TITOLO E ABSTRACT TEMA DI RICERCA DOTTORANDI DEI CORSI DI DOTTORATO DI INTERESSE NAZIONALE IN CUI I DOCENTI DIEE PARTECIPANO.

XL CICLO

Emmanuel Ayora

PhD: *Sustainable Development and Climate Change*. **(IUSS PAVIA)**

Tema di Ricerca:

Sistemi di gestione dell'energia basati su tecniche di Intelligenza artificiale nell'elettrificazione del trasporto pubblico.

Abstract:

Le recenti politiche internazionali di transizione energetica fissano obiettivi sempre più sfidanti per la riduzione delle emissioni inquinanti per il settore dei trasporti. Tuttavia, le auto private elettriche non sono una soluzione sostenibile a causa del loro elevato consumo per persona e km, e per lo scarso utilizzo dello spazio pubblico e i problemi di congestione. Di conseguenza, migliorare il trasporto pubblico locale è la soluzione migliore nel contesto urbano, soprattutto quando si considerano veicoli a zero emissioni. In particolare, le architetture dei sistemi di propulsione elettrica multi-sorgente con più fonti di energia sono molto promettenti per i veicoli di trasporto pubblico. Questi si basano su una combinazione di tecnologie tra batterie, supercondensatori, celle a combustibile a idrogeno, motori diesel e catenaria/ricarica wireless che richiedono una corretta gestione dei flussi di energia. In questo contesto, l'attività di ricerca riguarderà lo sviluppo di strategie avanzate di gestione e controllo dell'energia per sistemi di propulsione elettrica multi-sorgente per veicoli di trasporto pubblico, con particolare riferimento alle tecniche di intelligenza artificiale. Più in dettaglio, questi si baseranno sui dati di infomobilità raccolti durante i turni di servizio programmati ripetitivi che caratterizzano le flotte di trasporto pubblico, consentendo così

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

un'adeguata previsione dei dati e l'impiego di sistemi di gestione e controllo dell'energia basati sull'ottimizzazione in tempo reale.

Muzamil Hussain Wadho

PhD: *Sustainable Development and Climate Change*. **(IUSS PAVIA)**

Tema di Ricerca:

Sistemi di accumulo di energia ibridi altamente integrati per sistemi di propulsione elettrica marina.

Abstract:

Le recenti politiche internazionali di transizione energetica hanno fissato obiettivi di riduzione delle emissioni sempre più sfidanti per il settore dei trasporti, comprese le navi e le imbarcazioni. In particolare, l'Organizzazione Marittima Internazionale (IMO) ha fissato riduzioni ambiziose delle emissioni per il trasporto marittimo internazionale, come il 40% e il 70% entro il 2030 e il 2050 rispettivamente da conseguire attraverso miglioramenti dell'efficienza energetica e l'adozione di tecnologie e fonti energetiche a emissioni di gas serra prossime allo zero. In questo contesto, le architetture di propulsione elettrica multi-sorgente per imbarcazioni basate su una combinazione di tecnologie come batterie, supercondensatori, celle a combustibile a idrogeno e motori diesel sono tra le soluzioni tecnologiche più promettenti. L'attività di ricerca si concentra sullo studio, lo sviluppo e la prototipazione di configurazioni innovative e altamente integrate di sistemi ibridi di accumulo di energia per sistemi di propulsione elettrica marina. Poiché questi sistemi richiedono una corretta gestione dei flussi di energia tra le diverse fonti energetiche l'attività di ricerca si occupa anche dello sviluppo e dell'implementazione di strategie avanzate di gestione e controllo dell'energia combinando approcci convenzionali e innovativi, con particolare riferimento alle tecniche di intelligenza artificiale.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Hicham Eddoubi

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Machine Learning efficace contro Attacchi Avversari e Derive da Distribuzioni Non Note.

Abstract:

I recenti progressi dell'apprendimento automatico hanno portato all'adozione diffusa delle sue varie tecniche per risolvere numerosi problemi e compiti in molti campi; tuttavia, pur mostrando gradi di accuratezza estremamente elevati nei loro compiti, la maggior parte dei modelli di apprendimento automatico si basa sui dati di addestramento e come tale soffre di una mancanza di robustezza alla naturale progressione di dati e campioni che esiste al di fuori della distribuzione dei dati di addestramento. Inoltre, l'ascesa del campo dell'adversarial machine learning ha messo in evidenza le numerose debolezze dei modelli di apprendimento automatico, in quanto gli attori malintenzionati possono manipolare l'output dei modelli con relativa facilità, aggiungendo perturbazioni che possono passare inosservate all'occhio umano. Per questo motivo, questo progetto si concentra sul colmare il divario tra i risultati in laboratorio e le prestazioni in natura, poiché esiste un'urgente necessità di fortificare i modelli di apprendimento automatico contro le derive avversarie e i dati. Ad esempio, le immagini deepfake sono diventate estremamente realistiche e, sebbene esistano metodi di rilevamento, la loro robustezza agli attacchi avversari rimane in gran parte non verificata. La letteratura esistente non affronta questo problema in modo rigoroso. Pertanto, sono stati sviluppati strumenti di benchmark standardizzati per garantire metodi di rilevamento più efficaci e robusti.

