Universitatea
Transilvania
din Brașov

ȘCOALA DOCTORALĂ INTERDISCIPLINARĂ

Facultatea de Inginerie Electrică și Știința Calculatoarelor

Ing. Emmanuel TUYISHIME

Abordarea provocărilor legate de securitatea cibernetică în sistemele de inginerie la distanță bazate pe IoT/IIoT

REZUMAT

Conducător științific

Prof. dr. Petru Adrian COTFAS

BRAȘOV, 2026

CUPRINS

CUPRINS 1
REZUMAT 3
Chapter 1. Introducere 4
1.1. Context și motivația cercetării 4
1.2. Scopul și obiectivele cercetării 5
1.3. Structura tezei 5
Chapter 2. Sisteme de inginerie la distanță și provocări în domeniul securității cibernetice 6
2.1. Ingineria la distanță în educație 6
2.1.1 Context și paradigme de laborator 6
2.1.2 Provocări în materie de securitate cibernetică și strategii de atenuare în sistemele RL 7
2.2. Ingineria la distanță în industrie 8
2.2.1 Context și evoluție 8
2.2.2 Vulnerabilități de securitate cibernetică, actori de amenințare și vectori de atac în sistemele industriale RMC 9
2.2.3 Strategii de atenuare a riscurilor de securitate cibernetică și bune practici pentru sistemele industriale 9
2.3. Concluzie 10
Chapter 3. Proiectarea și implementarea arhitecturii de control al accesului "Zero Trust" pentru sistemele de inginerie la distanță 12
3.1. Implementarea într-un mediu de laborator la distanță 12
3.1.1 Arhitectura sistemului și contextul de implementare 12
3.1.2 Arhitectura ZTNA, controlul accesului și politica de securitate a dispozitivelor 13
3.2. Discuții 14
3.3. Concluzia capitolului 15
Chapter 4. Clasificarea traficului bazată pe învățarea automată, eficientă din punct de vedere al resurselor și orientată către selecția caracteristicilor, pentru atacurile de securitate MQTT-IoT 16
4.1. Metodologie și proiectarea experimentală 16
4.1.1 Descrierea setului de date 16
4.1.2 Selectarea caracteristicilor 17
4.2. Proiectarea și evaluarea experimentală 17
4.2.1 Configurarea și rezultatele clasificării binare 17
4.2.2 Configurarea și rezultatele clasificării multiclasă 18
4.3. Discutarea rezultatelor 20
4.4. Selectarea modelului și implicații practice 21
4.5. Concluzia capitolului 22
Chapter 5. Dezvoltarea unei arhitecturi modulare pentru detectarea în timp real a intruziunilor bazată pe învățare automată în mediile IoT/IIoT, cu integrare SIEM în cloud care respectă confidențialitatea .. 23

5.1. Proiectarea arhitecturii sistemului 23
5.2. Integrarea și comunicarea platformelor de sistem 24
5.2.1 Achiziția datelor la nivel de senzor 24
5.2.2 Middleware bazat pe Node-RED și stratul de integrare 24
5.2.3 Integrare în cloud cu protejarea confidențialității 25
5.2.4 Modelul amenințărilor și scenariile de atac 25
5.3. Inferența în învățarea automată 26
5.3.1 Mecanism de comutare a modelului în timpul rulării pentru inferența adaptivă a IDS 27
5.4. Rezultate, evaluarea performanței și analiza la nivel de sistem 28
5.4.1 Analiza performanței și a preciziei detectării 28
5.4.2 Performanța în ceea ce privește latența și debitul 28
5.4.3 Adaptarea la timpul de execuție și suprasarcina generată de comutarea modelelor 29
5.4.4 Integrarea în cloud, validarea operațională și eficiența costurilor 30
5.5. Concluzia capitolului 31
Chapter 6. Arhitecturi hibride reziliente de tip „edge–fog” pentru detectarea intruziunilor bazată pe ML în sistemele de monitorizare și control la distanță IoT/IIoT 32
6.1. Arhitectura sistemului și platforma experimentală 32
6.2. Scenarii experimentale și metodologia de evaluare 33
6.3. Rezultate și discuții 34
6.3.1 Latența de control și performanța în ceea ce privește fiabilitatea 34
6.3.2 Analiza utilizării resurselor 34
6.3.3 Latența inferenței și performanța de transfer 35
6.4. Concluzia capitolului 35
Chapter 7. Concluzii finale, contribuții originale, diseminarea rezultatelor și cercetări ulterioare 37
7.1. Concluzii 37
7.2. Contribuții originale ale cercetării 37
7.3. Diseminarea rezultatelor cercetării 38
7.4. Direcții pentru cercetări viitoare 39
Referințe 41

REZUMAT

Sistemele de inginerie la distanță permit interacțiunea cu procesele fizice și infrastructurile inginerești prin intermediul rețelelor distribuite și au căpătat o importanță din ce în ce mai mare atât în educația inginerească, cât și în practica industrială. Progresele în domeniul rețelelor, al cloud computingului și al tehnologiilor IoT/IIoT, accelerate de inițiativele Industriei 4.0, au extins flexibilitatea și scalabilitatea acestora, crescând în același timp expunerea la amenințările cibernetice. Pe măsură ce sistemele anterior izolate devin conectate la rețea, modelele convenționale de control al accesului bazate pe perimetru și mecanismele de detectare a intruziunilor, care consumă multe resurse, se confruntă cu dificultăți în a îndeplini cerințele contemporane de securitate, performanță și reziliență.

Această teză abordează aceste provocări prin proiectarea, implementarea și evaluarea experimentală a unor soluții complementare de securitate cibernetică pentru sistemele de inginerie la distanță bazate pe IoT și IIoT. Cercetarea este structurată în jurul a trei direcții interconectate: controlul accesului centrat pe identitate, detectarea intruziunilor eficientă din punct de vedere al resurselor și arhitecturi de implementare orientate spre reziliență.

Lucrarea începe cu o analiză sistematică a mediilor de inginerie la distanță din domeniile educațional și industrial, identificând tendințele tehnologice cheie, provocările de securitate cibernetică și lacunele de cercetare. Pentru a consolida controlul accesului, este proiectată și validată o arhitectură Zero Trust într-un mediu de laborator online, demonstrând aplicabilitatea controlului accesului centrat pe identitate și impus prin politici în sistemele de inginerie la distanță.

Pentru a îmbunătăți detectarea atacurilor în condiții de resurse limitate, se propune o abordare ușoară de detectare a intruziunilor bazată pe învățare automată. Abordarea introduce o metodologie statistică de selecție a caracteristicilor care reduce dimensionalitatea caracteristicilor, menținând în același timp o performanță competitivă de detectare a atacurilor de securitate IoT bazate pe MQTT. Pornind de la această bază, cercetarea investighează arhitecturi de detectare a intruziunilor adaptate la implementare prin intermediul implementărilor Edge–Cloud și hibride Edge–Fog, permițând monitorizarea în timp real, păstrând în același timp confidențialitatea și eficiența operațională.

Rezultatele experimentale demonstrează că abordările propuse realizează o detectare eficientă a intruziunilor cu o sarcină de calcul substanțial redusă, sprijinind în același timp implementarea în timp real în medii cu resurse limitate. Concluziile oferă o bază validată experimental pentru îmbunătățirea securității cibernetice și a rezilienței operaționale a sistemelor de inginerie la distanță bazate pe IoT/IIoT și stabilesc direcții pentru cercetări viitoare în domeniul securității adaptive, al inteligenței distribuite și al sistemelor ciber-fizice reziliente.

Chapter 1. Introducere

1.1. Context și motivația cercetării

Sistemele de inginerie la distanță permit utilizatorilor să interacționeze cu procesele fizice și infrastructurile inginerești prin intermediul rețelelor distribuite și au căpătat o importanță din ce în ce mai mare atât în învățământul ingineresc, cât și în practica industrială. În mediul educațional, laboratoarele la distanță extind accesul la experimentarea fizică dincolo de constrângerile temporale și geografice tradiționale, facilitând învățământul la distanță și partajarea resurselor [1], [2]. În contextul industrial, sistemele de monitorizare și control la distanță (RMC) sprijină supravegherea, întreținerea și automatizarea activelor dispersate geografic [3], [4].

Adoptarea rapidă a ingineriei la distanță a fost impulsionată de progresele înregistrate în domeniul tehnologiilor de rețea, al cloud computing-ului, al Internetului obiectelor (IoT) și al IoT-ului industrial (IIoT) [5] și a fost accelerată și mai mult de inițiativele Industriei 4.0 [6]. De la dispozitive casnice inteligente la fabrici industriale inteligente, activele și instalațiile sunt acum interconectate digital pe zone geografice vaste[6] . Această transformare a fost subliniată în mod deosebit în timpul pandemiei de COVID-19, care a obligat industriile și instituțiile de învățământ să adopte operațiuni la distanță și modalități hibride la o viteză fără precedent [7], [8]. În consecință, accesibilitatea la distanță a trecut de la a fi o comoditate la a deveni o necesitate operațională [9].

Cu toate acestea, aceste progrese introduc și riscuri substanțiale de securitate cibernetică. Platformele de inginerie la distanță distribuite funcționează pe infrastructuri de comunicații eterogene, cu mai multe straturi, care integrează active industriale, dispozitive încorporate cu resurse limitate, protocoale de rețea deschise și servicii bazate pe cloud [10], [11]. Deși această compoziție arhitecturală permite monitorizarea, experimentarea, întreținerea și interacțiunea la distanță scalabile, ea extinde simultan suprafața de atac la nivelul straturilor de detectare, comunicare și aplicații [12]. Convergența tehnologiei operaționale (OT) tradiționale cu mecanismele moderne de conectivitate complică și mai mult aplicarea măsurilor de securitate și limitează aplicabilitatea modelelor convenționale de securitate la nivel de întreprindere [13].

Abordările tradiționale de securitate cibernetică, dezvoltate în mare parte pentru infrastructurile IT convenționale ale întreprinderilor, nu se aliniază întotdeauna bine cu constrângerile operaționale ale sistemelor de inginerie la distanță. Multe mecanisme existente de control al accesului la distanță rămân bazate pe perimetru și tind să se bazeze pe încredere implicită odată ce accesul la rețea este stabilit, adesea prin intermediul rețelelor private virtuale (VPN). Abordarea bazată pe perimetru se confruntă cu provocări tot mai mari în contextele moderne ale întreprinderilor, care includ din ce în ce mai mult utilizatori la distanță, practici de tip „bring-your-own-device” (BYOD) și active bazate pe cloud [14]. În plus, aceste modele bazate pe perimetru oferă o protecție limitată împotriva amenințărilor din interior și a celor facilitate de persoane din interior, unde utilizarea abuzivă a accesului legitim, mai degrabă decât intruziunea externă, devine un factor de risc principal [15].

În același timp, constrângerile de calcul inerente sistemelor de inginerie la distanță, în special infrastructurilor RMC bazate pe IoT/IIoT, limitează fezabilitatea implementării unor mecanisme de securitate care consumă multe resurse, mai ales la marginea rețelei, unde funcționează senzori, actuatori și controlere încorporate. În consecință, mecanismele de securitate trebuie proiectate astfel încât să mențină integritatea operațională în timp real în condiții de resurse limitate [16], [17].

În acest context, problema centrală de cercetare abordată în această teză se referă la modul în care securitatea cibernetică a sistemelor de inginerie la distanță, în special a infrastructurilor RMC bazate pe IoT/IIoT, poate fi consolidată prin proiectarea și implementarea unor mecanisme de securitate care să abordeze controlul accesului centrat pe identitate, detectarea anomaliilor și distribuirea capacităților de detectare pe straturile sistemului, menținând în același timp cerințele operaționale în timp real și fiabilitatea sistemului.

1.2. Scopul și obiectivele cercetării

Scopul principal al acestei teze este de a proiecta, implementa și valida experimental mecanisme de securitate cibernetică și strategii de implementare care să sporească securitatea și reziliența sistemelor de inginerie la distanță bazate pe IoT/IIoT.

Pentru a atinge acest scop, teza urmărește următoarele obiective:

O1. Analizarea și sintetizarea caracteristicilor arhitecturale, a tehnologiilor facilitatoare și a provocărilor de securitate ale sistemelor de inginerie la distanță.

O2. Să investigheze și să operaționalizeze modelul „Zero Trust” ca model fundamental de control al accesului pentru mediile de inginerie la distanță.

O3. Proiectarea, evaluarea și implementarea unor mecanisme de detectare a intruziunilor bazate pe învățarea automată, eficiente din punct de vedere al resurselor, pentru sistemele de inginerie la distanță bazate pe IoT/IIoT, luând în considerare atât performanța de detectare, cât și constrângerile de implementare.

1.3. Structura tezei

Teza este structurată după cum urmează:

- Capitolul 1 prezintă necesitatea și motivația tezei, definește scopul și obiectivele cercetării și prezintă structura generală a tezei.
- Capitolul 2 prezintă fundamentele conceptuale și tehnologice ale sistemelor de inginerie la distanță, examinând arhitectura acestora, tehnologiile care le susțin și provocările legate de securitatea cibernetică atât în domeniul educațional, cât și în cel industrial.
- Capitolul 3 dezvoltă și validează o arhitectură de control al accesului de tip Zero Trust, centrată pe identitate, pentru mediile de inginerie la distanță, printr-un studiu de caz practic de laborator online.
- Capitolul 4 propune o metodologie de învățare automată, bazată pe selecția caracteristicilor și eficientă din punct de vedere al resurselor, pentru clasificarea atacurilor de securitate IoT bazate pe MQTT.
- Capitolul 5 dezvoltă o infrastructură modulară și orientată către confidențialitate pentru implementarea detectării intruziunilor în timp real, bazată pe învățare automată, cu monitorizare SIEM integrată în cloud.
- Capitolul 6 investighează reziliența operațională a sistemelor de monitorizare și control la distanță bazate pe IoT/IIoT în condițiile unor atacuri cibernetice și propune o implementare hibridă a sistemului IDS, validată prin evaluare experimentală.
- Capitolul 7 încheie teza prin sintetizarea principalelor concluzii și contribuții originale, prin rezumarea modalităților de diseminare a rezultatelor și prin prezentarea orientărilor pentru cercetările viitoare.

Chapter 2. Sisteme de inginerie la distanță și provocări în domeniul securității cibernetice

2.1. Ingineria la distanță în educație

2.1.1 Context și paradigme de laborator

Învățământul ingineresc s-a bazat în mod tradițional pe laboratoare fizice (față în față), unde studenții interacționează direct cu echipamentele experimentale într-un mediu comun pentru a-și consolida înțelegerea conceptuală și a dobândi experiență practică. Aceste laboratoare practice tradiționale oferă beneficii pedagogice, dar sunt limitate de factori precum costul, disponibilitatea echipamentelor, spațiul, întreținerea și riscurile de siguranță [18], [19].

Pentru a depăși aceste limitări, au fost introduse paradigme alternative de laborator, inclusiv laboratoarele virtuale (VL), care se bazează pe simulări software, și laboratoarele la distanță (RL), care permit interacțiunea cu echipamente fizice reale prin intermediul infrastructurilor de rețea. În sens mai larg, aceste medii sunt adesea denumite laboratoare online, cuprinzând atât experimente simulate accesibile de la distanță (VL), cât și instalații operate de la distanță (laboratoare la distanță), reprezentând platforme accesibile prin rețea care susțin experimentarea dincolo de constrângerile temporale și spațiale [20] .

Mediile de laborator sunt clasificate de obicei pe baza a două dimensiuni: locația utilizatorului (locală sau la distanță) și natura resurselor experimentale (fizice sau virtuale) [21], [22]. Acest lucru duce la patru categorii principale:

1. Laboratoare fizice practice, care implică interacțiunea directă cu echipamente fizice.
2. Laboratoare virtuale locale, bazate pe simulări executate pe mașini locale.
3. Laboratoare virtuale la distanță, în care mediile simulate sunt accesate prin rețele.
4. Laboratoare la distanță, care oferă acces prin rețea la echipamente fizice reale.

Dintre aceste paradigme, laboratoarele la distanță (RL) au căpătat o importanță deosebită datorită capacității lor de a păstra realismul experimentării fizice, îmbunătățind în același timp accesibilitatea și scalabilitatea. Laboratoarele la distanță permit utilizatorilor să interacționeze cu dispozitive fizice distribuite geografic prin intermediul unor interfețe web, extinzând astfel accesul la laborator către un public mai larg [1], [23], [24].

De-a lungul timpului, aceste paradigme de laborator au evoluat în componente pe deplin integrate ale educației inginerești. Ele susțin implementarea la scară largă, partajarea interinstituțională și accesul continuu, abordând provocări cheie legate de scalabilitate și flexibilitate pedagogică. Importanța lor a fost evidențiată și mai mult în timpul pandemiei de COVID-19, care a accelerat adoptarea modalităților de învățare online și hibride [25], [26].

Odată cu maturizarea și adoptarea pe scară largă a acestora, laboratoarele virtuale și la distanță au fost implementate din ce în ce mai mult ca infrastructuri organizate, la scară largă, mai degrabă decât ca instrumente didactice izolate. Un număr substanțial de lucrări raportează dezvoltarea unor platforme de laborator online care susțin învățarea și experimentarea în diverse domenii, inclusiv electronică, energie electrică și microelectronică, acționări electrice, energie regenerabilă, chimie, fizică, precum și control și automatizare [1], [27]–[33]. Implementările inițiale, însă, erau predominant specifice unei singure instituții și realizate la comandă, ceea ce a dus la sisteme izolate, cu interoperabilitate, reutilizare și accesibilitate interinstituțională limitate [34]. Aceste constrângeri au împiedicat adoptarea pe scară mai largă și partajarea interinstituțională.

Pentru a remedia aceste limitări, cercetarea s-a orientat către arhitecturi federate care permit integrarea laboratoarelor distribuite geografic în cadrul unor structuri comune [34]. În acest context, sistemele de gestionare a laboratoarelor la distanță (RLMS) au apărut ca un strat cheie de facilitare, oferind acces unificat, programare și gestionarea experimentelor pentru resurse eterogene de laborator la distanță [35].

2.1.2 Provocări în materie de securitate cibernetică și strategii de atenuare în sistemele RL

Având în vedere faptul că sunt conectate la internet și au o natură ciber-fizică, sistemele RL prezintă o suprafață de atac complexă și extinsă, expunând atât activele digitale, cât și echipamentele fizice la riscuri de securitate cibernetică. Aceste riscuri afectează nu numai proprietățile tradiționale de securitate a informațiilor, precum confidențialitatea, integritatea și disponibilitatea (CIA), ci se extind și la nerepudiere, autentificare, confidențialitate și siguranță (CIANA+PS) [36], [37]. Spre deosebire de mediile de laborator convenționale, sistemele RL sunt accesibile în mod continuu, extrem de interconectate și adesea implementate în cadrul unor rețele instituționale mai ample, crescând astfel vulnerabilitatea lor la atacuri cibernetice atât active, cât și pasive [38].

Dintr-o perspectivă fundamentală, amenințările la adresa securității cibernetice din sistemele RL ar trebui înțelese în cadrul definiției mai largi a amenințărilor cibernetice formulată de Institutul Național de Standarde și Tehnologie (NIST), care definește o amenințare ca fiind orice circumstanță sau eveniment capabil să afecteze în mod negativ operațiunile organizaționale, activele sau persoanele prin acces neautorizat, modificare, divulgare sau refuz de serviciu [39] . În mediile educaționale de RL, astfel de amenințări subminează direct fiabilitatea experimentelor, integritatea datelor generate și, în unele cazuri, siguranța fizică a echipamentelor de laborator și a utilizatorilor.

Mai multe studii indică faptul că mecanismele de securitate ale aplicațiilor web care susțin experimentele la distanță rămân insuficiente [40], [41]. Această deficiență a fost atribuită în mare măsură practicilor de dezvoltare care acordă prioritate conținutului educațional, experimentării și implementării rapide, în detrimentul integrării sistematice a considerentelor de securitate [37]. Ca urmare, sistemele RL la distanță moștenesc frecvent vulnerabilități care decurg din mecanisme de autentificare slabe, servicii web nesigure și o infrastructură insuficient monitorizată.

Vulnerabilitățile se manifestă prin multiple vectori de atac care amenință proprietățile CIANA+PS ale sistemelor RL.

