmi di rilevamento stocastico di cyber-attacchi nel contesto delle microreti elettriche”, nel presente semestre sono state valutate le prestazioni dell’algoritmo selezionato precedente semestre.</p> <p>Per quantificare le prestazioni dell’algoritmo nel rilevamento delle anomalie, sono state adottate metriche standard come Silhouette Score (utilizzato per valutare la qualità dei cluster ottenuti e Davies-Bouldin Index (utilizzato per valutare la separazione dei cluster ottenuti). Sono state inoltre considerate metriche tipiche dell’anomaly detection come Accuracy, Precision, Recall ed F1-Score.</p> <p>Queste misure hanno permesso di quantificare l’efficacia del modello nel rilevare le anomalie introdotte, fornendo un quadro completo della sua capacità di generalizzare anche su dati non visti.</p> <p>L’attività non ha registrato scostamenti rispetto al capitolato e ha raggiunto tutti gli obiettivi prefissati.</p> <p>Nel semestre, è stato anche redatto il rapporto tecnico di sintesi delle attività svolte.</p> <ul style="list-style-type: none"> • <i>Rapporto Tecnico RdS_PTR22-24_PR2.1_LA3.12_148 «Sviluppo e confronto prestazionale di algoritmi di rilevamento di cyber-attacchi nel contesto delle microreti elettriche».</i>