Daniele Ghiani

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Tecniche di Machine Learning per il Rilevamento Adattivo di Malware in Scenari di Minaccia in Evoluzione Costante

Abstract:

Il software dannoso (ovvero il malware) è una minaccia informatica pervasiva e di grande impatto, in grado di compromettere dati sensibili, interrompere servizi critici e causare gravi danni economici. Nell'ultimo decennio, l'apprendimento automatico (ML) è emerso come una tecnologia chiave per migliorare il rilevamento del malware, grazie alla sua capacità di apprendere modelli complessi da grandi volumi di dati e automatizzare il processo di identificazione. Tuttavia, il malware si evolve rapidamente nel tempo, modificando spesso la sua struttura e il suo comportamento per eludere i metodi di rilevamento. Di conseguenza, per mantenere elevate le prestazioni di rilevamento è necessario aggiornare frequentemente i rilevatori basati su ML. Allo stesso tempo, la riqualificazione dei modelli su grandi insiemi di dati storici è spesso impraticabile a causa degli elevati costi computazionali e delle crescenti preoccupazioni sulla privacy e sulla conservazione dei dati. Un'alternativa pratica è quella di aggiornare i modelli utilizzando solo i dati più recenti. Se da un lato questo approccio risponde ai vincoli di privacy ed efficienza, dall'altro introduce la sfida dell'oblio catastrofico, in cui il modello perde la capacità di richiamare le conoscenze apprese in precedenza. Per affrontare questa sfida, questa ricerca esplora l'uso di tecniche di apprendimento continuo (CL), che consentono ai modelli di ML di apprendere da nuovi dati preservando le prestazioni su compiti precedentemente appresi. Oltre all'oblio catastrofico, che si riferisce alle metriche delle prestazioni globali, questo studio analizza anche il problema della regressione, un fenomeno correlato in cui esempi specifici, una volta classificati correttamente, possono essere classificati in modo errato negli stati futuri del modello, evidenziando la complessità di mantenere prestazioni coerenti nel tempo. L'impatto di questo problema e le strategie di mitigazione applicabili non sono ancora state affrontate in contesti di apprendimento continuo. Al centro di questo progetto di ricerca c'è la necessità di sistemi di rilevamento del

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

malware in grado di adattarsi efficacemente alle nuove minacce, pur mantenendo la capacità di rilevare i comportamenti dannosi osservati in precedenza.

Aurora Arrus

PhD: *Cybersecurity*. **(IMT Alti studi Lucca)**

Tema di Ricerca:

Framework Avanzato per il Rilevamento di Malware nei Sistemi IoT Basati su Linux mediante Emulazione Binaria.

Abstract:

La proliferazione dei dispositivi Internet of Things (IoT), in particolare quelli basati su Linux, ha introdotto importanti sfide di cybersicurezza a causa della loro diversità architettonica e delle limitate funzionalità di sicurezza. Le tecniche di rilevamento del malware esistenti, spesso ottimizzate per gli ambienti informatici standard, non sono adatte all'ecosistema IoT, altamente eterogeneo e con risorse limitate. Questo progetto di ricerca propone lo sviluppo di un framework avanzato per il rilevamento di malware che sfrutta l'emulazione binaria completa per replicare le condizioni operative del mondo reale su varie architetture IoT. Integrando l'emulazione della CPU e del sistema operativo con le tecnologie di containerizzazione, il framework mira ad analizzare in modo efficiente il comportamento del malware mantenendo scalabilità, sicurezza e isolamento. I dati raccolti dall'analisi statica e dall'esecuzione binaria alimenteranno gli algoritmi di apprendimento automatico per identificare modelli e comportamenti dannosi.

Nicola Deidda

PhD: *Cybersecurity*. **(IMT Alti studi Lucca)**

Tema di Ricerca:

Machine learning avanzato per la gestione delle minacce informatiche.