- Atacuri asupra aplicațiilor web: Atacurile de tip „SQL Injection” și „XPath Injection” exploatează validarea insuficientă a datelor de intrare și securizarea insuficientă a aplicațiilor [42], [43]. S-a demonstrat că platformele RL prezintă astfel de vulnerabilități [37] , permițând accesul neautorizat la date, manipularea acestora și executarea de cod arbitrar, ceea ce poate compromite integritatea experimentală.
- Atacuri la nivelul stratului de comunicații: Atacurile de tip „Man-in-the-Middle” (MITM) exploatează canalele de comunicații nesigure [37]. Dincolo de interceptarea datelor de autentificare și încălcarea confidențialității, astfel de atacuri pot permite manipularea ostilă a parametrilor experimentali, introducând astfel riscuri legate de siguranță și de integritatea echipamentelor.
- Atacuri asupra disponibilității: Atacurile de tip Denial-of-Service (DoS) și Distributed Denial-of-Service (DDoS) pot perturba operațiunile RL prin suprasolicitarea serverelor sau a infrastructurii de rețea [37] . În plus, abuzul asupra mecanismelor de rezervare a laboratoarelor poate crea condiții de refuz al serviciului la nivelul stratului de aplicație.
- Atacuri bazate pe dispozitive și atacuri ciber-fizice: Sistemele RL sunt expuse la exploatarea firmware-ului, la alterarea hardware-ului și la manipularea mediului, ceea ce poate compromite disponibilitatea sistemului, integritatea datelor și funcționarea în condiții de siguranță.

Deși atacurile documentate care vizează în mod explicit sistemele RL rămân limitate, dovezi mai ample evidențiază o expunere substanțială la risc. Mai multe rapoarte clasează în mod constant sectorul educațional printre cele mai vizate industrii de campaniile de malware, phishing și ransomware [86]–[89] și indică niveluri relativ scăzute de pregătire cibernetică [90], [91]. Rapoarte recente indică o creștere semnificativă a atacurilor de tip ransomware împotriva universităților, care exploatează frecvent vulnerabilitățile legate de accesul la distanță, fiind de așteptat o escaladare suplimentară pe măsură ce infrastructura de lucru la distanță se extinde [92].

Consecințele includ pierderea datelor, compromiterea proprietății intelectuale, încălcări ale reglementărilor, afectarea reputației și erodarea încrederii în experimentarea la distanță [26], [44]. Este important de menționat că natura ciber-fizică a sistemelor RL permite propagarea riscurilor între domenii, situație în care intruziunile digitale pot provoca daune fizice sau pericole pentru siguranță.

În ciuda acestor riscuri, considerentele de securitate rămân secundare în mare parte a literaturii de specialitate [37] . Analizele publicate în [45] și [26] au identificat relativ puține lucrări care abordează în mod explicit siguranța și securitatea în mediile RL federate și OLMS.

- Autentificare și controlul accesului: Strategiile inițiale de atenuare a riscurilor puneau accentul pe schemele de autentificare cu nume de utilizator și parolă și pe abordări alternative, cum ar fi parolele bazate pe imagini. Cercetări mai recente au explorat autentificarea asistată de tehnologia blockchain și mecanismele de verificare descentralizate pentru a spori reziliența împotriva compromiterii credențialelor în infrastructurile distribuite de RL [46] . Cu toate acestea, autentificarea în sine nu asigură o securitate cuprinzătoare a sistemului.
- Modele de securitate pe niveluri: Krbeček et al. [47] au propus un model de securitate care adaptează mecanismul de protecție în funcție de complexitatea experimentului. Deși utilă pentru ilustrarea cerințelor de securitate diferențiate, această abordare riscă să subestimeze experimentele cu complexitate redusă ca potențiale puncte de intrare în rețelele instituționale.
- Măsuri de control bazate pe arhitectură și virtualizare: Separarea client-server, virtualizarea, tehnica „sandboxing”, imaginile numai pentru citire și segmentarea rețelei au fost propuse pentru a reduce suprafețele de atac și a limita propagarea programelor malware [48].
- Guvernanță și aliniere la standarde: Zonarea de securitate, gestionarea dinamică a încrederii și conformitatea cu reglementările, inclusiv respectarea GDPR, au fost propuse ca mecanisme de guvernanță [45] . Alinierea la standarde internaționale precum ISO/IEC 27000, ISO/IEC 15048 și IEC 62443 sprijină gestionarea sistematică a riscurilor.
- Măsuri de apărare la nivel de rețea: Segmentarea VLAN, criptarea, implementarea sistemelor IDS/IPS, firewall-urile pentru aplicații web, honeypot-urile, utilizarea VPN-urilor și monitorizarea continuă a traficului sunt recomandate pentru a consolida reziliența rețelei [37]. De asemenea, a fost explorată consolidarea specifică a protocoalelor, inclusiv integrarea securizată a MQTT în sistemele RL bazate pe IoT [49].

2.2. Ingineria la distanță în industrie

2.2.1 Context și evoluție

Sistemele industriale au fost proiectate în mod tradițional ca medii localizate și în mare măsură izolate, activitățile de monitorizare și control fiind limitate la instalațiile de la fața locului[50] . Formele timpurii de operare la distanță se bazau pe soluții cu fir de rază scurtă, menite să extindă camerele de control locale, mai degrabă decât să permită o separare geografică reală între operatori și procesele industriale [51]. Această izolare arhitecturală a fost motivată nu numai de constrângeri tehnologice, ci și de considerente de siguranță, fiabilitate și securitate inerente mediilor industriale.

Evoluția către controlul industrial la distanță (RMC) a început la mijlocul secolului al XX-lea, odată cu progresele înregistrate în domeniul calculului digital și al telecomunicațiilor [52]. Introducerea controlerelor logice programabile (PLC), a sistemelor de control de supraveghere și achiziție de date (SCADA) și a sistemelor de control distribuit (DCS) a marcat o schimbare majoră, permițând un control mai flexibil, scalabil și distribuit geografic al proceselor industriale [5], [53]. Aceste tehnologii au pus bazele sistemelor moderne de RMC, permițând operatorilor să monitorizeze stările sistemului și să emită comenzi de control din locații din ce în ce mai îndepărtate [50].

Integrarea ulterioară a protocoalelor de comunicații digitale, a conectivității la internet și a tehnologiilor fără fir a extins și mai mult aria de acoperire a sistemelor RMC, facilitând supravegherea centralizată a activelor distribuite geografic [51]. Ca urmare, soluțiile RMC au fost adoptate pe scară largă în sectoarele

de infrastructură critică, inclusiv energie, transporturi, sănătate, tratarea apei și producție, impulsionate de obiectivele comune de eficiență operațională, fiabilitate și siguranță [10], [54].

În mediile industriale moderne, soluțiile RMC au trecut de la a fi capabilități opționale la a deveni necesități operaționale. Multe sectoare depind acum de sistemele RMC pentru a menține productivitatea, a asigura siguranța personalului și a reduce costurile operaționale [55], [56]. Această dependență a fost deosebit de evidentă în timpul pandemiei de COVID-19, când accesul la distanță la sistemele industriale a devenit crucial pentru menținerea continuității activității și protejarea forței de muncă [57]–[59].

Sistemele industriale RMC susțin diverse aplicații, inclusiv teleoperarea în medii periculoase [60], [61], controlul robotic și automatizat al proceselor, precum și monitorizarea proceselor în timp real [62]. În plus, tehnologiile RMC permit întreținerea, diagnosticarea, instruirea și simularea de la distanță, sporind reziliența operațională și reducând timpul de nefuncționare [51], [63].

2.2.2 Vulnerabilități de securitate cibernetică, actori de amenințare și vectori de atac în sistemele industriale RMC

Sistemele industriale RMC prezintă o suprafață de atac semnificativ extinsă, rezultată din convergența tehnologiilor operaționale învechite, a practicilor de proiectare nesigure și a integrării sporite cu rețelele IT și serviciile conectate la Internet [13], [64]. Vulnerabilitățile provin din sisteme și protocoale învechite sau care nu mai beneficiază de suport, lipsite de securitate încorporată, precum Modbus și DNP3, care transmit adesea date în text simplu și sunt susceptibile la interceptare și manipulare [65], [66].

Aceste puncte slabe sunt agravate și mai mult de segmentarea inadecvată a rețelei între mediile IT și OT, ceea ce permite deplasarea laterală și compromiterea activelor critice. Riscuri suplimentare decurg din mecanismele slabe de autentificare și control al accesului, inclusiv datele de autentificare implicite, gestionarea deficitară a privilegiilor și tehnologiile nesigure de acces la distanță, precum Telnet și RDP necriptat [12] , precum și vulnerabilitățile introduse de componentele terțe și dependențele din lanțul de aprovizionare [65] . Constrângerile operaționale, în special gestionarea întârziată a patch-urilor din cauza perioadelor de nefuncționare și a problemelor de compatibilitate, lasă vulnerabilitățile cunoscute nesoluționate [67] , în timp ce securitatea fizică insuficientă permite manipularea directă și accentuează convergența riscurilor ciber-fizice.

Aceste slăbiciuni sistemice au transformat mediile industriale în ținte principale pentru actori de amenințare sofisticați care exploatează atât vulnerabilități cunoscute, cât și vulnerabilități de tip „zero-day” [68], [69] , așa cum o demonstrează incidentele cu impact ridicat, precum Stuxnet (2010), care a permis distrugerea fizică a echipamentelor industriale [70], [71] , atacul asupra oțelăriei germane (2014) și întreruperile rețelei electrice din Ucraina (2015–2016), precum și atacurile de tip ransomware și asupra lanțului de aprovizionare la scară largă, inclusiv NotPetya, WannaCry, Colonial Pipeline (2021) și SolarWinds (2020) [72] , alături de perturbări mai recente care afectează infrastructura critică și sistemele de sănătate [73], [74] . Sistemele industriale sunt expuse la diverși vectori de atac, inclusiv malware, ransomware, phishing, injecție SQL, atacuri asupra suporturilor amovibile și în scenariile de acces la distanță, compromiterea datelor de autentificare, uzurparea identității, atacuri de tip „Man-in-the-Middle” (MITM), replay, injectarea de date false și atacuri de tip „denial-of-service” care vizează infrastructurile de comunicații și autentificare [71], [72].

Peisajul amenințărilor este intensificat și mai mult de diversitatea adversarilor, care variază de la persoane din interior și grupuri de infractori cibernetici până la spioni industriali și actori ai statelor-națiune, ale căror motivații includ câștiguri financiare, spionaj și obiective geopolitice, sporind astfel sofisticarea atacurilor și complicând detectarea, atribuirea și răspunsul [53], [71].

2.2.3 Strategii de atenuare a riscurilor de securitate cibernetică și bune practici pentru sistemele industriale

Tabelul 2.1 rezumă principalele strategii de atenuare a riscurilor de securitate cibernetică pentru sistemele industriale, organizate în categorii funcționale cheie care abordează prevenirea, detectarea, reziliența și guvernanța.

Tabelul 2.1. Rezumatul strategiilor de atenuare a riscurilor de securitate cibernetică și al celor mai bune practici pentru sistemele industriale.

Categorie	Măsuri cheie	Scop	Referințe
Prevenire și detectare	Firewall-uri, IDS/IPS, monitorizare	Segmentarea rețelei și detectarea pe mai multe niveluri a amenințărilor pentru a atenua amenințările interne și cele de tip zero-day.	[53], [65], [75], [65], [76]
Comunicare și autentificare securizate	Criptare TLS	Asigură confidențialitatea și integritatea datelor în transit.	[77], [78]
	Învățarea pasivă a caracteristicilor (PFL)	Permite detectarea amenințărilor în traficul criptat	[78]
	Autentificare criptografică (AES, SHA-2)	Previne spoofing-ul, replay-ul și accesul neautorizat.	[53], [77]
	MFA, Zero Trust	Asigură o verificare riguroasă a identității și un control continuu al accesului.	[79],[80], [81]
Platforme de testare pentru securitate	Bancuri de testare fizice / virtuale / hibride	Permite evaluarea în condiții de siguranță a atacurilor și a măsurilor de apărare în condiții controlate.	[69], [82], [75]
	VICSORT și cadre similare	Susțin experimentarea scalabilă și eficientă din punct de vedere al resurselor.	[83]
Reziliență și recuperare	Redundanță, comutare automată, segmentare	Menținerea funcționării și limitarea impactului în cazul întreruperilor.	[84], [85]
	Ciclul de viață D2R2+DR	Reziliență structurată: apărare, detectare, remediere, recuperare, perfecționare.	[86], [87]
Standarde și cadre de referință	ISA/IEC 62443, NIST SP 800-82, ISO/IEC 27000	Asigură guvernanța securității bazată pe riscuri și conformitatea.	[88], [89] [90], [91]
	MITRE CREF, ENISA	Ghid pentru ingineria rezilienței și accesul securizat la distanță.	[92],[93]

2.3. Concluzie

Acest capitol a stabilit fundamentele conceptuale ale sistemelor de inginerie la distanță atât în laboratoarele educaționale la distanță, cât și în mediile industriale RMC. În ciuda obiectivelor diferite, ambele domenii se bazează pe arhitecturi interconectate bazate pe IoT/IIoT care încorporează platforme cloud, servicii web, protocoale industriale și tehnologii de acces la distanță, extinzând semnificativ suprafața de atac.

Analiza a arătat că laboratoarele la distanță din mediul educațional, deși îmbunătățesc accesibilitatea, se confruntă adesea cu autentificare slabă, comunicații nesigure și monitorizare limitată. În schimb, sistemele industriale se confruntă cu probleme similare, agravate de tehnologiile învechite, protocoalele nesigure, convergența IT–OT și prioritățile de proiectare axate pe disponibilitate. În ambele domenii, vulnerabilitățile recurente includ gestionarea slabă a identității, segmentarea inadecvată a rețelei, canalele de comunicații nesigure și capacitățile limitate de detectare a intruziunilor, incidentele industriale demonstrând potențialul unor consecințe operaționale și fizice grave.

O sinteză inter-domenii relevă lacune cheie: abordări de securitate fragmentate și specifice fiecărui domeniu, o luare în considerare limitată a interacțiunilor ciber-fizice între straturi și un sprijin insuficient pentru mediile cu resurse limitate. În special, lipsa mecanismelor de securitate ușoare și gata de implementare la nivelurile de margine și de poartă rămâne o limitare critică.

Aceste constatări evidențiază necesitatea unei abordări unificate de securitate cibernetică, adaptată la implementare, care să integreze controlul accesului centrat pe identitate, detectarea eficientă a intruziunilor și mecanisme de protecție stratificate în toate arhitecturile de sistem. În consecință, această teză abordează aceste provocări prin combinarea unei investigații privind controlul accesului de tip Zero Trust, a unui sistem de detectare a intruziunilor (IDS) bazat pe învățare automată (ML) eficient din punct de vedere al resurselor și a strategiilor de implementare adaptative, îndeplinind astfel obiectivul O1 și stabilind fundamentul pentru contribuțiile ulterioare.

Chapter 3. Proiectarea și implementarea arhitecturii de control al accesului "Zero Trust" pentru sistemele de inginerie la distanță

Sistemele de inginerie la distanță invalidează ipotezele tradiționale de securitate bazate pe perimetru, deoarece necesită acces continuu de la distanță la resurse fizice prin intermediul infrastructurilor conectate la Internet. Modelul convențional de tip „castel și șanț", care presupune rețele interne de încredere, nu mai este adecvat în mediile moderne caracterizate de utilizatori distribuiți, integrare în cloud și expunere crescută la amenințări din interior și la mișcări laterale [94] ,[95].

Accesul la distanță bazat pe VPN, deși este larg adoptat, extinde încrederea în rețea către utilizatorii autentificați și introduce riscuri semnificative de securitate din cauza vulnerabilităților, a configurărilor greșite și a modelelor de încredere implicită. Numărul tot mai mare de exploatări legate de VPN, inclusiv atacuri cu ransomware și atacuri asupra credențialelor, evidențiază aceste limitări [80].

Ca răspuns, a apărut paradigma Zero Trust (ZT), care înlocuiește încrederea implicită cu verificarea continuă bazată pe identitate, context și politici, conform principiului „nu te încrede niciodată, verifică întotdeauna" [96]. ZT pune accentul pe controlul accesului bazat pe identitate, pe principiile privilegiilor minime și pe monitorizarea continuă [97] și a fost adoptat pe scară largă ca răspuns la amenințările cibernetice în continuă evoluție [81].

În ciuda maturității sale, aplicarea conceptului Zero Trust, în special a accesului la rețea de tip Zero Trust (ZTNA), la sistemele de inginerie la distanță rămâne insuficient explorată în cercetarea academică. Acest capitol abordează această lacună prin propunerea și implementarea unei arhitecturi de control al accesului bazată pe ZTNA pentru medii de laborator la distanță, demonstrând că securitatea centrată pe identitate și bazată pe politici poate înlocui modelele tradiționale bazate pe perimetru.

3.1. Implementarea într-un mediu de laborator la distanță

3.1.1 Arhitectura sistemului și contextul de implementare

Arhitectura de control al accesului ZT a fost implementată și evaluată într-un mediu de laborator la distanță cu scop educațional, care găzduiește experimente accesibile prin Internet. Infrastructura de laborator la distanță utilizată în acest capitol se bazează pe o platformă de laborator serial online concepută pentru a sprijini experimentarea la distanță cu tehnologii de comunicații seriale, inclusiv RS232, RS422 și RS485 [98]. În această teză, laboratorul servește ca un sistem operațional de inginerie la distanță, oferind un mediu realist și constrâns pentru evaluarea mecanismelor de control al accesului bazate pe ZT.

Așa cum se ilustrează în Figura 3.1, arhitectura de securitate ZT propusă este implementată utilizând un cadru ZTNA compus din următoarele componente logice:

- Furnizor de identitate (IdP): responsabil pentru autentificarea utilizatorilor.
- PDP: evaluează cererile de acces în raport cu politicile definite.
- PEP: mediază și impune traficul autorizat.

În această implementare, se utilizează o platformă comercială ZTNA [99] pentru a realiza aceste funcții. Componenta de control acționează ca PDP, gestionând evaluarea politicilor și emiterea token-urilor de acces. În același timp, conectorii funcționează ca PEP-uri, aplicând deciziile de acces prin controlul fluxului de trafic între utilizatori și resursele laboratorului. Obiectivele principale de securitate ale arhitecturii propuse sunt prevenirea accesului neautorizat la resursele laboratorului, atenuarea utilizării abuzive a credențialelor și a mișcării laterale, protejarea integrității și disponibilității experimentelor, precum și reducerea expunerii la atacuri bazate pe rețea.

În consecință, pentru a impune limite clare de încredere, arhitectura este împărțită logic în trei zone principale de încredere:

- Zona utilizatorului: dispozitivele utilizatorilor și aplicațiile client care funcționează în afara controlului instituțional.
- Zona de control: IdP, PDP și PEP responsabile de verificarea identității și de aplicarea accesului.

— Zona de resurse la distanță: servere de experimentare și dispozitive fizice de laborator.

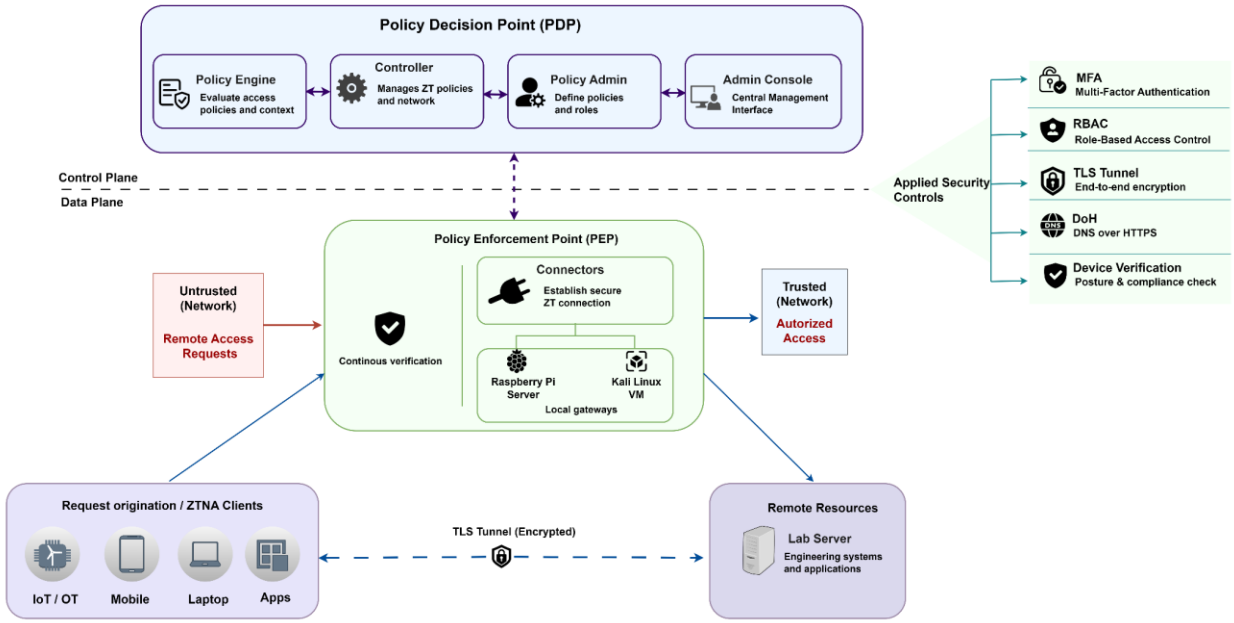


Figura 3.1. Arhitectura logică a cadrului propus de control al accesului Zero Trust.