Abstract:

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

I modelli di apprendimento automatico sono ampiamente utilizzati nell'analisi e nel rilevamento delle minacce informatiche, a supporto di attività quali l'analisi del traffico di rete, il rilevamento delle anomalie e la classificazione del malware. L'emergere di modelli linguistici di grandi dimensioni (LLM) introduce nuove opportunità a più livelli di granularità, che vanno dall'analisi delle vulnerabilità nel codice sorgente e nel codice macchina alla gestione, all'arricchimento e alla contestualizzazione dei feed di cyber threat intelligence (CTI). Poiché le minacce informatiche diventano sempre più sofisticate, caratterizzate da tecniche di offuscamento avanzate, canali di comunicazione nascosti e tattiche in rapida evoluzione, i processi CTI tradizionali spesso si scontrano con il volume schiacciante di dati non strutturati ed eterogenei, nonché con le elevate esigenze poste agli analisti umani. Gli LLM offrono soluzioni promettenti automatizzando compiti critici come l'estrazione dei dati da fonti diverse, la sintesi delle minacce, la correlazione degli indicatori di minaccia e la generazione di approfondimenti analitici. Questo progetto esplora l'integrazione degli LLM e di altre tecniche avanzate di apprendimento automatico nei flussi di lavoro di intelligence e gestione delle minacce informatiche, concentrandosi sul loro potenziale per migliorare la prevenzione, il rilevamento precoce, l'analisi e la risposta agli incidenti. Inoltre, esamina le sfide dell'applicazione degli LLM nella sicurezza informatica, comprese le preoccupazioni relative all'accuratezza dei modelli e alla protezione dei dati. Valutando sia le opportunità che i limiti, questo lavoro mira a fornire una prospettiva lungimirante sul ruolo in evoluzione dei LLM nel rafforzamento delle capacità di intelligence sulle minacce informatiche.

Christian Scano

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Tema di Ricerca: *Machine Learning efficace per il Rilevamento delle Vulnerabilità nelle Applicazioni Web*

Abstract:

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Le applicazioni Web costituiscono una spina dorsale critica dei moderni ecosistemi digitali. Tuttavia, rimangono altamente esposte a uno spettro in espansione di attacchi sofisticati, tra cui SQL Injection (SQLi), Cross-Site Scripting (XSS) e classi di vulnerabilità emergenti. Per mitigare questi rischi, sono ampiamente diffusi i Web Application Firewall (WAF), che tradizionalmente adottano approcci basati su regole che si affidano a firme statiche e a euristiche create a mano. Tuttavia, questi metodi spesso mostrano una limitata adattabilità e resilienza nei confronti di tecniche di attacco offuscate o nuove. L'avvento dei WAF basati sull'apprendimento automatico offre un'alternativa promettente, consentendo l'identificazione dinamica di modelli complessi di minacce e migliorando la reattività dei sistemi di sicurezza. Questo progetto di ricerca si concentra sullo sviluppo di metodologie complete per l'attacco e la difesa delle applicazioni web in questo panorama in evoluzione. Dal punto di vista offensivo, studia approcci black-box per valutare sistematicamente la robustezza delle difese web, compresi i WAF basati su regole e potenziati dall'apprendimento automatico. Generando payload avversari in grado di aggirare le misure di sicurezza, il progetto mira a valutare la resilienza di questi sistemi in scenari di attacco realistici. Particolare attenzione viene posta sulla generazione di esempi avversari all'interno della natura discreta e strutturata degli input web, garantendo la conservazione della semantica e il mantenimento della funzionalità malevola. Inoltre, un'ulteriore direzione di ricerca si concentra sui test black-box su larga scala delle applicazioni web per scoprire le vulnerabilità note. Questa linea di lavoro mira a sviluppare metodologie efficienti e scalabili per il rilevamento delle vulnerabilità, simulando il comportamento di un attaccante esterno senza richiedere l'accesso al codice sorgente. Dal punto di vista difensivo, il progetto mira a progettare robusti modelli di apprendimento automatico in grado di rilevare il traffico web anomalo e dannoso in tempo reale. Questi modelli intendono migliorare la resilienza contro le manipolazioni avversarie e garantire prestazioni elevate anche in caso di evoluzione delle minacce. Strategie come l'addestramento degli avversari, la modellazione d'insieme e l'ottimizzazione robusta guidano lo sviluppo di difese che riducono al minimo i falsi positivi, pur mantenendo affidabili le capacità di rilevamento delle minacce. Integrando direzioni di ricerca offensive e difensive, questo progetto vuole far progredire lo sviluppo di soluzioni di sicurezza proattive, adattive e resilienti per le applicazioni web, contribuendo così alla protezione e all'affidabilità delle infrastrutture digitali critiche.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Claudio Frongia

PhD: *Micro and Nano-Electronics*. **(Università degli Studi di Pavia)**

Tema di Ricerca:

Sviluppo di un circuito integrato basato sulla piattaforma RISC-V a bassissimo consumo per l'ottimizzazione dell'acquisizione e dell'elaborazione dei biosegnali.

Abstract:

Il progetto di ricerca si concentra su due obiettivi fondamentali:

1. Lo sviluppo di un circuito integrato personalizzato basato su RISC-V per l'accelerazione dell'elaborazione dei biosegnali e di altre applicazioni avanzate di elaborazione digitale del segnale (DSP).
2. La progettazione di sistemi front-end analogici adattivi per l'acquisizione efficiente di più segnali e la conversione biosegnale-spike.

Il front-end analogico è adattato all'acquisizione di segnali eterogenei come EEG, EMG, ENG ed ECoG. Si stanno esplorando tecniche efficienti di codifica dei segnali misti, tra cui la modulazione delta, la modulazione sigma-delta e l'incrocio multilivello, con l'obiettivo di ridurre l'energia consumata e la dimensione dei dati, preservando le informazioni cruciali del biosegnale. Il core RISC-V personalizzato è stato progettato per fungere da interfaccia tra il front-end analogico e una potenziale rete neurale di spike (SNN), eseguendo la preelaborazione del segnale e gestendo l'instradamento degli spike attraverso un meccanismo di Address-Event Representation (AER). Verranno esplorate diverse strategie di integrazione innovative per interfacciare il front-end analogico con il core RISC-V personalizzato. L'obiettivo finale del progetto è quello di raggiungere un efficace compromesso tra basso consumo energetico ed elevata affidabilità delle informazioni nell'acquisizione, elaborazione e analisi dei biosegnali. In collaborazione con Insyde srls, stiamo progettando un microcontrollore RISC-V personalizzato per applicazioni DSP avanzate, dotato di RAM per istruzioni e dati (architettura Harvard), timer (con modulazione PWM e altre funzioni avanzate), interfacce bus SPI master, I3C, APB e AXI, e un modulo core_top che include il core del processore, l'interfaccia di debug (DM+DTM, alias interfaccia JTAG) e la FPU. Le

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

estensioni delle istruzioni non standard di RISC-V, come fast_mult, fast_mac, fast_mult_fp e fast_matmul, sono integrate per supportare le principali applicazioni DSP, tra cui le trasformate di Fourier e il filtraggio FIR e IIR. Per l'ottimizzazione delle operazioni DSP vengono sfruttati l'algoritmo di Karatsuba, l'algoritmo di Booth, la matematica vedica (per la moltiplicazione veloce e il MAC) e le strategie di esecuzione vettoriale (per la moltiplicazione veloce delle matrici).

Mahdi Yektai

PhD: *Micro and Nano-Electronics*. **(Università degli Studi di Pavia)**

Tema di Ricerca:

Sviluppo di uno stimolatore di corrente CMOS ad alta tensione per il ripristino del feedback sensoriale.

Abstract:

I progressi delle neuroscienze e della robotica hanno aperto nuove possibilità per lo sviluppo di protesi neurali innovative per la sostituzione degli arti. Per garantire il successo di tali protesi, è fondamentale stabilire una connessione stabile e affidabile tra l'arto artificiale, i muscoli residui e il sistema nervoso. La comunicazione con il sistema nervoso può essere stabilita con tecniche invasive o non invasive. Tuttavia, per ripristinare il senso naturale del tatto, i dispositivi protesici e le strategie di stimolazione devono essere in grado di imitare il modello naturale di attivazione dei recettori cutanei. L'uso di interfacce invasive con il Sistema Nervoso Periferico ha mostrato risultati promettenti grazie alla loro selettività nell'elicitazione di sensazioni tattili somatotopiche, ma presentano svantaggi legati all'invasività dovuta all'intervento chirurgico, alla reazione fibrotica e alla scarsa stabilità a lungo termine. La stimolazione elettrica transcutanea dei nervi (TENS) è una tecnologia emergente nel campo delle protesi degli arti superiori e inferiori per ripristinare il feedback sensoriale senza la necessità di un intervento chirurgico. Lo sviluppo di stimolatori elettrici adatti alla TENS richiede diverse sfide tecnologiche. La stimolazione elettrica deve essere eseguita in modalità controllata dalla corrente (CCM) per evitare danni ai tessuti e la conformità della tensione deve essere elevata per garantire la capacità di fornire la carica adeguata alle fibre nervose. Inoltre, lo stimolatore deve avere più canali di stimolazione per

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

imitare l'attivazione naturale dei tessuti nervosi periferici e deve funzionare in diverse situazioni per quanto riguarda il consumo di energia, l'area e la temperatura. Questa tesi si propone di realizzare un circuito integrato CMOS ad alta tensione in grado di stimolare correttamente i nervi periferici attraverso la pelle.

Ejaz Zohaib

PhD: *Photovoltaics*. **(Università degli Studi di Salerno)**

Tema di Ricerca:

Sviluppo di sistemi di conversione per la gestione in corrente continua di impianti fotovoltaici orientati alla produzione di idrogeno verde.