3.1.2 Arhitectura ZTNA, controlul accesului și politica de securitate a dispozitivelor

În arhitectura propusă de acces la rețea Zero Trust (ZTNA), resursele protejate sunt organizate în rețele la distanță, care abstractizează infrastructura subiacentă (de exemplu, medii locale sau VPC) și permit accesul securizat, controlat prin politici, prin intermediul platformei Twingate. Accesul este gestionat centralizat prin intermediul controlerului, în timp ce conectorii servesc drept puncte de aplicare a politicilor, stabilind tuneluri criptate de ieșire către resursele interne fără a expune perimetrul rețelei. O configurație cu mai mulți conectori (bazată pe Raspberry Pi și mașini virtuale) îmbunătățește disponibilitatea, echilibrarea încărcării și toleranța la erori.

Resursele sunt definite folosind adresarea bazată pe IP sau intervale CIDR (Classless Inter-Domain Routing) și rămân inaccesibile direct de pe dispozitivele utilizatorilor finali. Utilizatorii le accesează prin sesiuni autentificate inițiate prin aplicația client, după o integrare bazată pe invitație și verificarea identității.

Așa cum se ilustrează în Figura 3.2, controlul accesului este aplicat prin mecanisme de autentificare și autorizare centrate pe identitate, inclusiv integrarea cu furnizori externi de identitate (Google SSO), controlul accesului bazat pe roluri (RBAC) și autentificarea multifactorială folosind TOTP pentru rolurile privilegiate. Deciziile de acces respectă principiul privilegiului minim, asigurându-se că utilizatorii interacționează numai cu resursele autorizate în condiții definite, minimizând astfel mișcarea laterală și suprafața de atac.

În plus, politicile de securitate la nivel de dispozitiv sunt aplicate înainte de acces, impunând respectarea standardelor de securitate predefinite (criptare, firewall-uri, antivirus și verificări ale integrității sistemului). Comunicarea dintre clienți și resurse este securizată prin tuneluri TLS cu certificate fixate și DNS-over-HTTPS (DoH), asigurând confidențialitatea, integritatea și protecția împotriva interceptării sau falsificării. Monitorizarea continuă și înregistrarea activității de acces susțin în plus detectarea amenințărilor și răspunsul la acestea.

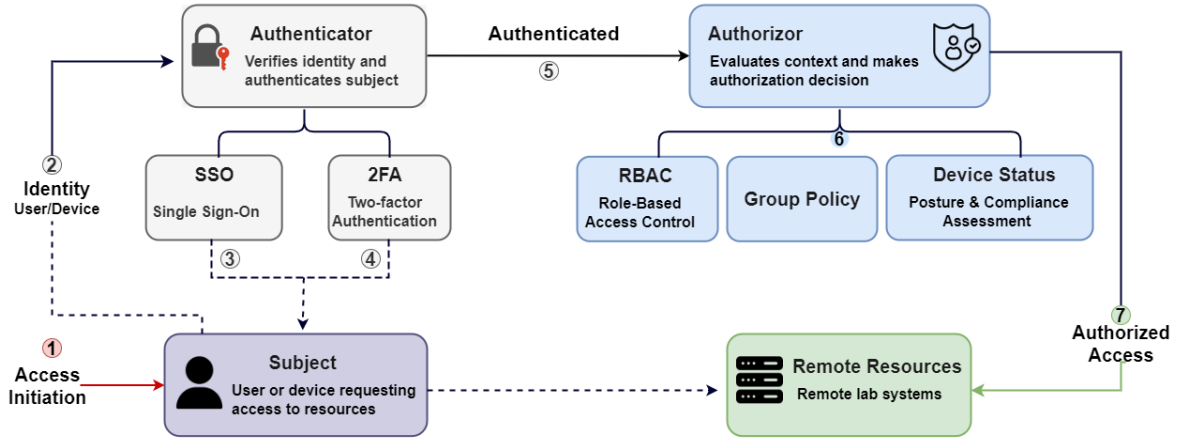


Figura 3.2. Fluxul de lucru al controlului accesului la nivel înalt, de la inițierea de către client până la autorizarea resurselor.

3.2. Discuții

Arhitectura de control al accesului prezentată în acest capitol demonstrează o schimbare fundamentală de la accesul la distanță bazat pe perimetru la un model ZT centrat pe resurse. Spre deosebire de VPN-uri, care acordă acces larg la rețea după autentificare și permit mișcarea laterală, ZTNA aplică verificarea continuă, politici bazate pe identitate și principiile privilegiului minim, eliminând încrederea implicită și restricționând accesul la resursele autorizate în mod explicit.

Implicațiile de securitate ale acestei schimbări sunt ilustrate în Figura 3.3, care prezintă un scenariu de atac prin utilizarea datelor de autentificare furate. În arhitecturile bazate pe VPN, datele de autentificare compromise permit de obicei accesul nelimitat la rețea și mișcarea laterală. În schimb, modelul ZT impune decizii de acces la nivel de resursă bazate pe identitate, starea dispozitivului și politică, refuzând accesul dispozitivelor neautorizate și limitând domeniul de aplicare al accesului, limitând astfel atacul și reducând impactul acestuia.

Dincolo de securitate, ZTNA îmbunătățește scalabilitatea operațională și gestionabilitatea prin înlocuirea configurațiilor centrate pe rețea cu un control al accesului centralizat, bazat pe politici. Acest lucru reduce efortul administrativ, simplifică alocarea drepturilor utilizatorilor și sporește adaptabilitatea în medii dinamice, cum ar fi laboratoarele la distanță. În plus, prin limitarea mișcării laterale, ZTNA reduce impactul potențial și costul incidentelor de securitate.

Cu toate acestea, ZTNA nu detectează în mod inerent activitățile rău intenționate din cadrul sesiunilor autorizate. Amenințările interne, identitățile compromise sau utilizarea abuzivă a privilegiilor legitime pot rămâne nedetectate, în special în sistemele ciber-fizice, unde acțiunile autorizate pot avea consecințe fizice. Prin urmare, deși ZT oferă o bază solidă pentru controlul accesului, aceasta trebuie completată cu mecanisme de monitorizare și de detectare a intruziunilor, aspect care stă la baza capitolelor următoare.

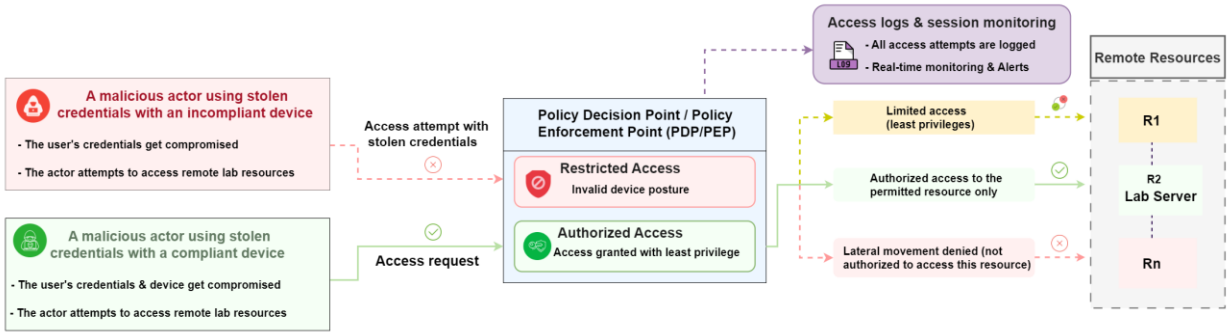


Figura 3.3. Conținerea unui atac cu date de autentificare furate în cadrul unei arhitecturi Zero Trust, ilustrând modul în care aplicarea bazată pe politici (PDP/PEP) și validarea stării dispozitivului restricționează accesul și împiedică mișcarea laterală în cadrul resurselor de inginerie la distanță.

3.3. Concluzia capitolului

Acest capitol a investigat problema accesului la distanță securizat în sistemele de inginerie la distanță, cu accent special pe laboratoarele educaționale online ca medii ciber-fizice reprezentative. Analiza a demonstrat că mecanismele tradiționale de securitate bazate pe perimetru, în special modelele de acces la distanță centrate pe VPN, introduc limitări structurale atunci când sunt aplicate infrastructurilor comune de inginerie la distanță.

Bazându-se pe cadrul ZT al NIST [154], capitolul a propus și a implementat o arhitectură de control al accesului la nivel de resurse, centrată pe identitate și cu un nivel de detaliere ridicat, care elimină încrederea implicită în rețea, impune accesul cu privilegii minime și limitează mișcarea laterală în cadrul infrastructurii laboratorului. Implementarea practică într-un mediu de laborator serial online a confirmat că controlul accesului ZT poate fi integrat în platforme de inginerie la distanță din lumea reală fără a expune topologia rețelei interne sau a acorda privilegii excesive, păstrând în același timp ușurința de utilizare și continuitatea operațională.

O analiză comparativă a evidențiat avantajele abordării ZT față de accesul tradițional bazat pe VPN în ceea ce privește granularitatea accesului, reducerea mișcării laterale și auditabilitatea îmbunătățită. În același timp, capitolul a recunoscut limitările soluțiilor bazate exclusiv pe controlul accesului, în special incapacitatea acestora de a detecta comportamente rău intenționate sau anomale provenite de la utilizatori autorizați sau de la identități compromise.

Prin urmare, acest capitol îndeplinește Obiectivul O2 prin proiectarea, implementarea și validarea unei arhitecturi de control al accesului la nivel de resurse, centrată pe identitate și cu un nivel ridicat de detaliere, adaptată mediilor de laborator online. În consecință, acesta stabilește controlul accesului ZT ca strat fundamental de securitate pentru sistemele de inginerie la distanță, demonstrând eficacitatea acestuia în atenuarea riscurilor asociate modelelor de acces bazate pe perimetru. Cu toate acestea, controlul accesului nu poate aborda singur amenințările ulterioare compromiterii sau comportamentul anormal în cadrul sesiunilor de încredere. Aceste limitări motivează integrarea unor mecanisme complementare de detectare și monitorizare pentru a identifica activitatea anormală în mediile ciber-fizice. Prin urmare, capitolele următoare extind cadrul de securitate prin dezvoltarea unor tehnici eficiente din punct de vedere al resurselor de detectare a intruziunilor și a anomaliilor, adaptate sistemelor de inginerie la distanță bazate pe IoT/IIoT.

Chapter 4. Clasificarea traficului bazată pe învățarea automată, eficientă din punct de vedere al resurselor și orientată către selecția caracteristicilor, pentru atacurile de securitate MQTT-IoT

Acest capitol propune o metodă FS ușoară, denumită Statistical Moments Difference Thresholding (SMDT), care selectează caracteristici discriminative pe baza diferențelor dintre momentele statistice (medie, abatere standard, asimetrie, curtozie). Evaluată pe setul de date MQTTset [100] , metoda demonstrează că se poate obține o reducere semnificativă a caracteristicilor, menținând în același timp o performanță ridicată de detectare. Deși limitată la evaluarea offline, această lucrare stabilește fundamentul metodologic pentru implementarea ulterioară în timp real și integrarea în sistemele IoT/IIoT.

4.1. Metodologie și proiectarea experimentală

Această secțiune descrie proiectul experimental și fluxul metodologic utilizat pentru a studia clasificarea traficului rău intenționat cu utilizare eficientă a resurselor în medii IoT bazate pe MQTT. Metodologia adoptată urmează un proces structurat care cuprinde selectarea setului de date, preprocesarea datelor și analiza exploratorie, selectarea caracteristicilor și clasificarea bazată pe învățare automată (ML). Cadrul general de selectare a caracteristicilor și de clasificare adoptat în acest capitol este ilustrat în Figura 4.1.

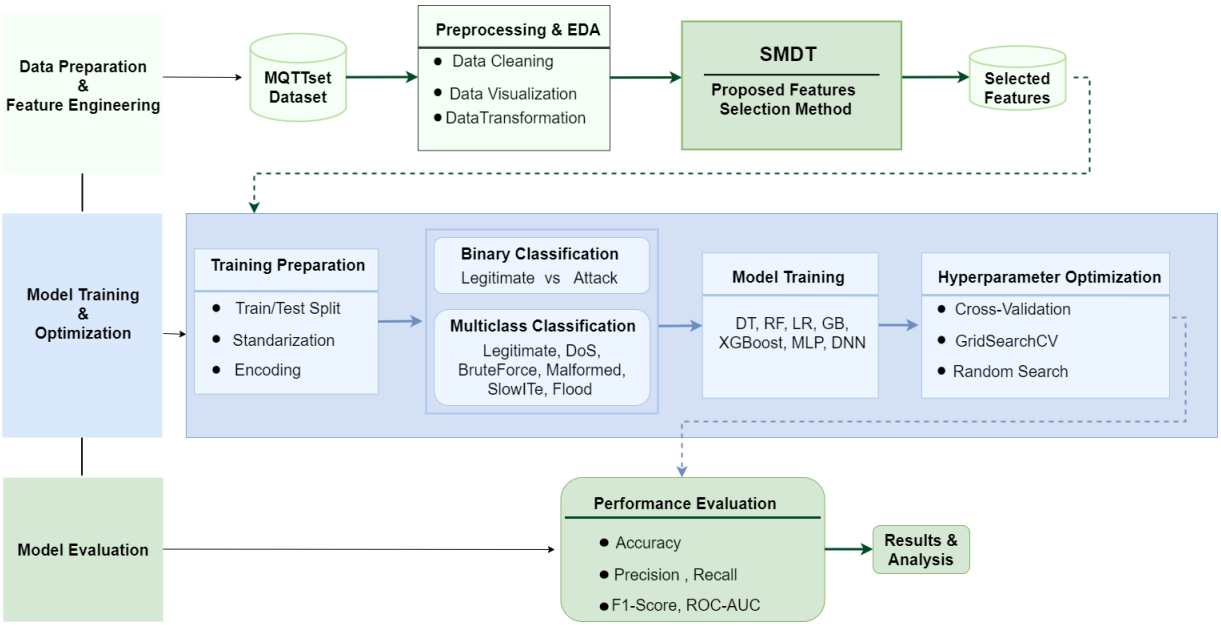


Figura 4.1. Prezentare conceptuală a cadrului de clasificare a traficului adoptat în acest capitol, evidențiind reducerea dimensionalității bazată pe SMDT și fluxul de clasificare binară și multiclasă care urmează.

4.1.1 Descrierea setului de date

Acest studiu utilizează MQTTset, un set de date IoT disponibil public, conceput special pentru a captura comunicațiile MQTT, așa cum este descris în [101] și pus la dispoziție online la [100]. MQTTset a fost generat folosind o rețea de senzori IoT menită să reproducă caracteristicile cheie ale implementărilor bazate pe MQTT din lumea reală. Infrastructura include un broker MQTT implementat folosind Eclipse Mosquitto v1.6.2 și o rețea de opt senzori interconectați, și anume senzori de temperatură, intensitate luminoasă, umiditate, mișcare, gaz CO, fum, controlor de viteză a ventilatorului și senzori de blocare a ușilor, coordonați prin intermediul brokerului. Setul de date rezultat conține atât trafic legitim (benign), cât și trafic rău intenționat (de atac), permițând învățarea supravegheată pentru detectarea intruziunilor în medii IoT compatibile cu MQTT. MQTTset încorporează multiple scenarii de atac care vizează rețelele MQTT [101]. Clasele de atac și distribuția traficului sunt ilustrate în Figura 4.2.

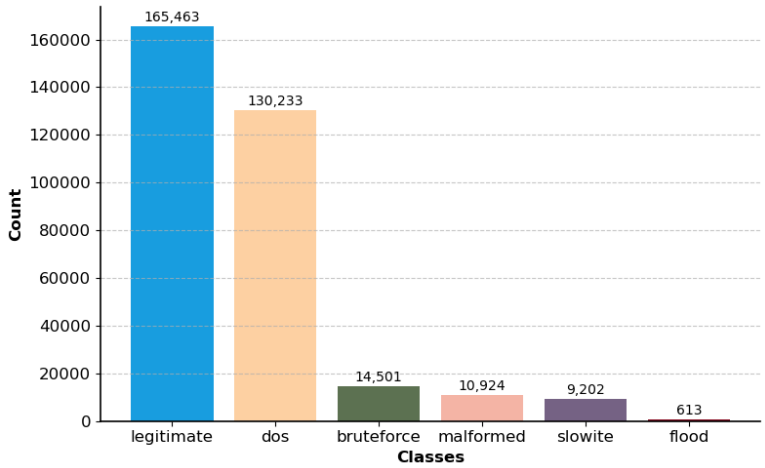


Figura 4.2. Distribuția claselor în setul de date MQTTset redus și echilibrat — tipuri benigne vs. tipuri de atac.

4.1.2 Selectarea caracteristicilor

FS constituie o etapă critică în fluxul de lucru al învățării automate (ML), având ca scop identificarea unui subset de caracteristici informative care contribuie cel mai eficient la performanța predictivă, reducând în același timp redundanța și zgomotul [102]. Prin eliminarea atributelor irelevante sau slab informative, FS atenuează [103] supraînvățarea, reduce complexitatea computațională și abordează provocările de generalizare care sunt deosebit de pronunțate în seturile de date cu dimensiuni mari, descrise în mod obișnuit ca „blestemul dimensionalității”[104]. Aceste considerente sunt deosebit de relevante în mediile IoT și IIoT, unde constrângerile de resurse impun mecanisme de detectare ușoare, dar totuși discriminatorii.

Pentru a aborda aceste provocări, acest studiu introduce metoda SMDT. Abordarea SMDT utilizează primele patru momente statistice centrale[105], media, abaterea standard, asimetria și curtoza, pentru a cuantifica diferențele de distribuție între traficul legitim și cel rău intenționat. Aceste momente au fost selectate datorită capacității lor complementare de a surprinde tendința centrală, dispersia, asimetria și comportamentul cozilor distribuțiilor caracteristicilor [106]. O astfel de caracterizare statistică multidimensională este deosebit de potrivită pentru traficul IoT, care prezintă frecvent distribuții eterogene, negaussiene și puternic asimetrice.

4.2. Proiectarea și evaluarea experimentală

4.2.1 Configurarea și rezultatele clasificării binare

4.2.1.1 Antrenarea și selectarea modelului

Sarcina de clasificare binară a fost definită pentru a distinge traficul MQTT ca fiind legitim (0) sau un atac (1), utilizând setul de date MQTTset redus și echilibrat pentru a remedia dezechilibrul dintre clase. Caracteristicile au fost normalizate utilizând standardizarea Z-score (StandardScaler) pentru a îmbunătăți convergența și performanța modelului [107], [108] , iar setul de date a fost împărțit în seturi de antrenare și testare (70/30) utilizând eșantionarea stratificată pentru a păstra distribuția claselor[109].

Optimizarea modelului a fost realizată folosind GridSearchCV cu validare încrucișată în cinci părți (k = 5) pentru a regla sistematic hiperparametrii și a reduce supraînvățarea. După identificarea configurațiilor optime, modelele au fost reantrenate pe setul complet de antrenament.

Pentru modelul DNN, reglarea hiperparametrilor a fost realizată folosind Keras Tuner cu Random Search, optimizând parametri precum dropout și rata de învățare [110]. Arhitectura rețelei a constat din trei straturi ascunse (64, 32, 16 neuroni) cu activare ReLU și dropout pentru regularizare, precum și un strat de ieșire sigmoid pentru clasificarea binară [111]. Antrenarea a fost realizată folosind optimizatorul Adam și pierderea de entropie încrucișată binară [112] , urmată de reantrenare cu configurația optimă timp de 10 epoci.

4.2.1.2 Evaluarea performanței

Performanța modelelor antrenate a fost evaluată folosind metrici standard de clasificare, inclusiv acuratețea, precizia, recall-ul și scorul F1. Pentru a obține o înțelegere mai aprofundată a comportamentului de predicție, au fost analizate matricile de confuzie pentru toate modelele. Matricea de confuzie prezintă distribuția rezultatelor pozitive adevărate (TP), a rezultatelor negative adevărate (TN), a rezultatelor pozitive false (FP) și a rezultatelor negative false (FN). Indicatorii de performanță consolidați pentru toate modelele evaluate sunt rezumați în Tabelul 4.1. Timpul de căutare (s) reflectă durata procesului de optimizare a hiperparametrilor, inclusiv GridSearchCV pentru modelele convenționale și Random Search prin Keras Tuner pentru DNN. În plus, Figura 4.3 prezintă matricile de confuzie pentru toate modelele.

Tabelul 4 .1 . Indicatori de performanță pentru clasificarea binară și timpii de calcul.