Abstract:

La ricerca prevede lo sviluppo di configurazioni innovative di sistemi di conversione per la gestione in corrente continua di impianti fotovoltaici dedicati alla produzione di idrogeno verde. In particolare, l'attività prevede lo sviluppo di un sistema di condizionamento della potenza degli impianti fotovoltaici finalizzato all'ottimizzazione dell'utilizzo dell'elettrolizzatore alcalino per minimizzare i costi di produzione dell'idrogeno. A questo scopo e con l'obiettivo di massimizzare l'efficienza di conversione, gli impianti fotovoltaici saranno interconnessi all'elettrolizzatore con convertitori DC/DC multiporta. Questi ultimi saranno caratterizzati da quattro porte bidirezionali per la gestione dei flussi di corrente continua dall'impianto fotovoltaico all'elettrolizzatore, al sistema di accumulo elettrochimico e alla rete. La gestione dei flussi di potenza e il dimensionamento delle apparecchiature saranno l'obiettivo del dottorato. Le attività di dottorato si svilupperanno per 12 mesi presso la Piattaforma Energie Rinnovabili di Sardegna Ricerche, dove è già presente una parte delle apparecchiature citate.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

XXIX CICLO

Alì Arshad

PhD: *Photovoltaics*. **(Università degli Studi di Salerno)**

Tema di Ricerca:

Sviluppo sistematico, modellazione e validazione sperimentale di un convertitore Multiattivo a Ponte (MAB) per stazioni di ricarica per veicoli elettrici alimentate da fotovoltaico.

Abstract:

Questa ricerca si concentra sullo sviluppo di un convertitore DC-DC Multi-Active Bridge (MAB) appositamente progettato per stazioni di ricarica per veicoli elettrici (EV) alimentate da sistemi fotovoltaici (PV). Il convertitore è sviluppato con un'enfasi sull'efficiente trasferimento di potenza alla batteria del veicolo elettrico utilizzando una topologia a ponte multi-attivo. Il modello proposto è ulteriormente validato attraverso test sperimentali per garantire prestazioni affidabili in condizioni operative realistiche. I risultati di questa ricerca mirano a contribuire alla progettazione di un'infrastruttura di ricarica per veicoli elettrici efficiente, scalabile e alimentata da fonti rinnovabili.

Moein Taghavikoutenaei

PhD: *Photovoltaics*. **(Università degli Studi di Salerno)**

Tema di Ricerca:

Sviluppo di sistemi di accumulo di energia per migliorare la qualità dell'energia e disaccoppiare i sistemi di ricarica ultrarapida dei veicoli elettrici alimentati da impianti fotovoltaici dalla rete elettrica.

Abstract:

L'attività prevede l'analisi, lo sviluppo e l'implementazione di sistemi di gestione integrati per impianti fotovoltaici, al fine di fornire servizi energetici su misura per la mobilità elettrica. L'obiettivo è identificare configurazioni integrate di impianti fotovoltaici e sistemi di accumulo per gestire i servizi energetici richiesti dai veicoli elettrici. L'attività esplorerà lo sviluppo di un sistema fotovoltaico/di accumulo integrato con stazioni di ricarica bidirezionali

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

e algoritmi di ottimizzazione per la gestione distribuita, finalizzati a massimizzare l'autoconsumo per la mobilità elettrica.

Sodessa Soma Shonkora

PhD: *Sustainable Development and Climate Change*. **(IUSS PAVIA)**

Tema di ricerca:

Nuove topologie di sistemi di conversione dell'energia: approcci alla progettazione e al controllo.

Abstract:

L'obiettivo principale di questa ricerca è esplorare e analizzare configurazioni innovative di sistemi di conversione dell'energia in contesti modulari e multi-sorgente, al fine di ottimizzare le applicazioni di elettrificazione in diversi settori, con un focus particolare sulle applicazioni marine. In particolare, lo studio mira a identificare e valutare nuove tecnologie di conversione dell'energia in grado di integrarsi efficacemente con varie fonti energetiche, sia rinnovabili che convenzionali, per migliorare l'efficienza dei sistemi. La ricerca comprenderà la modellazione e la progettazione di nuove topologie di convertitori elettronici di potenza capaci di adattarsi a diverse esigenze di elettrificazione, garantendo scalabilità e flessibilità. Verranno inoltre sviluppate e ottimizzate strategie di controllo per i sistemi di conversione dell'energia, esplorando tecniche di controllo adeguate per migliorare le prestazioni, la stabilità e la risposta dei sistemi in condizioni di carico e ambientali variabili. Seguirà una valutazione dell'efficienza e della stabilità operativa delle configurazioni proposte tramite simulazioni e prove sperimentali. Inoltre, la ricerca identificherà aree applicative specifiche per dimostrare le implicazioni pratiche dei risultati ottenuti.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Dell'Aquila Salvatore Dario

PhD: *Space Science and Technology*. **(Università degli Studi di Trento)**

Tema di Ricerca:

Applicazione di tecniche di ottimizzazione alla progettazione del layout dei satelliti (Satellite Layout Optimization Design, SLOD).

Abstract:

Il processo di progettazione di un satellite coinvolge diverse fasi critiche, dalla concezione preliminare del layout fino all'integrazione dettagliata dei sottosistemi e ai test finali. Nelle fasi iniziali, gli ingegneri definiscono la struttura meccanica, eseguono simulazioni orbitali e dimensionano i sottosistemi essenziali come l'alimentazione, il controllo termico e i sistemi di comunicazione. Le fasi di progettazione dettagliata impiegano strumenti computazionali avanzati, come l'Analisi agli Elementi Finiti (FEA) e la Dinamica dei Fluidi Computazionale (CFD), per garantire l'integrità strutturale e le prestazioni termiche. Tuttavia, questo processo è dispendioso in termini di tempo e costi, oltre a dipendere fortemente da competenze specialistiche difficili da mantenere nel tempo. Automatizzare e ottimizzare la progettazione del satellite, con particolare attenzione al layout, offre un vantaggio competitivo significativo. Focus della presente ricerca è l'applicazione di tecniche di ottimizzazione alla progettazione del layout del satellite (Satellite Layout Optimization Design, SLOD), attraverso un approccio innovativo che combini l'ottimizzazione dei livelli e delle posizioni, estendendo il problema a una formulazione multi-obiettivo volta a minimizzare sia il momento d'inerzia del satellite che le non-uniformità termiche. Ulteriore elemento di innovazione sarà l'introduzione della modellazione surrogata: basata su modelli a diversa fedeltà, con lo scopo di garantire un'adeguata accuratezza riducendo i costi computazionali e così accelerando il processo di ottimizzazione. In particolare, verrà esplorato l'uso del Geometric Deep Learning (GDL), e più precisamente delle Graph Convolutional Networks (GCN), come surrogati per i modelli termici del satellite derivati da simulazioni CFD. Il GDL consente l'analisi di geometrie CAD 3D in domini non euclidei, preservando informazioni topologiche complesse senza richiedere una parametrizzazione estensiva. Si ritiene che l'applicazione di questi modelli possa avere un impatto significativo sulla prototipazione rapida di satelliti.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Luca Scionis

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Applicazione di tecniche di ottimizzazione alla progettazione del layout dei satelliti.

Abstract:

Questa ricerca si inserisce nel campo del Adversarial Machine Learning e si concentra sulla valutazione della robustezza dei modelli di visione tramite intelligenza artificiale quando sottoposti ad attacchi mirati. Il lavoro si sviluppa attraverso diverse fasi complementari. La prima fase riguarda l'ottimizzazione degli iperparametri per una specifica categoria di attacchi, noti come attacchi a norma minima. È stato sviluppato un framework per aumentarne l'efficacia e, attraverso questo strumento, sono state introdotte curve di valutazione della robustezza. Questi grafici mostrano come la capacità di un modello di resistere agli attacchi varia in funzione dell'intensità delle perturbazioni applicate alle immagini. Successivamente, la ricerca si concentra sulla valutazione degli attacchi black-box, in cui l'attaccante non ha accesso diretto ai dettagli del modello. Sono state definite linee guida pratiche per garantire un'analisi più corretta e realistica di questi attacchi, contribuendo a evidenziare e risolvere problemi critici presenti nella letteratura esistente. Il lavoro attuale esplora la combinazione di più attacchi a norma minima in un ensemble, con l'obiettivo di ottenere una valutazione più completa e affidabile della robustezza dei modelli. Questo approccio consente una misurazione più precisa dell'efficacia delle tecniche difensive, offrendo una visione più concreta delle vulnerabilità ancora presenti nei sistemi di visione artificiale.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Affan Younas

PhD: *Cybersecurity*. **(IMT Alti studi Lucca)**

Tema di Ricerca:

Modelli di Machine Learning per l'analisi e il rilevamento di minacce furtive e vulnerabilità latenti nel codice sorgente.

Abstract:

I sistemi software moderni costituiscono la base dell'infrastruttura digitale odierna, abilitando un'ampia gamma di applicazioni in ambiti diversi. Con l'aumento della complessità di questi sistemi, cresce anche la probabilità che si annidino vulnerabilità di sicurezza nel codice sorgente. Tali vulnerabilità, spesso latenti e dipendenti dal contesto, sono intrinsecamente difficili da rilevare e possono comportare gravi rischi per la sicurezza se non identificate e affrontate nelle prime fasi del ciclo di sviluppo del software. Questo progetto di ricerca esplora l'utilizzo di modelli di apprendimento automatico e apprendimento profondo per analizzare automaticamente il codice sorgente e individuare potenziali vulnerabilità. Sfruttando architetture basate su transformer come CodeBERT, insieme a informazioni strutturali derivate dagli Abstract Syntax Tree (AST), l'approccio consente al modello di comprendere in modo più efficace sia la logica che il contesto del codice. Il metodo include anche fasi di elaborazione specifiche per il dominio, al fine di rappresentare accuratamente le proprietà strutturali e semantiche uniche dei linguaggi di programmazione. Oltre a migliorare l'accuratezza nel rilevamento, il framework proposto è in grado di identificare le specifiche linee di codice più probabilmente vulnerabili. L'obiettivo è sviluppare modelli di apprendimento automatico automatizzati e ad alta precisione, che supportino gli sviluppatori nell'individuazione e nella risoluzione di debolezze di sicurezza lungo tutto il ciclo di vita dello sviluppo software, contribuendo così alla creazione di sistemi software più sicuri e resilienti.