Model	Precizie	Precizie	Recall	Scorul F1	AUC ROC	Timp de căutare (s)	Timp de antrenare (s)	Timp de testare (s)
RF	0,95	0,95	0,95	0,95	0,99	2280,81	6,96	0,45
LR	0,95	0,95	0,95	0,95	0,99	221,58	11,27	0,99
DT	0,95	0,95	0,95	0,95	0,99	74,98	0,12	0,01
GB	0,95	0,95	0,95	0,95	0,99	3051,20	43,08	0,45
XGBOOST	0,95	0,95	0,95	0,95	0,99	1252,83	12,38	0,04
MLP	0,89	0,91	0,89	0,89	0,95	3551,45	264,61	0,20
DNN	0,81	0,85	0,81	0,80	0,92	5602,99	722,57	6,44

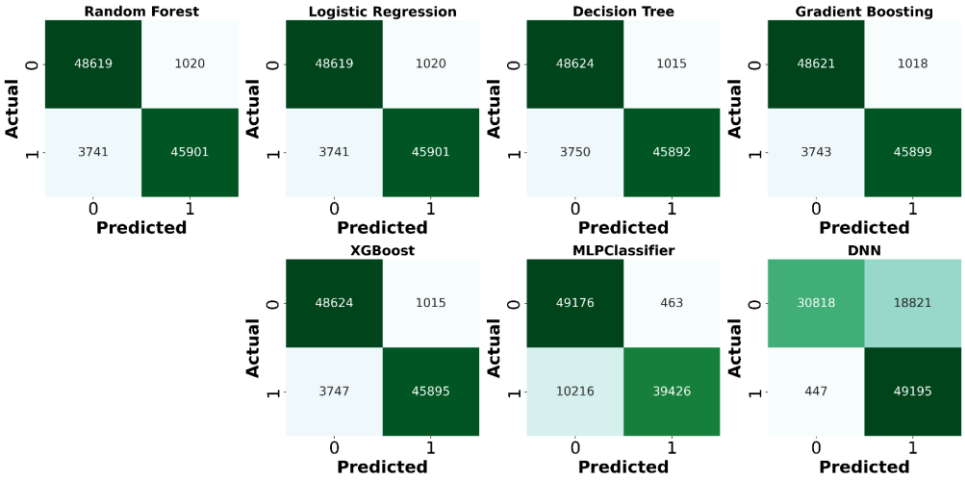


Figura 4.3. Matrici de confuzie pentru toate modelele evaluate (clasificare binară).

4.2.2 Configurarea și rezultatele clasificării multiclasă

În urma experimentelor de clasificare binară, care s-au concentrat pe distingerea traficului MQTT legitim de cel rău intenționat, analiza a fost extinsă la o configurație de clasificare multiclasă. Această extindere permite identificarea unor categorii specifice de atacuri: forță brută, DoS, flooding, date malformate și SlowITe. Această granularitate susține atât caracterizarea precisă a amenințărilor, cât și strategiile de

atenuare țintite. În această configurație, sarcina de clasificare implică șase clase distincte, comparativ cu formularea cu două clase adoptată în scenariul binar.

Performanța modelului a fost evaluată folosind metrici adaptați din cazul clasificării binare. Mai precis, evaluarea a cuprins următoarele componente:

a) Raport de clasificare: Pentru fiecare model au fost calculate acuratețea, precizia, recall-ul și scorul F1. Rezultatele agregate sunt prezentate în Tabelul 4.2. Timpul de căutare prezentat în tabel indică timpul necesar pentru optimizarea hiperparametrilor înainte de antrenarea finală a modelului.

Tabelul 4.2. Performanța modelului: Indicatori de evaluare și timpi de căutare (multiclasă).

Model	Acuratețe	Precizie	Recuperare	Scor F1	Timp de căutare (s)	Timp de antrenare (s)	Timp de testare (s)
RF	0,91	0,90	0,91	0,90	1547,43	16,21	1,15
LR	0,79	0,79	0,79	0,75	1834,67	8,00	0,01
DT	0,91	0,91	0,91	0,90	9,24	0,12	0,01
GB	0,91	0,91	0,91	0,90	24489,46	505,96	4,80
XGBOOST	0,91	0,91	0,91	0,90	49323,92	15,75	0,06
MLP	0,82	0,85	0,82	0,80	3573,60	141,93	0,11
DNN	0,78	0,77	0,78	0,74	5081,92	702,20	6,03

b) Matricea de confuzie: Pentru a analiza comportamentul de predicție în toate categoriile de atacuri, au fost generate matrici de confuzie pentru fiecare model. În configurația multiclasă, matricea de confuzie se extinde la o grilă N × N, unde N corespunde numărului de clase. Fiecare celulă reprezintă numărul de instanțe asociate cu o anumită pereche de clase reale/prevăzute, permițând o inspecție detaliată a modelelor de clasificare. Pentru concisitate, Figura 4.4 prezintă matricea de confuzie numai pentru modelul RF.

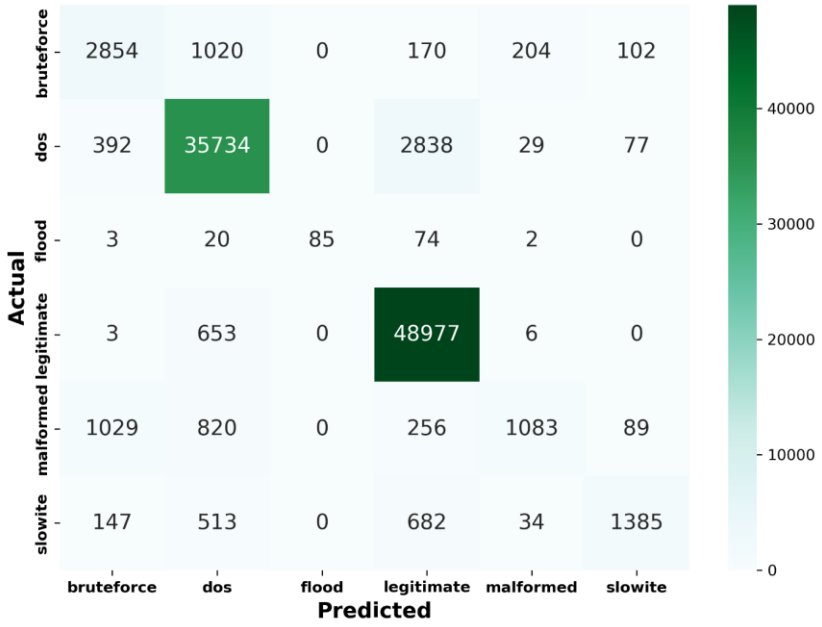


Figura 4.4. Matricea de confuzie — Random Forest (multiclasă).

4.3. Discutarea rezultatelor

Pentru clasificarea binară, modelele clasice de învățare automată (DT, RF, GB, XGBoost) au prezentat performanțe solide și consistente, atingând valori ale acurateței, preciziei, recall-ului și scorului F1 de aproximativ 0,95, cu valori AUC ale curbei ROC apropiate de 0,99 (a se vedea Tabelul 4.1). În schimb, modelele bazate pe rețele neuronale au demonstrat performanțe comparativ mai scăzute. Modelul MLP a atins o acuratețe moderată (0,89), în timp ce rețeaua neuronală profundă (DNN) a atins o acuratețe de 0,81 și un AUC al curbei ROC de 0,92.

În plus, matricile de confuzie (a se vedea Figura 4.3) oferă informații suplimentare cu privire la caracteristicile erorilor modelelor evaluate. Deși rețeaua neuronală profundă (DNN) a prezentat o precizie generală mai scăzută, aceasta a demonstrat o sensibilitate ridicată, identificând corect o proporție mare de instanțe de atac (49.195) și generând un număr mai mic de rezultate fals negative (447). Acest comportament a fost însă însoțit de un număr substanțial mai mare de rezultate fals pozitive (18.821), ceea ce indică o specificitate limitată și o tendință de a genera alarme false în exces, așa cum se reflectă și în Figura 4.7. Un astfel de comportament poate fi nedorit în mediile operaționale în timp real, unde alertele false frecvente pot duce la o utilizare ineficientă a resurselor și la oboseală cauzată de alerte. În schimb, MLP a prezentat un profil de eroare opus, generând mai puține rezultate fals pozitive (463), dar mai multe rezultate fals negative (10.216). Deși acest lucru reduce alertele inutile, crește riscul de a omite atacuri. Aceste rezultate subliniază importanța echilibrării sensibilității de detectare și a fiabilității operaționale în implementările în timp real.

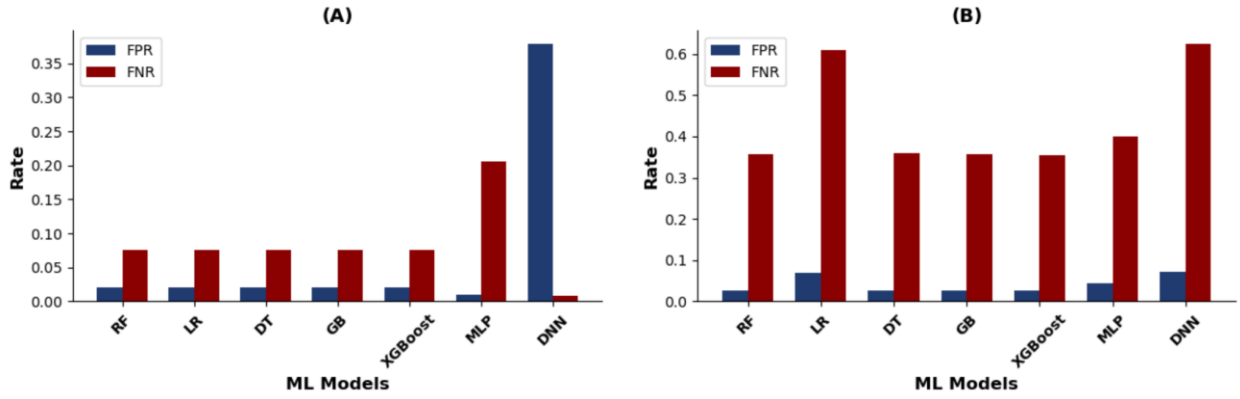


Figura 4.5. FPR și FNR pentru diferite modele de învățare automată: (A) cazul clasificării binare și (B) cazul clasificării multiclasă.

În scenariul multiclasă, performanța s-a degradat la toate modelele din cauza dezechilibrului între clase și a complexității crescute a sarcinii. Modelele de tip ansamblu și cele bazate pe arbori (RF, DT, GB și XGBoost) au menținut o performanță relativ stabilă, cu precizie și scoruri F1 în jur de 0,90 (a se vedea Tabelul 4.2), în timp ce LR, MLP și DNN au prezentat o eficacitate mai scăzută. Matricea de confuzie (a se vedea Figura 4.5) indică faptul că majoritatea clasificărilor eronate au avut loc în clasele de atac minoritare, precum „malformed", „SlowITe" și „flooding", sugerând că discriminarea claselor rare rămâne o provocare chiar și după reducerea caracteristicilor.

Timpul de antrenare și de optimizare a variat substanțial de la un model la altul (a se vedea Figura 4.6). Metodele bazate pe arbori s-au dovedit în mod constant cele mai eficiente, în timp ce MLP și DNN au generat o sarcină de procesare semnificativ mai mare.

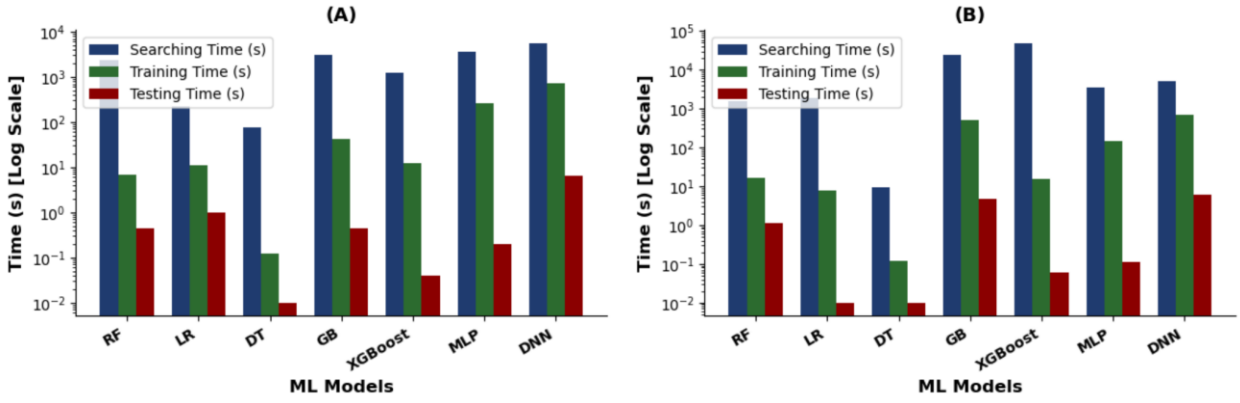


Figura 4.6. Timpul de calcul pentru diferite modele de învățare automată: (A) cazul clasificării binare și (B) cel al clasificării multiclasă.

4.4. Selectarea modelului și implicații practice

Din perspectiva implementării, rezultatele indică faptul că modelele DT și RF oferă cel mai bun compromis între performanța de detectare și eficiența computațională pentru mediile de inginerie la distanță bazate pe IoT, cu resurse limitate. DT, în special, oferă o latență redusă atât la antrenare, cât și la inferență, ceea ce îl face potrivit pentru monitorizarea în timp real. Deși abordările de tip ansamblu, precum GB și XGBoost, ating performanțe ridicate de detectare, cerințele lor de calcul mai mari le fac mai potrivite pentru medii mai puțin limitate din punct de vedere al resurselor. În schimb, modelele MLP și DNN prezintă un raport performanță-cost mai scăzut pentru implementarea online. În ansamblu, selecția modelului ar trebui să ia în considerare nu numai acuratețea, ci și latența, utilizarea resurselor și compromisurile legate de erori, modelele bazate pe arbori demonstrând un profil echilibrat, potrivit pentru detectarea practică a intruziunilor în rețelele IoT.

4.5. Concluzia capitolului

Acest capitol a abordat detectarea traficului rău intenționat în sistemele de inginerie la distanță IoT/IIoT bazate pe MQTT, evidențiind limitările apărării bazate exclusiv pe controlul accesului și necesitatea unor mecanisme complementare de detectare a intruziunilor. Capitolul contribuie la obiectivul O3 prin dezvoltarea și validarea unui cadru de clasificare a traficului bazat pe selecția caracteristicilor, adaptat mediilor cu resurse limitate bazate pe MQTT. A fost propus un cadru de învățare automată eficient din punct de vedere al resurselor, centrat pe metoda de selecție a caracteristicilor SMDT, care reduce dimensionalitatea caracteristicilor, păstrând în același timp performanța de detectare.

Rezultatele experimentale pe setul de date MQTTset au arătat că reducerea setului de caracteristici de la 33 la 5 menține o performanță competitivă atât în clasificarea binară, cât și în cea multiclasă, în special atunci când se utilizează modele ușoare, precum arborii de decizie și pădurile aleatorii. Analiza a relevat, de asemenea, compromisuri cheie, indicând faptul că modelele mai simple, combinate cu o selecție eficientă a caracteristicilor, oferă un echilibru mai bun între precizie și costul de calcul decât abordările mai complexe în medii cu resurse limitate.

Cu toate acestea, evaluarea s-a limitat la condiții offline și nu a luat în considerare constrângerile în timp real sau integrarea sistemului. Prin urmare, acest capitol stabilește bazele pentru Capitolul 5, care extinde lucrarea către implementarea în timp real și evaluarea operațională în medii IoT/IIoT.

Chapter 5. Dezvoltarea unei arhitecturi modulare pentru detectarea în timp real a intruziunilor bazată pe învățare automată în mediile IoT/IIoT, cu integrare SIEM în cloud care respectă confidențialitatea

Acest capitol propune un cadru IDS ușor, care respectă confidențialitatea și bazat pe ML, adaptat mediilor de monitorizare și control la distanță din IoT/IIoT. Arhitectura pune accentul pe inferența la marginea rețelei pentru detectarea în timp real, pe minimizarea strictă a datelor prin păstrarea traficului brut la nivel local și pe transmiterea selectivă a alertelor structurate către un sistem SIEM bazat pe cloud. În plus, introduce un mecanism dinamic de comutare a modelului în timpul rulării, care permite adaptarea flexibilă la amenințările în continuă evoluție, fără a întrerupe funcționarea sistemului. Cadrul este validat prin scenarii simulate de atac bazate pe MQTT, demonstrându-și fezabilitatea pentru implementarea în timp real.

5.1. Proiectarea arhitecturii sistemului

Această secțiune prezintă arhitectura și implementarea sistemului propus de detectare a intruziunilor bazat pe învățare automată (ML), destinat mediilor de monitorizare și control la distanță pentru IoT/IIoT. Sistemul adoptă un design modular, stratificat, care suportă achiziția datelor de la senzori, inferența în timp real a învățării automate la marginea rețelei (edge) și transmiterea securizată a rezultatelor detectării către o platformă SIEM bazată pe cloud, și anume Microsoft Sentinel. Așa cum se ilustrează în Figura 5.1, sistemul implementat cuprinde mai multe straturi funcționale, fiecare fiind responsabil pentru un set distinct de operațiuni.

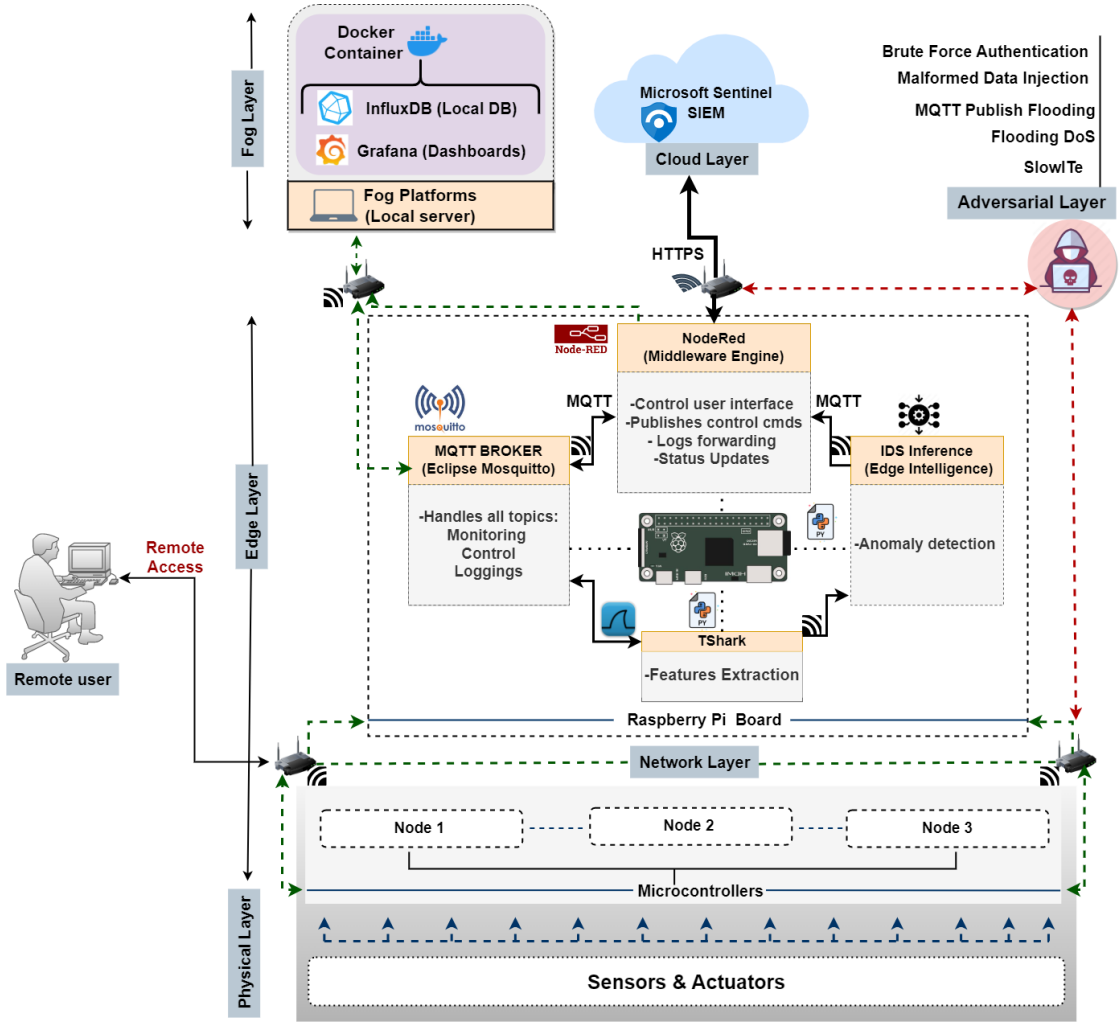


Figura 5.1. Arhitectura generală a platformei de testare Edge-Cloud IDS propusă.