Zohreh Shahrouei

PhD: *Autonomous Systems (Dausy)*. **(Politecnico di Bari)**

Tema di Ricerca:

Sistemi di gestione e automazione per il controllo energetico in edifici e processi industriali.

Abstract:

Il quadro di riferimento per la ricerca proposta si inserisce all'interno di progetti in corso presso il partner industriale, finanziati sia da aziende private che da enti pubblici, nonché presso il Dipartimento di Ingegneria Elettrica ed Elettronica, con finanziamenti derivanti dal PNRR. L'obiettivo del progetto è lo studio e lo sviluppo di strumenti per la gestione energetica dell'utilizzo dell'energia, sia in ambito civile sia in insediamenti industriali. Lo sfruttamento pieno delle fonti rinnovabili dovrebbe essere raggiunto tramite algoritmi di controllo distribuito e ottimizzazione, considerando possibilmente le caratteristiche specifiche degli utenti e dei produttori connessi alla rete. Il ruolo dei sistemi di accumulo energetico espliciti o impliciti, ad esempio batterie e strutture edilizie rispettivamente, sarà preso in considerazione nelle procedure di ottimizzazione, così come la conoscenza delle previsioni comportamentali e meteorologiche. A tal fine, i modelli del singolo utente o produttore saranno analizzati e sviluppati mediante approcci sia basati sulla modellazione fisica sia su dati. La progettazione del sistema di gestione e ottimizzazione energetica dovrà essere sufficientemente versatile da adattarsi al livello di monitoraggio, sicurezza e automazione dell'edificio o dell'attività industriale, a seconda dell'applicazione specifica.

Gli obiettivi principali del programma sono dettagliati di seguito:

- Definire un approccio flessibile per la gestione energetica in applicazioni civili e industriali.

  Tenendo conto della variabilità del contesto, sarà studiato e sviluppato un approccio teorico che possa essere adeguatamente adattato a diverse situazioni di gestione energetica, specificandone le condizioni di validità.
- Identificare un insieme di indici di prestazione utilizzabili per l'ottimizzazione dell'uso dell'energia.

La gestione di un sistema complesso può richiedere l'uso di indici di prestazione adeguati a scopi economici e tecnici che dipendono dall'applicazione. Ciò implica lo sviluppo di diversi strumenti.

- Applicazione di approcci di ottimizzazione in casi specifici. Considerando i casi applicativi gestiti da STAM durante il periodo del dottorato, gli approcci studiati e sviluppati saranno adattati al caso d'uso e testati in un contesto applicativo reale.

XXXVIII CICLO

Silvia Lucia Sanna

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Applicare Algoritmi di Intelligenza Artificiale all'Informatica forense per il Rilevamento dei Malware Android.

Abstract:

Negli ultimi decenni i dispositivi mobili sono ampiamente utilizzati dalla gente comune e dalle aziende; tra questi, Android è il sistema operativo (OS) mobile più usato al mondo. Inoltre, negli ultimi anni il numero di attacchi e minacce ai dispositivi mobili sta aumentando rapidamente, sia per le aziende che per i dispositivi personali. Per questi motivi, è importante sviluppare meccanismi di rilevamento efficienti. Le metodologie attualmente presenti in letteratura sono quasi tutte basate su tecniche statiche e dinamiche, ovvero sull'analisi dell'applicazione Android (apk) in base al suo codice (statico) o durante l'esecuzione (dinamico). La maggior parte dei lavori allo stato dell'arte utilizza i risultati di tali tecniche come fper gli algoritmi di Machine Learning (ML) o Deep Learning (DL) per classificare e rilevare il malware Android. Tali tecniche non considerano gli effetti dell'esecuzione del