5.2. Integrarea și comunicarea platformelor de sistem

5.2.1 Achiziția datelor la nivel de senzor

Stratul fizic constă în senzori distribuiți pe mai multe noduri de microcontrolere pentru a sprijini monitorizarea mediului și a securității. Așa cum se arată în Figura 5.2, un nod bazat pe Arduino colectează date de la componente ultrasonice, de vibrații și relee și le transmite prin comunicare serială către un nod ESP32, care agregă și publică datele către subiecte MQTT. Un al doilea nod ESP32 gestionează independent senzori suplimentari (flacără, gaz, temperatură/umiditate) și actuatori, permițând comunicarea bidirecțională prin intermediul subiectelor de control pentru funcționarea în buclă închisă. Toate nodurile ESP32 utilizează o configurație MQTT standardizată, transmițând date periodic (la fiecare 10 secunde) și prin actualizări declanșate de evenimente.

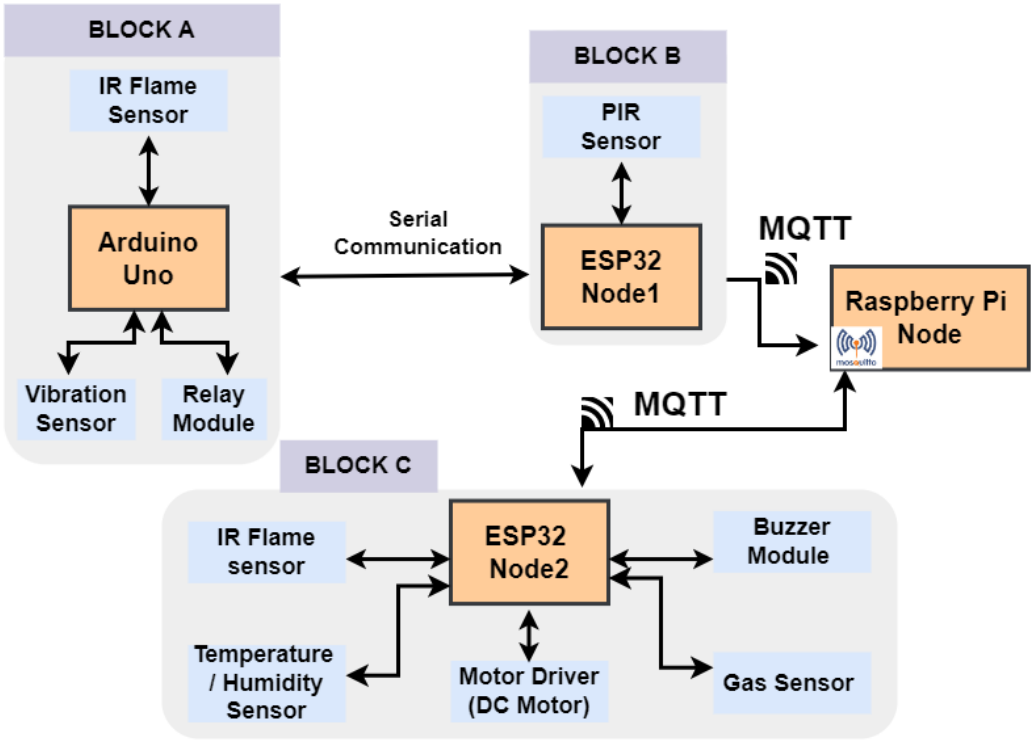


Figura 5.2. Arhitectura de achiziție a datelor și de comunicare la nivel de senzor.

5.2.2 Middleware bazat pe Node-RED și stratul de integrare

Node-RED este utilizat ca strat de middleware pentru a coordona comunicarea, procesarea datelor și integrarea în cadrul sistemului și este implementat pe un nod de margine Raspberry Pi. Acesta permite fluxuri de lucru în timp real, bazate pe evenimente, pentru achiziția datelor, transformarea acestora și interacțiunea cu servicii externe.

Platforma îndeplinește două funcții principale: (i) agregarea și monitorizarea datelor de la senzori și (ii) integrarea rezultatelor inferenței ML și a telemetriei de securitate. Aceasta se abonează la subiecte MQTT, prelucrează și formatează datele primite. Le transmite către InfluxDB pentru stocare și către un sistem SIEM bazat pe cloud pentru analiză, vizualizarea fiind asigurată prin intermediul tablourilor de bord Grafana.

În plus, Node-RED suportă controlul bidirecțional al dispozitivelor, permițând atât acțiuni automatizate bazate pe intrările senzorilor, cât și controlul manual prin intermediul unei interfețe web. Un mecanism

de feedback care utilizează subiecte de stare MQTT asigură sincronizarea între comenzi și stările actuatoarelor, îmbunătățind fiabilitatea sistemului și conștientizarea operațională în timp real.

5.2.3 Integrare în cloud cu protejarea confidențialității

Sistemul utilizează o strategie hibridă de înregistrare care protejează confidențialitatea, în care toate datele brute de trafic (de exemplu, încărcăturile pachetelor, identificatorii dispozitivelor și parametrii operaționali) rămân la marginea rețelei. În același timp, doar alertele structurate și metadatele minime sunt transmise către sistemul SIEM din cloud. Această abordare reduce riscurile de expunere a datelor , susține confidențialitatea și minimizează utilizarea lățimii de bandă, aliniindu-se la principiile de minimizare a datelor, precum cele din GDPR [113] și liniile directoare NIST [114].

Node-RED prelucrează rezultatele inferenței ML din subiectul MQTT „model/prediction” și transmite mai departe doar metadate compacte în format JSON, inclusiv marcajul temporal, clasa de atac prevăzută, versiunea modelului și atributele contextuale selectate. Nu se transmit pachete brute, caracteristici sau date de la senzori, asigurându-se astfel că datele operaționale sensibile rămân la nivel local.

Așa cum se ilustrează în Figura 5.3, datele de telemetrie sunt transmise în siguranță către Microsoft Sentinel prin intermediul API-ului Azure Monitor HTTP Data Collector, utilizând HTTPS criptat cu TLS și autentificare HMAC-SHA256. Odată preluate, datele sunt stocate în Azure Log Analytics, permițând interogări bazate pe KQL, vizualizare și răspuns automat la incidente.

Această strategie de integrare care protejează confidențialitatea oferă mai multe avantaje practice. Sistemul rămâne pe deplin operațional la marginea rețelei în timpul întreruperilor de conectivitate la cloud, asigurând capacități de detectare neîntrerupte. În același timp, respectarea principiilor de minimizare a datelor susține cerințele de reglementare, în timp ce volumul redus de jurnale scade costurile de stocare și procesare în cloud.

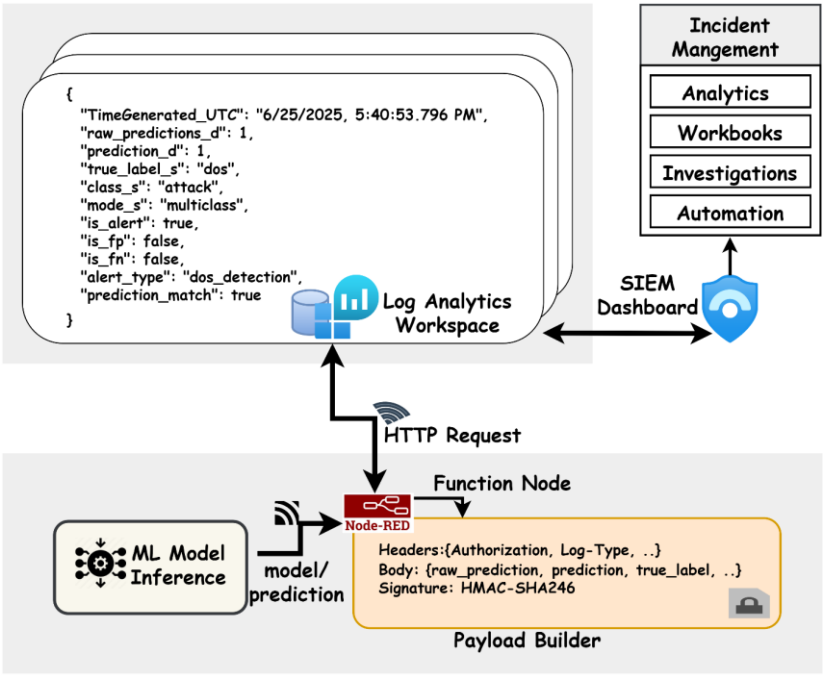


Figura 5.3. Arhitectură pentru transmiterea rezultatelor detectării la nivel de margine către sistemul SIEM din cloud.

5.2.4 Modelul amenințărilor și scenariile de atac

Această capitol definește un model de amenințări care vizează sistemele IoT/IIoT bazate pe MQTT implementate în medii de rețea nesigure sau slab segmentate. În modelul adversarial luat în considerare, un atacator obține acces la același segment de rețea ca și dispozitivele legitime și exploatează

vulnerabilitățile din mecanismele de comunicare MQTT pentru a degrada performanța sistemului, a perturba livrarea datelor sau a compromite confidențialitatea și disponibilitatea. Acest model de amenințare reflectă vectori de atac realiști, observați frecvent în implementările industriale și IoT care nu dispun de un control puternic al accesului, de segmentare a rețelei sau de monitorizare continuă. Figura 5.4 ilustrează atacurile simulate și instrumentele utilizate.

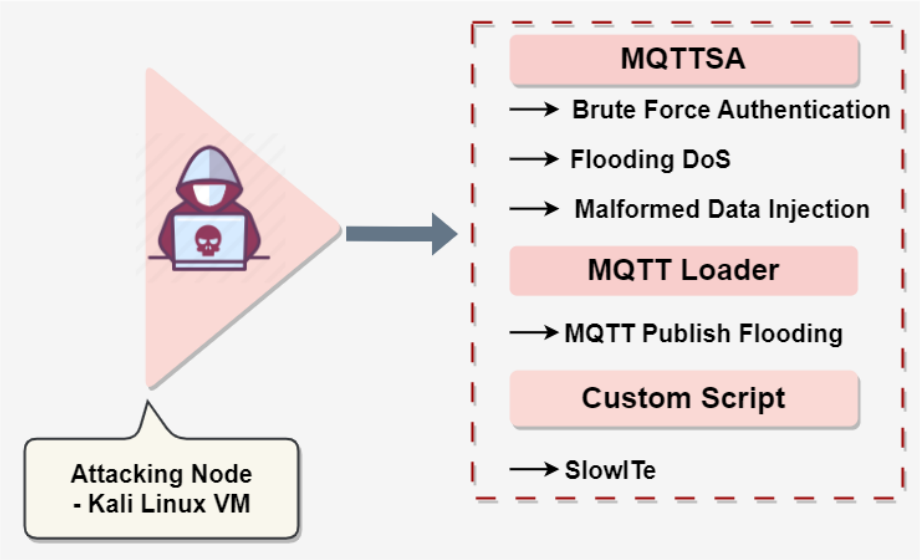


Figura 5.4. Atacuri simulate și instrumente utilizate.

5.3. Inferența în învățarea automată

Inferența reprezintă etapa din ciclul de viață al învățării automate în care un model antrenat este implementat pentru a genera predicții asupra unor date noi, nevăzute[115] . În această capitol , modelele antrenate offline pe setul de date MQTTset (Capitolul 4) sunt implementate într-un flux de detectare bazat pe periferie în timp real.

Pentru a echilibra precizia și eficiența computațională, au fost selectate clasificatoare DT ușoare pentru implementarea pe dispozitive de margine cu resurse limitate. În același timp, modelele mai complexe (de exemplu, abordările de tip ansamblu și neuronale) sunt rezervate pentru medii cu capacitate mai mare. Motorul de inferență este implementat sub forma unui script ușor care rulează pe un Raspberry Pi Zero 2 W (512 MB de RAM), în care modelele pre-antrenate sunt serializate cu ajutorul funcției pickle din Python și încărcate în timpul rulării.

Așa cum este ilustrat în Figura 5.5, sistemul se abonează la subiectul MQTT „traffic/analysis”, procesează vectorii de caracteristici primiți în conformitate cu schema de antrenare și efectuează clasificarea în timp real. Predicțiile sunt publicate în subiectul „model/prediction”, stocate local în InfluxDB pentru înregistrare și analiză criminalistică și formatate pentru transmiterea către sistemul SIEM din cloud, permițând monitorizarea centralizată în timp ce se menține procesarea la marginea rețelei.

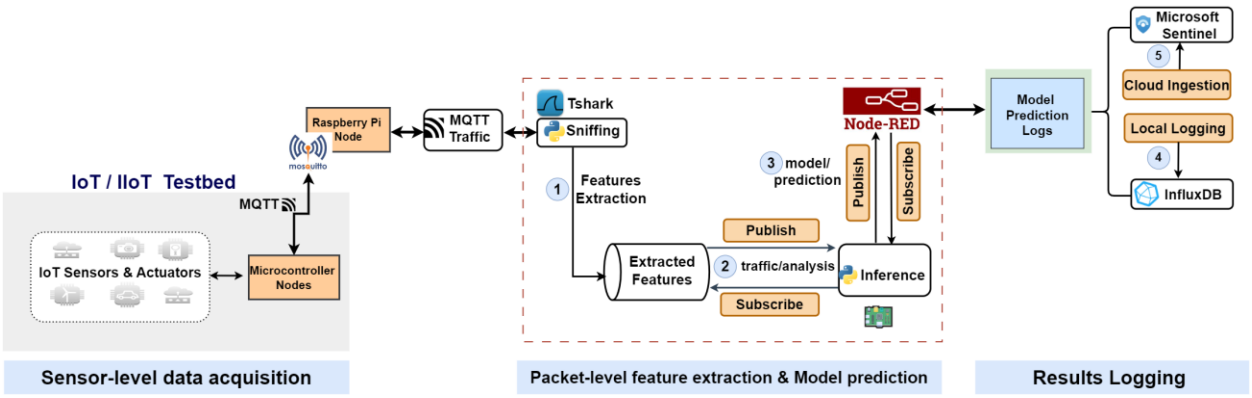


Figura 5.5. Flux de lucru end-to-end de inferență în timp real și redirecționare a alertelor.

5.3.1 Mecanism de comutare a modelului în timpul rulării pentru inferența adaptivă a IDS

Punerea în funcțiune a modelelor ML în producție necesită mecanisme de monitorizare, actualizare și înlocuire a modelelor fără a perturba funcționarea sistemului [116]. Pentru a rezolva această problemă, IDS-ul propus încorporează un mecanism ușor de comutare a modelelor în timpul rulării, aliniat la paradigmele ML adaptiv și de detectare a intruziunilor, în care modelele evoluează ca răspuns la datele în schimbare și la tiparele de amenințări [116], [117].

Mecanismul permite actualizări dinamice ale modelelor prin intermediul mesajelor de control bazate pe MQTT. Așa cum se ilustrează în Figura 5.6, un operator autorizat poate declanșa o comutare de model prin trimiterea unei comenzi JSON structurate care specifică modelul țintă și parametrii de configurare. După validare, motorul de inferență încarcă noul model în timpul rulării și actualizează setările relevante, inclusiv modul de clasificare (binar sau multiclasă), corespondențele etichetelor și configurațiile de înregistrare.

Această abordare oferă flexibilitate operațională, permițând tranziții fluide între modurile de detectare, activarea modelelor specializate pentru tipuri specifice de atacuri și implementarea modelelor recent reantrenate fără a întrerupe monitorizarea. De asemenea, aceasta permite revenirea la modelele validate anterior în cazul apariției unor probleme de performanță. În ansamblu, proiectarea decuplează ciclul de viață al modelului de fluxul de monitorizare, permițând adaptarea continuă, menținând în același timp stabilitatea și disponibilitatea sistemului.

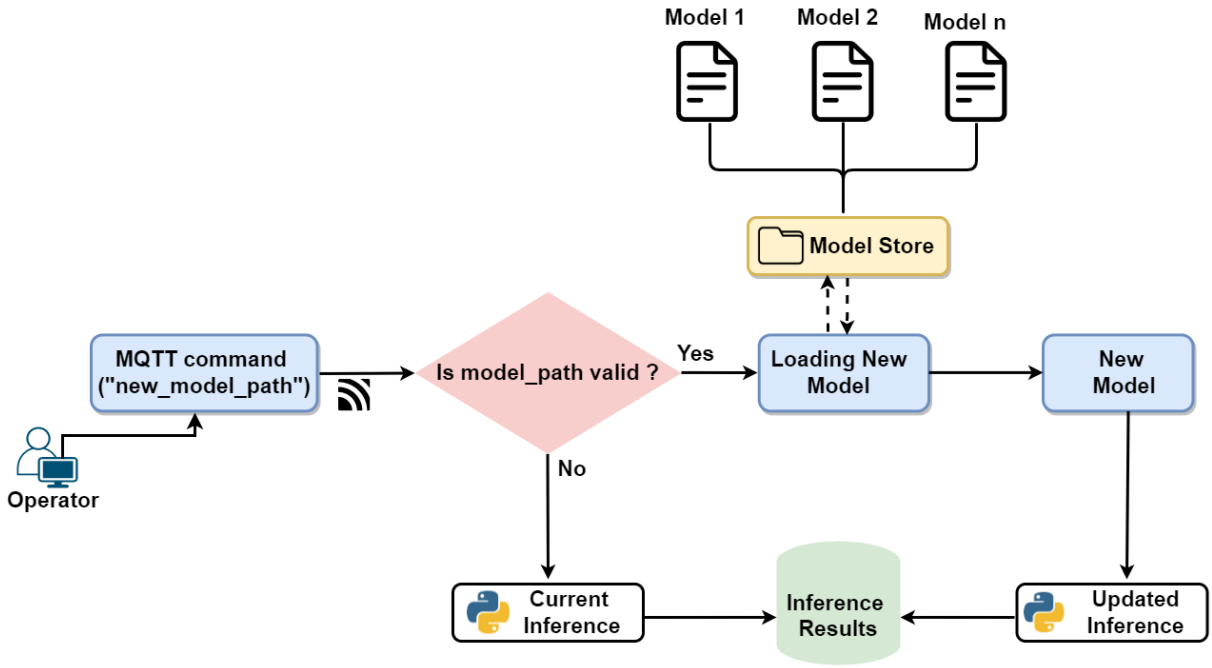


Figura 5.6. Flux de lucru de comutare a modelului în timpul rulării, care permite implementarea dinamică a modelelor alternative de inferență IDS prin comenzi de control bazate pe MQTT.

5.4. Rezultate, evaluarea performanței și analiza la nivel de sistem

5.4.1 Analiza performanței și a preciziei detectării

Sistemul de inferență bazat pe dispozitive periferice a atins o precizie medie de clasificare de 74,04% pe parcursul unei perioade de observare de 30 de zile în cadrul clasificării atacurilor multiple. Aceasta reprezintă o reducere semnificativă față de precizia de 91% obținută în timpul antrenării offline.

Această diferență de performanță reflectă diferențele de distribuție dintre mediile de antrenare și cele de implementare și evidențiază impactul devierii conceptuale și al modelelor de trafic în continuă evoluție din sistemele IoT/IIoT din lumea reală. Reprezentativitatea limitată a setului de date de antrenare în ceea ce privește variabilitatea operațională poate contribui, de asemenea, la această degradare, reducând transferabilitatea limitelor de decizie învățate [118].

Așa cum demonstrează rezultatele, evaluarea offline nu poate surprinde pe deplin complexitatea implementărilor în timp real. Menținerea preciziei de detectare pe termen lung în medii live necesită învățare adaptivă și reantrenarea periodică a modelului, aspecte considerate direcții pentru lucrări viitoare.

5.4.2 Performanța în ceea ce privește latența și debitul

Măsurătorile de latență au confirmat fezabilitatea implementării inferenței bazate pe învățarea automată la marginea rețelei. În medie, sistemul a atins o latență de inferență de 9,32 ms, în timp ce latența totală de la un capăt la altul, inclusiv descărcarea în cloud, a fost de 22,62 ms.

Așa cum se ilustrează în Figura 5.7, s-a observat o latență maximă de 50,9 ms în perioadele cu intensitate ridicată a traficului. Aceste vârfuri au fost atribuite în principal conflictelor de acces la CPU pe Raspberry Pi Zero 2 W.

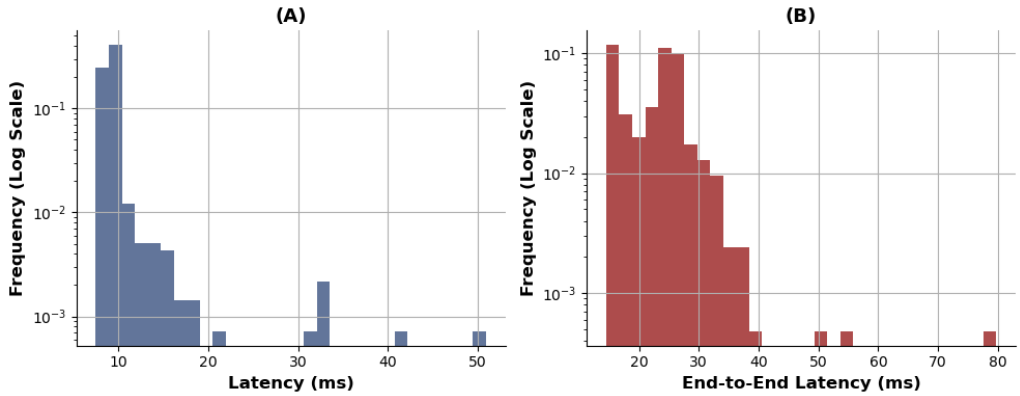


Figura 5.7. Distribuția latenței (A) și a latenței de la capăt la capăt (B) pentru sistemul de inferență implementat.

Analiza debitului a arătat că sistemul a menținut o rată medie de procesare de 4,95 predicții pe secundă. Figura 5.8 ilustrează variabilitatea debitului, cu scăderi ocazionale la 1,24 predicții pe secundă și vârfuri de 13,43 predicții pe secundă în timpul scenariilor de atac intens. Atacurile de tip „flooding” și cele cu pachete malformate au generat cele mai mari sarcini de procesare, ducând la reduceri tranzitorii ale capacității de răspuns.

Rezultatele privind latența și debitul demonstrează că inferența ușoară bazată pe periferie este viabilă pentru volume moderate de trafic. Cu toate acestea, mediile industriale cu debit ridicat ar putea avea nevoie de scalare orizontală sau de accelerare hardware pentru a menține o performanță constantă.

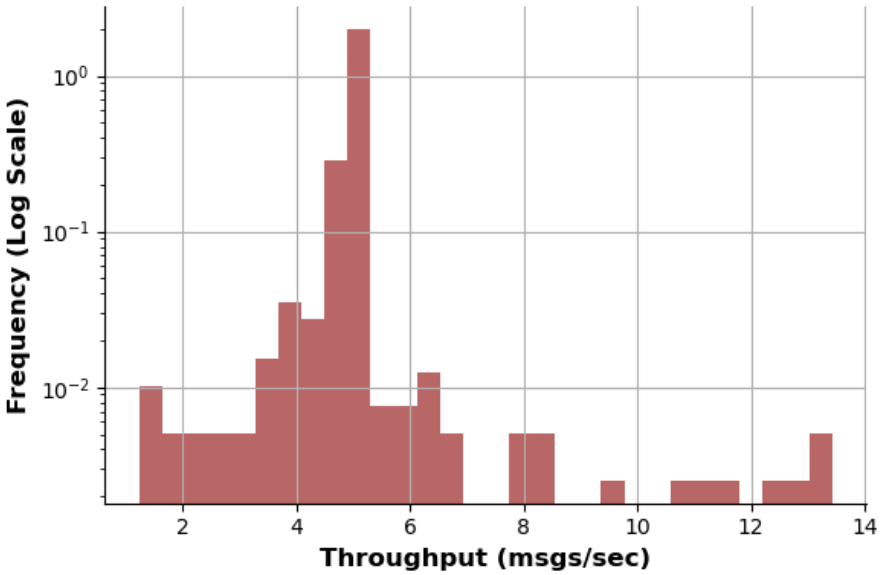


Figura 5.8. Distribuția debitului pentru sistemul de inferență implementat.

5.4.3 Adaptarea la timpul de execuție și suprasarcina generată de comutarea modelelor

Pentru a evalua suprasarcina introdusă de mecanismul de comutare a modelelor în timpul rulării, s-a măsurat pe nodul de margine latența necesară pentru încărcarea și activarea noilor modele în timpul execuției.

Latența de comutare a variat între 2,28 ms și aproximativ 200 ms, reflectând variațiile în ceea ce privește dimensiunea modelului și disponibilitatea resurselor pe platforma Raspberry Pi. Este important de menționat că procesul de comutare a rămas fără blocaje. Odată ce noul model a fost încărcat, inferența a fost reluată fără a fi necesară repornirea serviciului sau o întrerupere prelungită a funcționării.

5.4.4 Integrarea în cloud, validarea operațională și eficiența costurilor

A. Integrarea în cloud și validarea operațională

Rezultatele clasificării generate de motorul de inferență au fost publicate într-un subiect MQTT local și redirecționate de Node-RED către Azure Log Analytics pentru a fi preluate în Microsoft Sentinel. Această integrare hibridă păstrează avantajele monitorizării bazate pe SIEM centrate pe cloud, rămânând în același timp compatibilă cu constrângerile operaționale ale mediilor IoT/IIoT cu resurse limitate și sensibile la confidențialitate.

În cadrul platformei SIEM, jurnalele preluate erau stocate în tabele personalizate, permițând analiștilor să definească reguli de detectare, să coreleze alertele cu informațiile externe privind amenințările și să vizualizeze evenimentele de securitate prin intermediul unor tablouri de bord interactive. Așa cum se ilustrează în Figura 5.9, Sentinel agregă jurnalele de predicție în timp și generează automat incidente pentru scenarii de atac cu grad ridicat de încredere. Interfața de gestionare a incidentelor servește drept punct principal de acces pentru analiști, oferind o vizibilitate consolidată asupra alertelor și entităților afectate. Această interfață facilitează investigarea rapidă și sprijină evaluarea eficientă a potențialelor încălcări de securitate. În plus, registrele de lucru Microsoft Sentinel oferă vizualizări cantitative și interactive care îmbunătățesc vizibilitatea operațională și sprijină analiza de securitate. Aceste registre de lucru permit analiștilor să examineze tendințele istorice, distribuția atacurilor și variațiile temporale ale rezultatelor detectării.

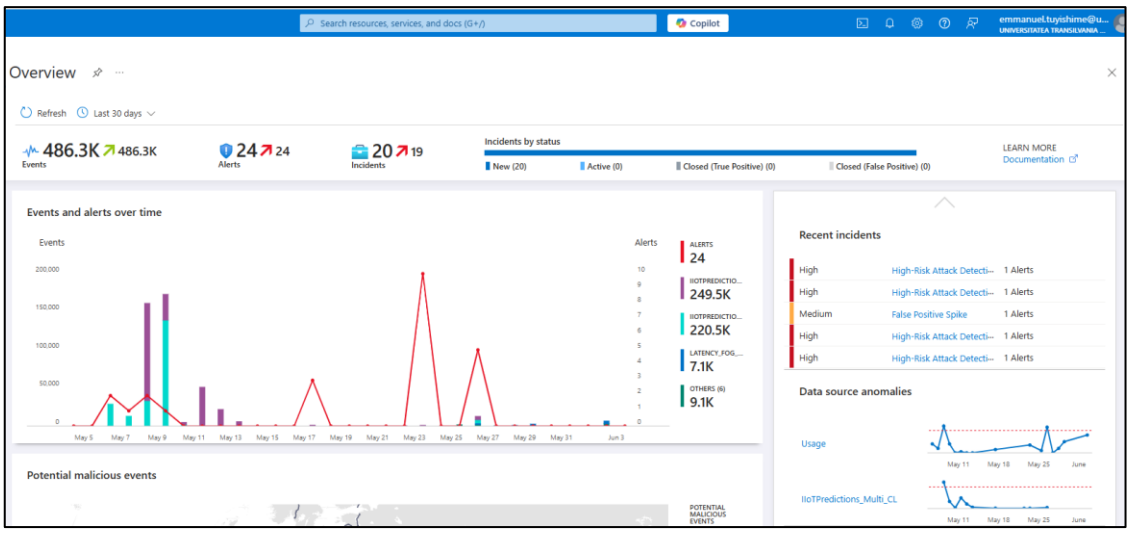


Figura 5.9. Prezentare generală a incidentelor și agregarea alertelor în Microsoft Sentinel pe baza jurnalelor de inferență la nivel de margine.

B. Eficiența costurilor și utilizarea resurselor cloud

Cadrul propus a fost evaluat din perspectiva consumului de resurse cloud în cadrul modelului de facturare bazat pe volum al Microsoft Sentinel, în care costurile variază în funcție de ingestia, procesarea și păstrarea datelor. Pentru a reduce cheltuielile operaționale, arhitectura adoptă o abordare de telemetrie selectivă, transmițând către cloud doar metadate compacte de predicție, în timp ce jurnalele detaliate sunt păstrate local în InfluxDB.

Pe parcursul unei evaluări de o lună, sistemul a procesat aproximativ 4,95 predicții pe secundă, fiecare înregistrare având o dimensiune medie de aproximativ 500 de bytes . Acest lucru a dus la un volum estimat de preluare zilnică de aproximativ 204 MB (6,1 GB pe lună). Pe baza tarifelor Sentinel (4,47 €/GB)[119] , costul lunar corespunzător este de aproximativ 27 €.

În schimb, soluțiile IDS convenționale centrate pe cloud, care transmit date la nivel de flux sau de pachet (2–5 KB per eveniment), ar genera 24–61 GB pe lună, generând costuri de aproximativ 109–272 €. Astfel, abordarea propusă realizează o reducere de 75–90% a volumului de date preluate, îmbunătățind

semnificativ eficiența din punct de vedere al costurilor. Această reducere permite implementări mai scalabile și mai sustenabile din punct de vedere economic, deoarece costurile de cloud cresc mai lent odată cu extinderea sistemului, întrucât sunt transmise doar rezultatele inferenței, și nu date de telemetrie brute sau de volum mare.

5.5. Concluzia capitolului

Acest capitol a demonstrat implementarea practică a detectării intruziunilor bazate pe ML în cadrul unei arhitecturi edge–cloud care respectă confidențialitatea, destinată sistemelor de monitorizare și control la distanță pentru IoT/IIoT. Pornind de la modelele offline dezvoltate în capitolul 4, lucrarea a validat detectarea în timp real la nodurile edge cu resurse limitate, valorificând în același timp cloud-ul pentru agregare, analiză și gestionarea incidentelor.

Arhitectura propusă permite detectarea cu latență redusă, minimizarea datelor și reducerea utilizării lățimii de bandă, menținând în același timp integrarea cu fluxurile de lucru de monitorizare și răspuns. Introducerea unui mecanism de comutare a modelelor în timpul rulării îmbunătățește și mai mult adaptabilitatea, permițând actualizări dinamice ale modelelor de detectare fără a întrerupe funcționarea sistemului.

Dincolo de performanță, capitolul subliniază importanța proiectării securității bazate pe arhitectură, arătând cum integrarea IDS în infrastructura sistemului îmbunătățește gestionabilitatea și reduce costurile pe termen lung ale cloud-ului. Cu toate acestea, limitările legate de modelele antrenate offline, constrângerile de resurse la marginea rețelei și domeniul de validare limitat indică necesitatea unei adaptabilități și scalabilități îmbunătățite, precum și a unei evaluări în condiții reale.

Astfel, acest capitol contribuie la îndeplinirea obiectivului O3, reducând decalajul dintre analiza offline a învățării automate și implementarea operațională, punând bazele pentru capitolul următor, care extinde cadrul către arhitecturi hibride, orientate spre reziliență.

Chapter 6. Arhitecturi hibride reziliente de tip „edge–fog” pentru detectarea intruziunilor bazată pe ML în sistemele de monitorizare și control la distanță IoT/IIoT

Acest capitol extinde cadrul anterior bazat pe perimetrul rețelei către o arhitectură hibridă Edge–Fog orientată spre reziliență. Studiul își propune (i) să cuantifice impactul atacurilor la nivelul stratului de rețea (inundarea cu pachete MQTT și injectarea de pachete malformate) asupra latenței și fiabilității sistemului și (ii) să evalueze dacă distribuirea inferenței IDS între straturile de perimetru și fog îmbunătățește reziliența. Prin implementarea unor modele de învățare automată identice în ambele straturi, arhitectura valorifică procesarea la marginea rețelei cu latență redusă și capacitatea de calcul mai mare la nivelul stratului “fog”, permițând detectarea redundantă și alertarea cooperativă, menținând în același timp performanța în timp real și îmbunătățind reziliența sistemului în condiții ostile [120].

6.1. Arhitectura sistemului și platforma experimentală

Această secțiune prezintă platforma de testare extinsă IoT/IIoT RMC utilizată pentru evaluarea arhitecturii hibride Edge–Fog IDS propuse. Bazându-se pe infrastructura din capitolul 5, sistemul este îmbunătățit pentru a suporta inferența distribuită și evaluarea rezilienței în condiții de atac cibernetic.

Așa cum se arată în Figura 6.1, arhitectura introduce o componentă IDS bazată pe fog care funcționează alături de nodul edge, formând o implementare hibridă. Nodul fog rulează un modul de inferență ML identic, oferind redundanță și capacitate de calcul suplimentară în timpul sarcinilor de lucru ridicate sau al întreruperilor. Atât instanțele edge, cât și cele fog împărtășesc același flux de extragere a caracteristicilor, aceiași pași de preprocesare și aceleași modele antrenate pentru a asigura coerența între experimente.

Pentru a asigura portabilitatea și reproductibilitatea, motorul de inferență bazat pe fog este implementat folosind containerizarea (Docker). Implementarea include scriptul de inferență, modelele antrenate în prealabil și fișierele de configurare, iar Dockerfile și Docker Compose gestionează dependențele, execuția, rețeaua și integrarea cu brokerul MQTT și sistemele de logare.

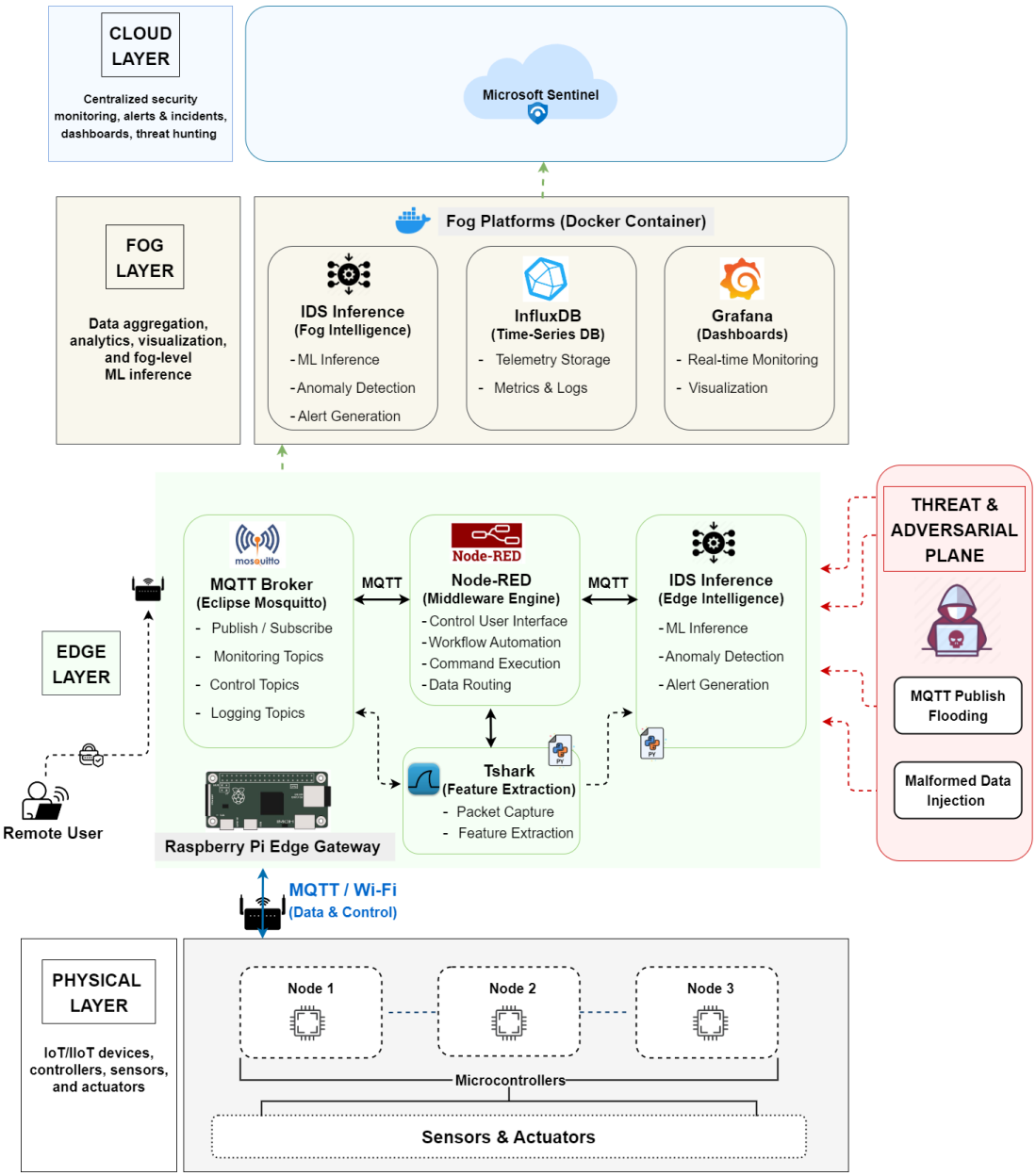


Figura 6.1. Arhitectură hibridă Edge–Fog bazată pe ML pentru sisteme de monitorizare și control la distanță IoT/IIoT.

6.2. Scenarii experimentale și metodologia de evaluare

Reziliența arhitecturii hibride Edge–Fog IDS a fost evaluată prin experimente controlate în cadrul a două scenarii de atac cibernetic: inundarea MQTT și injectarea de pachete malformate. Fiecare scenariu a fost testat în trei configurații de implementare, IDS bazat pe edge, bazat pe fog și hibrid, în cadrul unui flux de lucru în trei faze: linie de bază (funcționare normală), faza de atac și recuperarea post-atac. Au fost generate aproximativ 1.000 de comenzi de control automatizate pe fază pentru a asigura condiții de încărcare de lucru consistente.

Stratul de acționare a emulat procese ciber-fizice reprezentative folosind o încuietoare de ușă bazată pe releu (control discret) și un ventilator cu motor de curent continuu (control continuu), permițând evaluarea în cadrul diferitelor dinamici de control tipice sistemelor RMC IoT/IIoT.

Performanța a fost evaluată folosind indicatori-cheie, inclusiv latența de control mediană și la percentila 95, rata de succes a comenzilor și utilizarea procesorului (CPU) și a memoriei, oferind informații privind

capacitatea de răspuns, fiabilitatea și eficiența resurselor [121] . Indicatori suplimentari precum latența de inferență, latența end-to-end și debitul IDS (mesaje pe secundă), au fost utilizați pentru a evalua eficiența procesării de-a lungul fluxului de lucru de detectare. Toate datele au fost colectate și analizate folosind instrumente bazate pe Python în mediul Anaconda.

6.3. Rezultate și discuții

6.3.1 Latența de control și performanța în ceea ce privește fiabilitatea

Așa cum se ilustrează în Figura 6.2, în condiții normale de funcționare (linia de bază), sistemul a menținut latențe mediane de control cuprinse între 80 ms și 190 ms în toate modurile de implementare, confirmând adecvarea sa pentru funcționarea în timp real. Atunci când a fost supus atacurilor de tip „flooding" MQTT și de injectare a pachetelor malformate, latența a crescut moderat, gradul de degradare variind în funcție de stratul de implementare al IDS. În acest context, fiabilitatea operațională se reflectă în rata de succes a comenzilor, care măsoară proporția comenzilor de control transmise și executate cu succes de actuatoare, fără pierderi sau întârzieri excesive. Prin urmare, ratele ridicate de succes indică un comportament stabil și fiabil al sistemului atât în condiții normale, cât și în condiții adverse.

În timpul fazei de inundare MQTT, actuatorul încuietorii ușii a înregistrat o latență mediană de 194 ms (p95 = 253 ms) în cadrul IDS bazat pe edge și de 173 ms (p95 = 222 ms) în cadrul configurației bazate pe fog. În schimb, sistemul hibrid Edge–Fog IDS a atins cel mai bun echilibru, menținând o latență mediană de 172,5 ms (p95 = 233 ms) și o rată de succes a comenzilor de 98,6%, aproape identică cu performanța de referință. Un comportament similar a fost observat în cazul actuatorului ventilatorului de răcire, unde implementarea hibridă a atins din nou cea mai mică latență (84 ms) și cea mai mare fiabilitate (99,2%).

În cazul atacurilor prin injectarea de pachete malformate, sistemul hibrid de detectare a intruziunilor (IDS) a menținut o performanță apropiată de cea de referință, cu latențe mediane de 166,5 ms pentru actuatorul ușii și de 77 ms pentru ventilator, precum și rate de succes care depășesc 99,6%.

Deși abaterile observate ale latenței de control rămân moderate, atacurile evaluate au un impact mai pronunțat asupra latenței inferenței de detectare a intruziunilor și a stabilității debitului decât asupra latenței de control end-to-end, așa cum se demonstrează în secțiunea următoare.