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

malware nell'intero sistema operativo e, inoltre, alcuni algoritmi non sono efficienti a causa degli attacchi a, che modificano il comportamento o la struttura del malware per eludere il rilevamento degli algoritmi di intelligenza artificiale (AI). La maggior parte dei lavori che utilizzano l'analisi dinamica si basa sull'esecuzione del malware in emulatori, ma alcuni malware sono in grado di rilevare l'uso dell'emulatore e di modificare il comportamento in modo da non rilevare . Inoltre, esistono alcune famiglie di malware per le quali non è possibile utilizzare le tecniche tradizionali per rilevare la minaccia e il comportamento sospetto, come il malware “fileless” (ovvero il malware che viene eseguito nella RAM e non lascia tracce nel disco) o lo “stegomalware” (ovvero il malware che utilizza tecniche steganografiche per nascondere il payload dannoso). Questi malware eseguono il comportamento dannoso direttamente nella RAM e sono rilevabili solo in quel determinato lasso di tempo (cioè solo durante l'esecuzione). L'analisi forense digitale potrebbe essere utilizzata per superare questi problemi. Infatti, è possibile estrarre caratteristiche specifiche dalla RAM o monitorare directory specifiche nel disco per verificare gli effetti dell'esecuzione del malware nell'intero sistema operativo. Per applicare tali tecniche a dispositivi Android reali, è necessario effettuare il root (ovvero acquisire i privilegi di superutente), altrimenti il sistema operativo blocca l'accesso a specifiche aree di memoria, sia su disco che in RAM. L'acquisizione dei privilegi di root dipende strettamente dalla versione del sistema operativo utilizzato, dal fornitore, dalle patch di sicurezza di Google, dalla versione del kernel e attualmente non esiste una metodologia universale. Gli algoritmi di intelligenza artificiale possono essere applicati anche alle indagini di Digital Forensics in generale, ad esempio per rilevare automaticamente la presenza di specifici file multimediali oggetto dell'accusa o per generare rapporti automatici. La mia ricerca si occupa quindi di questi problemi.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Gupta Srishti

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Verso sistemi di machine learning efficaci addestrati incrementalmente in open world.

Abstract:

L'attuale crescita dell'Intelligenza Artificiale (IA) è attribuibile principalmente al calcolo ad alte prestazioni e alla disponibilità di grandi quantità di dati. Recentemente, dato che le prestazioni dei modelli di grandi dimensioni si sono stabilizzate, i ricercatori si trovano ad affrontare nuove sfide: cercare di stare al passo con i cambiamenti nei dati, gestire campioni non convenzionali (wild samples), prevenire attacchi avversari sui modelli fondamentali, e così via. In questo lavoro, ci concentriamo principalmente sui primi due problemi. Per risolvere il primo, la soluzione predefinita è il riaddestramento completo del modello da zero. Tuttavia, ciò presenta alcune criticità: a) l'addestramento di modelli di grandi dimensioni da zero è computazionalmente costoso, b) poco sostenibile dal punto di vista ambientale, e c) richiede molte risorse. Per quanto riguarda il secondo problema, i modelli sono implicitamente addestrati assumendo che i dati siano iid (indipendenti e identicamente distribuiti), cioè che i dati di addestramento siano campionati da una distribuzione sottostante dalla quale provengono anche i dati di test. Tuttavia, disporre di una distribuzione oracle non è possibile, e quindi questa è un'assunzione troppo generale per contesti reali. In questo lavoro affrontiamo questi problemi esplorando la dinamicità del modello tramite l'addestramento continuo — cioè l'addestramento continuo su nuovi dati senza ricominciare da zero — combinato con il rilevamento di dati fuori distribuzione, rendendo così il modello adatto ad applicazioni reali. La ricerca si focalizza inoltre sulla robustezza di questi sistemi IA realistici.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Yike Li

PhD: *Autonomous Systems (Dausy)*. **(Politecnico di Bari)**

Tema di Ricerca:

Controllo ottimale della sicurezza per i sistemi di controllo ferroviario di nuova generazione.

Abstract:

Rispetto alla costruzione di nuove linee ferroviarie, lo sviluppo di un sistema di segnalamento rappresenta un'alternativa più economica ed ecologica per far fronte alla crescente domanda di capacità. Sfruttando i progressi nella comunicazione Train-to-Train, il Virtual Coupling (VC) ha attirato sempre più attenzione come sistema di segnalamento ferroviario di nuova generazione. Invece del tradizionale accoppiamento fisico tramite assi meccanici, i treni operanti in modalità VC sono connessi tra loro attraverso una rete Wi-Fi o una connessione 5G, viaggiando alla stessa velocità e a distanza ravvicinata per formare un convoglio. Tuttavia, la sua implementazione presenta sfide critiche dal punto di vista del controllo, poiché i treni che seguono devono mantenere distanze minime in condizioni operative dinamiche, affrontando anche incertezze come perdite di comunicazione ed errori di misura. Questo progetto mira ad applicare metodologie di controllo ottimale al controllo dei treni in modalità VC. Si basa e amplia l'utilizzo delle Control Barrier Functions (CBFs), uno strumento rigoroso per il controllo della sicurezza, combinandole con la programmazione quadratica (QP), per sviluppare un controllore in grado di operare in tempo reale che garantisca sicurezza e stabilità nei convogli VC, senza richiedere coordinamento centralizzato o la previsione completa della traiettoria dei treni precedenti, mantenendo allo stesso tempo le brevi distanze tra i treni rese possibili dal VC. Oltre a garantire robustezza alle incertezze, la ricerca considera anche convogli VC composti da flotte eterogenee di treni nelle diverse fasi operative, al fine di aumentare l'applicabilità del controllore in scenari reali.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it