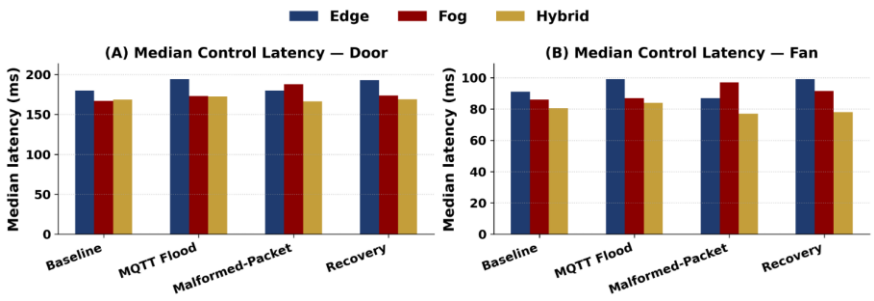


Figura 6.2. Latența mediană de control de la capăt la capăt în fazele de referință, de atac și de recuperare pentru (A) actuatorul încuietorii ușii și (B) actuatorul ventilatorului de răcire.

6.3.2 Analiza utilizării resurselor

Statisticile privind utilizarea resurselor indică faptul că suprasarcina de calcul a rămas modestă în toate configurațiile. Pentru IDS bazat pe edge, utilizarea medie a CPU a crescut ușor de la 5,4% la 6,2% în timpul inundării MQTT, cu valori de vârf care se apropie de 51%. Implementarea bazată pe fog a prezentat cel mai scăzut consum de resurse, cu o utilizare medie a CPU de 2% și o utilizare a memoriei de 37%. Configurația hibridă a înregistrat o utilizare medie a procesorului și a memoriei de 6,4%, respectiv 50%, rămânând cu mult în limitele acceptabile pentru sistemele încorporate și industriale. Utilizarea memoriei, care atinge valori maxime sub 65%, indică în plus faptul că arhitectura distribuită rămâne scalabilă și eficientă din punct de vedere al resurselor. Reducerea suprasolicitării de calcul îmbunătățește, de

asemenea, eficiența energetică, ceea ce este deosebit de avantajos pentru implementările IoT cu consum energetic limitat.

6.3.3 Latența inferenței și performanța de transfer

Implementarea bazată pe tehnologia „fog” a demonstrat o performanță superioară în ceea ce privește inferența, înregistrând o latență medie de inferență mai mică (5,06 ms față de 9,32 ms la marginea rețelei) și o latență end-to-end mai mică (12,96 ms față de 22,63 ms), cu întârzieri maxime reduse (a se vedea Figura 6.3). Aceste rezultate reflectă capacitatea de calcul mai mare a nodului fog, în timp ce marginea, cu resurse limitate, a prezentat o variabilitate mai mare în condiții de trafic intens.

Analiza debitului (vezi Figura 6.4) a arătat rate medii similare (~4,95 mesaje/s) pentru ambele implementări; cu toate acestea, rețeaua „fog” a oferit o performanță mai stabilă, în timp ce rețeaua de margine a înregistrat fluctuații și scăderi în condiții de concurență pentru resurse.

În ciuda acestor îmbunătățiri, evaluarea s-a limitat la două scenarii de atac și la o configurație cu un singur nod. Lucrările viitoare se vor extinde la tipuri suplimentare de atacuri, scalabilitate cu mai multe noduri și integrarea cu mecanisme de securitate de tip zero-trust” și adaptative.

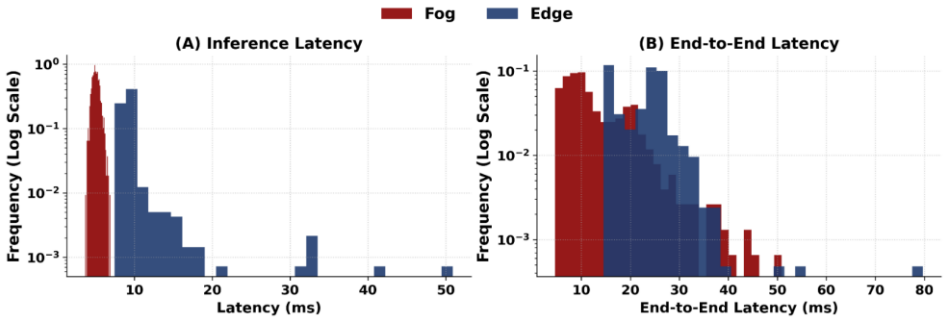


Figura 6.3. Distribuția latenței (A) și a latenței end-to-end (B) pentru sistemul de inferență implementat.

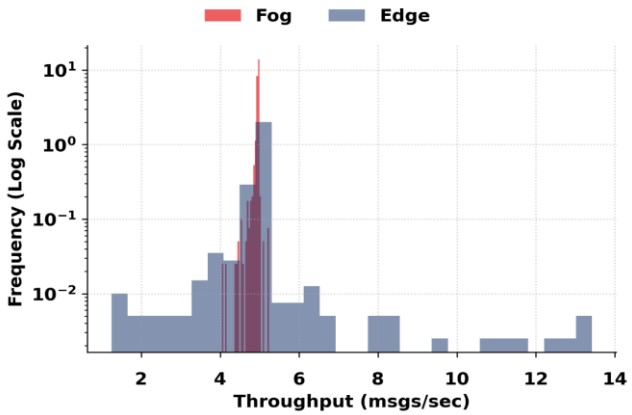


Figura 6.4. Distribuția debitului pentru sistemul de inferență implementat.

6.4. Concluzia capitolului

Acest capitol a evaluat reziliența sistemelor de monitorizare și control la distanță (RMC) bazate pe IoT/IIoT în condițiile unor atacuri cibernetice, concentrându-se asupra influenței plasării sistemului de inferență IDS bazat pe ML. Folosind platforma de testare prezentată în capitolul 5, studiul a evaluat impactul atacurilor de tip MQTT Flood și Malformed-Packet și a investigat eficacitatea unei implementări hibride Edge–Fog. Prin urmare, aceasta contribuie la realizarea și la finalizarea obiectivului O3.

Rezultatele experimentale au arătat că ambele atacuri au produs doar creșteri moderate ale latenței de control (4–20 ms), fără a perturba funcționarea sistemului. În timp ce performanța de control end-to-end

a rămas în mare parte stabilă, stratul IDS a suferit efecte mai vizibile, în special în ceea ce privește latența inferenței și stabilitatea debitului. Arhitectura hibridă Edge–Fog a atenuat aceste efecte prin distribuirea inferenței între nodurile de tip edge și fog, valorificând redundanța și stabilitatea superioară a procesării oferită de stratul fog. Lucrările viitoare se vor axa pe scalabilitate, învățarea adaptivă și integrarea modelului Zero Trust.

Chapter 7. Concluzii finale, contribuții originale, diseminarea rezultatelor și cercetări ulterioare

7.1. Concluzii

Această teză de doctorat abordează provocările de securitate cibernetică ale sistemelor de inginerie la distanță bazate pe IoT/IIoT, cu accent special pe controlul securizat al accesului, detectarea intruziunilor eficientă din punct de vedere al resurselor și arhitecturile de implementare orientate spre reziliență. Cercetarea a fost motivată de convergența crescândă a conectivității distribuite, a componentelor eterogene ale sistemului și a cerințelor operaționale în timp real, care, împreună, extind suprafața de atac, limitând în același timp aplicabilitatea abordărilor convenționale de securitate centrate pe IT.

Obiectivele tezei (O1–O3), așa cum sunt definite în capitolul 1, sunt abordate printr-o investigație progresivă care acoperă caracterizarea sistemului, controlul accesului centrat pe identitate, detectarea intruziunilor bazată pe învățarea automată și arhitecturile IDS adaptate implementării, în capitolele 2–6. Analiza inițială inter-domenii a stabilit că sistemele de inginerie la distanță prezintă o convergență structurală între mediile educaționale și industriale, determinată de integrarea IoT/IIoT și de conectivitatea la cloud, moștenind în același timp vulnerabilități din ambele domenii.

Plecând de la această bază, teza a demonstrat că controlul accesului centrat pe identitate, implementat prin principiile Zero Trust, atenuează în mod eficient riscurile asociate cu încrederea implicită și expunerea la privilegii excesive. Cu toate acestea, rezultatele au confirmat, de asemenea, că controlul accesului nu este suficient pentru a detecta amenințările comportamentale sau cele ulterioare compromiterii, fiind astfel necesare mecanisme complementare de detectare.

Din perspectiva detectării, teza a introdus o metodologie de învățare automată bazată pe selecția caracteristicilor pentru clasificarea traficului bazat pe MQTT. Rezultatele au arătat că detectarea intruziunilor poate fi adaptată la medii IoT/IIoT cu resurse limitate, fără o sarcină de calcul prohibitivă, permițând implementarea practică la marginea rețelei și pe platforme încorporate.

La nivel de sistem, această teză investighează strategii de implementare pentru detectarea intruziunilor, abordând compromisurile dintre eficacitatea detectării, latență, utilizarea resurselor și confidențialitatea datelor. A fost proiectată și validată experimental o arhitectură IDS modulară, care ține cont de confidențialitate, combinând inferența la nivel de margine, eficientă din punct de vedere al resurselor, cu monitorizarea centralizată bazată pe cloud. În plus, rezultatele experimentale indică faptul că distribuirea inferenței de-a lungul continuumului edge–fog–cloud îmbunătățește reziliența la atacurile cibernetice. În special, implementarea hibridă edge–fog a prezentat o degradare redusă a latenței, o fiabilitate constantă a acționării și o performanță a sistemului apropiată de valoarea de referință, menținând în același timp un consum minim de resurse.

Teza adoptă o perspectivă stratificată, la nivel de sistem, care aliniază proiectarea securității cu realitățile operaționale ale mediilor IoT/IIoT distribuite, în timp real. Rezultatele arată că îmbunătățirea securității sistemelor de inginerie la distanță necesită mecanisme complementare și coordonate, care combină controlul accesului centrat pe identitate, detectarea intruziunilor eficientă din punct de vedere al resurselor și strategii adaptate la modul de implementare la nivelurile de edge , fog și cloud.

7.2. Contribuții originale ale cercetării

Această teză prezintă un set de contribuții originale și complementare la securitatea cibernetică a sistemelor de inginerie la distanță bazate pe IoT/IIoT. Aceste contribuții promovează o perspectivă la nivel de sistem care acoperă controlul accesului, detectarea intruziunilor și proiectarea securității adaptată la implementare.

Principalele contribuții sunt rezumate după cum urmează.

1. **Contribuții conceptuale și arhitecturale**

Această teză oferă o caracterizare structurată și orientată spre securitate a sistemelor de inginerie la distanță din domeniile educațional și industrial, identificând vulnerabilitățile comune care decurg din

convergența IT/OT, conectivitatea distribuită și integrarea sistemelor vechi. De asemenea, ea pune în practică principiile Zero Trust prin proiectarea și validarea unei arhitecturi de control al accesului centrată pe identitate și la nivel de resurse, demonstrând eficacitatea acesteia în atenuarea mișcării laterale și a expunerii excesive a privilegiilor în medii la distanță.

2. **Contribuții metodologice în detectarea intruziunilor bazată pe învățarea automată**

Se propune și se validează o metodologie bazată pe selecția caracteristicilor pentru clasificarea traficului MQTT, permițând detectarea intruziunilor cu utilizare eficientă a resurselor, cu o dimensionalitate redusă a caracteristicilor. Abordarea menține o performanță ridicată de detectare, sprijinind în același timp implementarea pe dispozitive periferice cu resurse limitate, îmbunătățind aplicabilitatea sistemelor IDS bazate pe învățare automată în sistemele IoT/IIoT.

3. **Contribuții la nivel de sistem la arhitecturile IDS implementabile**

Teza proiectează și validează o arhitectură IDS Edge–Cloud modulară, care ține cont de confidențialitate, care integrează inferența la nivel de margine cu un sistem SIEM selectiv bazat pe cloud. Pe baza acestui lucru, este introdusă o implementare hibridă Edge–Fog, demonstrând o reziliență îmbunătățită în fața atacurilor cibernetice prin reducerea degradării latenței, menținerea unei fiabilități ridicate și păstrarea performanței sistemului cu un consum minim de resurse.

7.3. Diseminarea rezultatelor cercetării

Contribuțiile științifice prezentate în această teză au fost diseminate prin reviste cu factor de impact ridicat, lucrări ale conferințelor internaționale și un capitol dintr-o carte editată. Publicațiile enumerate mai jos includ atât lucrări care susțin direct contribuțiile de cercetare prezentate în teză, cât și studii complementare publicate în perioada doctoratului.

A. Publicații în reviste (evaluate ISI)

1. Tuyishime, E., Balan, T. C., Cotfas, P. A., Cotfas, D. T., & Rekeraho, A. (2023). **Enhancing cloud security—proactive threat monitoring and detection using a SIEM-based approach**. Applied Sciences, 13(22), 12359. https://doi.org/10.3390/app132212359 (*IF: 2,9, Q2, JCR 2025*).

2. Rekeraho, A., Cotfas, D. T., Cotfas, P. A., Bălan, T. C., **Tuyishime, E.**, & Acheampong, R. (2024). **Cybersecurity challenges in IoT-based smart renewable energy**. International Journal of Information Security, 23(1), 101-117. https://doi.org/10.1007/s10207-023-00732-9 (*IF: 5, Q1, JCR 2025*).

3. Rekeraho, A., Cotfas, D. T., Cotfas, P. A., **Tuyishime, E.**, Balan, T. C., & Acheampong, R. (2024). **Enhancing security for IoT-based smart renewable energy remote monitoring systems**. *Electronics*, *13*(4), 756. https://doi.org/10.3390/electronics13040756 (*IF: 2,9, Q2, JCR 2025*).

4. **Tuyishime, E.,** Martalò, M., Cotfas, P. A., Popescu, V., Cotfas, D. T., & Rekeraho, A. (2025)**. Resource-Efficient Traffic Classification Using Feature Selection for Message Queuing Telemetry Transport-Internet of Things Network-Based Security Attacks.** Applied Sciences, 15(8), 4252. Applied Sciences, 15(8), 4252. https://doi.org/10.3390/app15084252, (IF: 2,9, Q2, JCR 2025).

5. Rekeraho, A., Cotfas, D. T., Balan, T. C., Cotfas, P. A., Acheampong, R., & **Tuyishime, E.** (2025). **Cybersecurity Threat Modeling for IoT-Integrated Smart Solar Energy Systems: Strengthening Resilience for Global Energy Sustainability**. Sustainability, 17(6), 2386. https://doi.org/10.3390/su17062386, (*IF: 4,1, Q2, JCR 2025*).

6. Acheampong, R., Balan, T. C., Popovici, D. M., **Tuyishime, E.**, Rekeraho, A., & Voinea, G. D. (2025). **Balancing usability, user experience, security and privacy in XR systems: A multidimensional approach**. International Journal of Information Security, 24(3), 1-18.

   https://doi.org/10.1007/s10207-025-01025-z, (*IF: 5, Q1, JCR 2025).*

B. Lucrări prezentate la conferințe internaționale (evaluate de ISI și BDI)

7. Manzi, F., **Tuyishime, E.**, Hitayezu, A., Muhawenayo, G., Nsengiyumva, P., and Jayavel, K. (2023, November). **Leveraging Machine Learning and Raspberry Pi for Enhanced Wildlife Remote Monitoring and Localization**. In 2023 International Conference on Modeling & E-Information Research, Artificial Learning and Digital Applications (ICMERALDA) (pp. 301-306). IEEE

   https://doi.org/10.1109/ICMERALDA60125.2023.10458213

8. Hitayezu, A., Umutoni, R. M., **Tuyishime, E.**, Jayavel, K., & Kabiri, C. (2023, December**). Enhancing Road Safety with Cloud-Integrated IoT Road Signal Detection System**. In 2023 IEEE 16th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC) (pp. 117-122). IEEE. https://doi.org/10.1109/MCSoC60832.2023.00025, WOS:001190988000017

9. **Tuyishime, E.,** Radu, F., Cotfas, P., Cotfas, D., Balan, T., & Rekeraho, A. (2024, June). **Online laboratory access control with zero trust approach: Twingate use case**. In 2024, the 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-7). IEEE. https://doi.org/10.1109/ECAI61503.2024.10607562

10. Radu, F., Cotfas, P. A., **Tuyishime, E.**, Cotfas, D. T., Constantin, A., Alexandru, M., & Popescu, V. (2025, October). **Secure Testing and Simulation System Based on Raspberry Pi**. In 2025, IEEE 31st International Symposium for Design and Technology in Electronic Packaging (SIITME) (pp. 98-102). IEEE. https://doi.org/10.1109/SIITME67657.2025.11293695

11. **Tuyishime, E.**, Cotfas, P. A., Balan, T. C., Rekeraho, A., Cotfas, D. T., & Popescu, V. (2026). **ML-Based Intrusion Detection in IoT/IIoT with Privacy-Aware Offloading to Cloud SIEM**. In *Proceedings of the 12th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP*; ISBN 978-989-758-800-6; ISSN 2184-4356, SciTePress, pages 489-496.

    https://doi.org/10.5220/0014213600004061

12. **Tuyishime, E.,** Cotfas, P. A., Cotfas, D. T., Balan, T. C., & Popescu, V. (2026). **Hybrid Edge–Fog ML-Driven IDS for Resilient IoT/IIoT Remote Monitoring and Control.** In: Proceedings of the 23rd International Conference on Smart Technologies & Education (STE2026). **[Accepted for publication]**.

C. Capitole de carte (LNNS, Springer)

13. Radu, F., **Tuyishime, E.**, Cotfas, P., Cotfas, D., Balan, T., Rekeraho, A. (2024). **Online Serial Laboratories**. In: May, D., Auer, M.E., Kist, A. (eds) Online Laboratories in Engineering and Technology Education. Lecture Notes in Networks and Systems, vol 1135. Springer, Cham.

    https://doi.org/10.1007/978-3-031-70771-1_19

7.4. Direcții pentru cercetări viitoare

Deși această teză a adus mai multe contribuții la abordarea provocărilor legate de securitatea cibernetică în sistemele inginerești la distanță, rămân câteva limitări și direcții de cercetare deschise care trebuie abordate în lucrările viitoare, inclusiv:

1. Mecanisme de învățare adaptivă pentru IDS bazate pe ML: Sistemul actual se bazează pe modele antrenate offline. Extinderea cercetării către abordări de învățare adaptivă și federată ar permite modelelor IDS să se adapteze dinamic la schimbările de date și la modelele de atac în continuă evoluție din mediile IoT/IIoT.
2. Analiza scalabilității în implementările multinod de tip edge–fog: Mediile industriale la scară largă implică de obicei mai multe clustere și gateway-uri distribuite. Lucrările viitoare ar trebui să evalueze performanța, precizia detectării și consumul de resurse în scenarii cu mai multe clustere și cu un grad ridicat de concurență.
3. Arhitectură de securitate ciber-fizică cu auto-reparare: Dincolo de detectare, sistemele viitoare ar trebui să integreze mecanisme automatizate de răspuns, izolare și recuperare, permițând infrastructuri RMC autoadaptabile bazate pe IoT/IIoT.

4. Extinderea WebSocket peste QUIC [122] și MQTT (WSQM) la sistemele de inginerie la distanță: Cercetările viitoare ar putea explora extinderea abordării WSQM [123] la mediile de inginerie la distanță, cu accent special pe transportul criptat cu latență redusă, persistența sesiunii și integrarea cu controale de securitate bazate pe politici.

Referințe

[1] R. Heradio, L. de la Torre, and S. Dormido, “Virtual and remote labs in control education: A survey,” *Annu. Rev. Control*, vol. 42, pp. 1–10, Jan. 2016.

[2] J. Miranda, C. Navarrete, J. Noguez, J.-M. Molina-Espinosa, M.-S. Ramírez-Montoya, S. A. Navarro-Tuch, M.-R. Bustamante-Bello, J.-B. Rosas-Fernández, and A. Molina, “The core components of education 4.0 in higher education: Three case studies in engineering education,” *Comput. Electr. Eng.*, vol. 93, p. 107278, July 2021.

[3] J.-Q. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, “Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges,” vol. 19, no. 3, pp. 1504–1526, 2017.

[4] P. Helo, Y. Hao, R. Toshev, and V. Boldosova, “Cloud manufacturing ecosystem analysis and design,” *Robot. Comput.-Integr. Manuf.*, vol. 67, p. 102050, Feb. 2021.

[5] F. J. Folgado, D. Calderón, I. González, and A. J. Calderón, “Review of Industry 4.0 from the Perspective of Automation and Supervision Systems: Definitions, Architectures and Recent Trends,” *Electronics*, vol. 13, no. 4, p. 782, Jan. 2024.

[6] D. Miller, “Remote Access Grows Even as Cybersecurity Fears Surge,” *Automation World*, 16-Sept-2021. [Online]. Available: https://www.automationworld.com/cybersecurity/article/21722664/remote-access-grows-even-as-cybersecurity-fears-surge. [Accessed: 14-Feb-2026].

[7] A. V. den Beemt, S. Groothuijsen, L. Ozkan, and W. Hendrix, “Remote labs in higher engineering education: engaging students with active learning pedagogy,” vol. 35, no. 2, pp. 320–340, Aug. 2023.

[8] T. Chamunorwa, H. A. Modran, D. Ursuțiu, C. Samoilă, and H. Hedeșiu, “Cloud-Based, Expandable—Reconfigurable Remote Laboratory for Electronic Engineering Experiments,” *Electronics*, vol. 11, no. 20, p. 3292, Jan. 2022.

[9] J. Amankwah-Amoah, Z. Khan, G. Wood, and G. Knight, “COVID-19 and digitalization: The great acceleration,” *J. Bus. Res.*, vol. 136, pp. 602–611, Nov. 2021.

[10] B. Galloway and G. P. Hancke, “Introduction to Industrial Control Networks,” *IEEE Commun. Surv. Tutor.*, vol. 15, no. 2, pp. 860–880, 2013.

[11] J. Cecílio and P. Furtado, “Industrial Control Systems: Concepts, Components, and Architectures,” in *Wireless Sensors in Industrial Time-Critical Environments*, J. Cecílio and P. Furtado, Eds. Cham: Springer International Publishing, 2014, pp. 7–18.

[12] S. Vitla, “Unsecured Remote Desktop Protocol (RDP) Access: A Gateway for Ransomware Attacks and Corporate Extortion,” *J. Comput. Sci. Technol. Stud.*, vol. 6, no. 2, pp. 150–165, May 2024.

[13] E. Byres, D. Leversage, and N. Kube, “Security incidents and trends in SCADA and process industries,” *Ind. Ethernet Book*, vol. 39, no. 2, pp. 12–20, 2007.

[14] Y. Chen, H. Hu, and G. Cheng, “Design and implementation of a novel enterprise network defense system bymaneuveringmulti-dimensional network properties,” *Front. Inf. Technol. Electron. Eng.*, vol. 20, no. 2, pp. 238–252, Feb. 2019.

[15] J. Kindervag, B. Stephanie, M. Kelley, and B. Josh, “No More Chewy Centers: The Zero Trust Model Of Information Security,” Forrester Research, Inc., Cambridge, MA 02139 USA, Mar. 2016.

[16] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things,” *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021.

[17] J. Arshad, M. A. Azad, R. Amad, K. Salah, M. Alazab, and R. Iqbal, “A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT,” *Electronics*, vol. 9, no. 4, p. 629, Apr. 2020.

[18] L. Gomes and S. Bogosyan, “Current Trends in Remote Laboratories,” *IEEE Trans. Ind. Electron.*, vol. 56, no. 12, pp. 4744–4756, Dec. 2009.

[19] B. Aktan, C. A. Bohus, L. A. Crowl, and M. H. Shor, “Distance learning applied to control engineering laboratories,” *IEEE Trans. Educ.*, vol. 39, no. 3, pp. 320–326, Aug. 1996.

[20] S. Frerich, D. Kruse, M. Petermann, and A. Kilzer, “Virtual Labs and Remote Labs: Practical experience for everyone,” in *2014 IEEE Global Engineering Education Conference (EDUCON)*, 2014, pp. 312–314.

[21] H. Tjahyadi, K. Prasetya, and I. M. Murwantara, “Digital Twin Based Laboratory for Control Engineering Education,” *Int. J. Inf. Educ. Technol.*, vol. 13, no. 4, pp. 704–711, 2023.
[22] J. Ma and J. V. Nickerson, “Hands-on, simulated, and remote laboratories: A comparative literature review,” *ACM Comput. Surv.*, vol. 38, no. 3, pp. 7-es, Sept. 2006.
[23] J. Grodotzki, T. R. Ortelt, and A. E. Tekkaya, “Remote and Virtual Labs for Engineering Education 4.0: Achievements of the ELLI project at the TU Dortmund University,” *Procedia Manuf.*, vol. 26, pp. 1349–1360, Jan. 2018.
[24] A. Van den Beemt, S. Groothuijsen, L. Ozkan, and W. Hendrix, “Remote labs in higher engineering education: engaging students with active learning pedagogy,” *J. Comput. High. Educ.*, vol. 35, no. 2, pp. 320–340, Aug. 2023.
[25] T. Chamunorwa, H. A. Modran, D. Ursuțiu, C. Samoilă, and H. Hedeșiu, “Cloud-Based, Expandable—Reconfigurable Remote Laboratory for Electronic Engineering Experiments,” *Electronics*, vol. 11, no. 20, p. 3292, Jan. 2022.
[26] A. E. Pena-Molina and M. M. Larrondo-Petrie, “Safety and Security Considerations for Online Laboratory Management Systems,” *J. Cybersecurity Priv.*, vol. 5, no. 2, p. 24, June 2025.
[27] J. Machotka, Z. Nedic, and Ö. Göl, “Collaborative Learning in the Remote Laboratory NetLab,” *J. Syst. Cybern. Inform.*, vol. 6, June 2008.
[28] C. Lazar and S. Carari, “A remote-control engineering laboratory,” *IEEE Trans. Ind. Electron.*, vol. 55, no. 6, pp. 2368–2375, 2008.
[29] P. A. Cotfas, D. T. Cotfas, D. Ursutiu, and C. Samoila, “Remote Laboratory in Photovoltaics,” *Int. J. Online Eng.*, vol. 5, no. 3, 2009.
[30] D. Pop, D. G. Zutin, M. E. Auer, K. Henke, and H. D. Wuttke, “An online lab to support a master program in remote engineering,” in *2011 Frontiers in Education Conference (FIE*, 2011, pp. 2–1.
[31] C. A. Jara, F. A. Candelas, S. T.Puente, and F. Torres, “Hands-on experiences of undergraduate students in Automatics and Robotics using a virtual and remote laboratory”,” *Comput. Educ.*, vol. 57, pp. 2451–2461, 2011.
[32] A. Rojko, D. Hercog, and K. Jezernik, “Power Engineering and Motion Control Web Laboratory: Design, Implementation, and Evaluation of Mechatronics Course,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 10, pp. 3343-3354, Oct. 2010.
[33] M. A. Vivar and A. R. Magna, “Design, implementation and use of a remote network lab as an aid to support teaching computer network,” in *2008 Third International Conference on Digital Information Management*, 2008, pp. 905–909.
[34] M. Tawfik, D. Lowe, S. Murray, M. De La Villefromoy, M. Diponio, E. Sancristobal, M. J. Albert, G. Diaz, and M. Castro, “Grid Remote Laboratory Management System,” in *2013 10th International Conference on Remote Engineering and Virtual Instrumentation (REV)*, 2013, pp. 1–9.
[35] M. Kalúz, P. Orduña, J. García-Zubia, M. Fikar, and L. Ĉirka, “Sharing Control Laboratories by Remote Laboratory Management System WebLab-Deusto,” *IFAC Proc. Vol.*, vol. 46, no. 17, pp. 345–350, Jan. 2013.
[36] E. Werner, J. C. Matias, M. D. Berejuck, and H. Saliah-Hassane, “Main Attacks and Ways to Keep Security Guidelines Updated in Remote Laboratories,” in *Online Engineering and Society 4.0*, vol. 298, M. E. Auer, K. R. Bhimavaram, and X.-G. Yue, Eds. Cham: Springer International Publishing, 2022, pp. 115–121.
[37] Y. Larbaoui, A. Naddami, and A. Fahli, “Security, Control and Management of Smart Remote Laboratory for Remote Experiments in Electricity and Electronics,” *Int. J.*, vol. 9, no. 3, 2020.
[38] E. Lisova, I. Šljivo, and A. Čaušević, “Safety and security co-analyses: a systematic literature review,” *IEEE Syst J*, vol. 13, no. 3, pp. 2189–2200, 2018.
[39] Joint Task Force Transformation Initiative, “Guide for conducting risk assessments,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012.
[40] R. K. Alqurashi, M. A. AlZain, B. Soh, M. Masud, and J. Al-Amri, “Cyber Attacks and Impacts: A Case Study in Saudi Arabia,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1, pp. 217-224, 2020.
[41] S. Christey and R. A. Martin, “CWE - Vulnerability Type Distributions in CVE,” in *Cwe.mitre.org*, p. .
[42] M. Bach-Nutman, “Understanding The Top 10 OWASP Vulnerabilities.” arXiv, 17-Dec-2020.

[43] M. A. Al-Shareeda, S. Manickam, and S. A. Sari, “A Survey of SQL Injection Attacks, Their Methods, and Prevention Techniques,” in *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)*, 2022, pp. 31–35.
[44] “Top 6 Industries Targeted By Threat Actors In 2024 | Cyble,” 03-Dec-2024. .
[45] D. Uckelmann, D. Mezzogori, G. Esposito, M. Neroni, D. Reverberi, and M. Ustenko, “Safety and Security in Federated Remote Labs–A Requirement Analysis,” in *Cross Reality and Data Science in Engineering: Proceedings of the 17th International Conference on Remote Engineering and Virtual Instrumentation 17*, 2021, pp. 21–36.
[46] E. Werner, J. C. Matias, M. D. Berejuck, and H. Saliah-Hassane, “Evaluation of blockchain techniques to ensure secure access on remote FPGA laboratories,” in *2021 9th International Symposium on Digital Forensics and Security (ISDFS*, 2021, pp. 1–6.
[47] M. Krbeček, F. Schauer, and R. Jasek, “Security aspects of remote e-laboratories,” *Int J Online Eng*, vol. 9, no. 3, pp. 34–39, 2013.
[48] Th. Richter, R. Watson, S. Kassavetis, M. Kraft, P. Grube, D. Boehringer, P. de Vries, E. Hatzikraniotis, and S. Logothetidis, “The WebLabs of the University of Cambridge: A study of securing remote instrumentation,” in *2012 9th International Conference on Remote Engineering and Virtual Instrumentation (REV)*, 2012, pp. 1–5.
[49] J. A. Sanchez-Viloria, L. F. Zapata-Rivera, C. Aranzazu-Suescun, A. E. Molina-Pena, and M. M. Larrondo-Petrie, “Online Laboratory Communication Using MQTT IoT Standard,” in *2021 World Engineering Education Forum/Global Engineering Deans Council (WEEF/GEDC)*, 2021, pp. 550–555.
[50] D. Dumo, “Cyber security concerns of Supervisory Control and Data Acquisition (SCADA) systems,” in *2010 IEEE International Conference on Technologies for Homeland Security (HST)*, 2010, pp. 473–475.
[51] A. Aijaz and M. Sooriyabandara, “The Tactile Internet for Industries: A Review,” *Proc. IEEE*, vol. 107, no. 2, pp. 414–435, Feb. 2019.
[52] K. J. A˚ström and P. R. Kumar, “Control: A perspective,” *Automatica*, vol. 50, no. 1, pp. 3–43, Jan. 2014.
[53] U. P. D. Ani, H. (Mary) He, and A. Tiwari, “Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective,” *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, Jan. 2017.
[54] “Critical Infrastructure Sectors | CISA.” [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors. [Accessed: 29-Dec-2025].
[55] “The Ultimate Guide to Physical Security.” [Online]. Available: https://buildings.honeywell.com/us/en/brands/our-brands/lenels2/news/insights/the-ultimate-guide-to-physical-security. [Accessed: 29-Dec-2025].
[56] M. P. Coole and D. J. Brooks, “Physical Security: Best Practices,” in *Encyclopedia of Security and Emergency Management*, L. R. Shapiro and M.-H. Maras, Eds. Cham: Springer International Publishing, 2021, pp. 730–737.
[57] M. Rapaccini, N. Saccani, C. Kowalkowski, M. Paiola, and F. Adrodegari, “Navigating disruptive crises through service-led growth: The impact of COVID-19 on Italian manufacturing firms,” *Ind. Mark. Manag.*, vol. 88, pp. 225–237, July 2020.
[58] A. Margherita and M. Heikkilä, “Business continuity in the COVID-19 emergency: A framework of actions undertaken by world-leading companies,” *Bus. Horiz.*, vol. 64, no. 5, pp. 683–695, Sept. 2021.
[59] “REMOTE CONTROL, the ultimate convenience technology to address COVID-19 pandemic concerns and demographic workforce pressures,” *Condition Monitoring*. July-2020.
[60] T. Johan, D. Kristofer, M. György, S. Björn, M. Gunnar, M. Tomas, S. John, N. Jan, N. Jonas, M. Carlos, Z. Biao, and W. Jianjun, “Industrial remote operation: 5G rises to the challenge - Ericsson Technology Review,” Nov. 2015.
[61] G. M. Achilli, F. Chinello, C. Fang, P. G. Hernandez, S. Logozzo, and M. C. Valigi, “Preliminary Study on a Handle with Haptic Devices for Collaborative Robotics in a Remote Maintenance Environment,” in *Proceedings of I4SDG Workshop 2023: IFToMM for Sustainable Development Goals*, 2023, pp. 484–491.

[62] L. Seiffert, J. Sczodrok, J. Ghofrani, and K. Wieczorek, *Remote Technol. Common Pract. Ind. Maint. What Experts Say Telecom*, vol. 3, no. 4, pp. 548–563, Sept. 2022.
[63] D. Mourtzis, V. Siatras, and J. Angelopoulos, "Real-time remote maintenance support based on augmented reality (AR," *Appl. Sci.*, vol. 10, no. 5, 2020.
[64] "Configuring and Managing Remote Access for Industrial Control Systems," Centre for the Protection of National Infrastructure, 2010.
[65] M. R. Asghar, Q. Hu, and S. Zeadally, "Cybersecurity in industrial control systems: Issues, technologies, and challenges," *Comput. Netw.*, vol. 165, p. 106946, Dec. 2019.
[66] C. Alcaraz, G. Fernandez, and F. Carvajal, "Security Aspects of SCADA and DCS Environments," in *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*, J. Lopez, R. Setola, and S. D. Wolthusen, Eds. Berlin, Heidelberg: Springer, 2012, pp. 120–149.
[67] T. Menze, "The state of industrial cybersecurity in the era of digitalization," *Online Httpsics Kaspersky Commed. ARC ICS-2020-Trend-Rep. Pdf*, 2020.
[68] M. Marali, S. D. Sudarsan, and A. Gogioneni, "Cyber security threats in industrial control systems and protection," in *2019 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2019, pp. 1–7.
[69] M. Conti, D. Donadel, and F. Turrin, "A Survey on Industrial Control System Testbeds and Datasets for Security Research," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, pp. 2248–2294, 2021.
[70] J. P. Farwell and R. Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, vol. 53, no. 1, pp. 23–40, Feb. 2011.
[71] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, "Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 35, p. 100464, Dec. 2021.
[72] T. Alladi, V. Chamola, and S. Zeadally, "Industrial Control Systems: Cyberattack trends and countermeasures," *Comput. Commun.*, vol. 155, pp. 1–8, Apr. 2020.
[73] K. Pawel and K. Nikita, "The Russia-Ukraine Cyber War Part 3: Attacks on Telecom and Critical Infrastructure," *LevelBlue*, 05-Mar-2025. .
[74] S. Gatlan, "Ransomware attack forces 100 Romanian hospitals to go offline," *BleepingComputer*, 12-Feb-2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/ransomware-attack-forces-100-romanian-hospitals-to-go-offline/. [Accessed: 15-Mar-2026].
[75] R. Sangkhro and A. K. Agrawal, "Cybersecurity in Industrial Control Systems: A Review of the Current Trends and Challenges," in *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2023, pp. 355–359.
[76] D. Wu, A. Ren, W. Zhang, F. Fan, P. Liu, X. Fu, and J. Terpenny, "Cybersecurity for digital manufacturing," *J. Manuf. Syst.*, vol. 48, pp. 3–12, July 2018.
[77] A. Shahzad, M. Lee, H. D. Kim, S. Woo, and N. Xiong, "New Security Development and Trends to Secure the SCADA Sensors Automated Transmission during Critical Sessions," *Symmetry*, vol. 7, no. 4, pp. 1945–1980, Dec. 2015.
[78] S. Ndichu, S. McOyowo, H. Okoyo, and C. Wekesa, "A Remote Access Security Model based on Vulnerability Management," *Int. J. Inf. Technol. Comput. Sci.*, vol. 12, no. 5, pp. 38–51, Oct. 2020.
[79] C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," *Ad Hoc Netw.*, vol. 156, p. 103414, Apr. 2024.
[80] "2024 VPN Risk Report [HPE]," *Cybersecurity Insiders*. .
[81] S. W. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST*, Aug. 2020.
[82] H. Holm, M. Karresand, A. Vidström, and E. Westring, "A Survey of Industrial Control System Testbeds," in *Secure IT Systems*, 2015, pp. 11–26.
[83] C. Ekisa, D. Ó. Briain, and Y. Kavanagh, "VICSORT - A Virtualised ICS Open-source Research Testbed," in *2022 Cyber Research Conference - Ireland (Cyber-RCI)*, 2022, pp. 1–8.
[84] F. Björck, M. Henkel, J. Stirna, and J. Zdravkovic, "Cyber Resilience – Fundamentals for a Definition," in *New Contributions in Information Systems and Technologies*, 2015, pp. 311–316.
[85] D. Galinec and W. Steingartner, "Combining cybersecurity and cyber defense to achieve cyber resilience," in *2017 IEEE 14th International Scientific Conference on Informatics*, 2017, pp. 87–93.

[86] T. N. I. Alrumaih, M. J. F. Alenazi, N. A. AlSowaygh, A. A. Humayed, and I. A. Alablani, “Cyber resilience in industrial networks: A state of the art, challenges, and future directions,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 9, p. 101781, Oct. 2023.
[87] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines,” *Comput. Netw.*, vol. 54, no. 8, pp. 1245–1265, June 2010.
[88] K. Stouffer, “Guide to Operational Technology (OT) Security,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-82r3, 2023.
[89] “ISA/IEC 62443 Series of Standards - ISA,” *isa.org*. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed: 04-Jan-2026].
[90] “ISO - ISO/IEC 27000 family — Information security management,” *ISO*. [Online]. Available: https://www.iso.org/standard/iso-iec-27000-family. [Accessed: 04-Jan-2026].
[91] *VDI/VDE 2182 Blatt 1 - IT-security for industrial automation - General model*. 2020.
[92] D. Bodeau and R. Graubart, “Cyber Resiliency Design Principles Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines,” MITRE CORP, Technical Report MTR170001, Jan. 2017.
[93] D. Liveri, A. Sarri, and E. Darra, “ENISA’s Contribution to National Cyber Security Strategies,” in *Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden*, M. Bartsch and S. Frey, Eds. Wiesbaden: Springer Fachmedien, 2018, pp. 43–64.
[94] I.-A. Dumitru, “Zero Trust Security,” in *Proceedings of the International Conference on Cybersecurity and Cybercrime - 2022*, vol. IX, Romania: Asociatia Romana pentru Asigurarea Securitatii Informatiei, 2022, pp. 99–104.
[95] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, “Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust,” *Comput. Secur.*, vol. 110, p. 102436, Nov. 2021.
[96] J. Kindervag, B. Stephanie, and C. Lindsey, “No More Chewy Centers: Introducing The Zero Trust Model Of Information Security,” Forrester Research, Inc., Cambridge, MA 02139 USA, Sept. 2010.
[97] J. Kindervag, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture,” 2010.
[98] F. Radu, E. Tuyishime, P. Cotfas, D. Cotfas, T. Balan, and A. Rekeraho, “Online Serial Laboratories,” in *Online Laboratories in Engineering and Technology Education: State of the Art and Trends for the Future*, D. May, M. E. Auer, and A. Kist, Eds. Cham: Springer, Cham, 2024, pp. 375–390.
[99] “Twingate: It’s time to ditch your VPN.” [Online]. Available: https://www.twingate.com/. [Accessed: 14-Jan-2026].
[100] “MQTTset,” *CNR IEIIT*, 2021. [Online]. Available: https://www.kaggle.com/datasets/cnrieiit/mqttset. [Accessed: 16-Jan-2026].
[101] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, and E. Cambiaso, “MQTTset, a New Dataset for Machine Learning Techniques on MQTT,” *Sensors*, vol. 20, no. 22, p. 6578, Jan. 2020.
[102] G. Chandrashekar and F. Sahin, “A survey on feature selection methods,” *Comput. Electr. Eng.*, vol. 40, no. 1, pp. 16–28, Jan. 2014.
[103] S. García, S. Ramírez-Gallego, J. Luengo, J. M. Benítez, and F. Herrera, “Big data preprocessing: methods and prospects,” *Big Data Anal.*, vol. 1, no. 1, p. 9, Nov. 2016.
[104] R.-C. Chen, C. Dewi, S.-W. Huang, and R. E. Caraka, “Selecting critical features for data classification based on machine learning methods,” *J. Big Data*, vol. 7, no. 1, p. 52, July 2020.
[105] T. J. Ulrych, D. R. Velis, A. D. Woodbury, and M. D. Sacchi, “L-moments and C-moments,” *Stoch. Environ. Res. Risk Assess.*, vol. 14, no. 1, pp. 50–68, Mar. 2000.
[106] T. Li, “Robust estimations from distribution structures: II. Central Moments.” arXiv, June-2024.
[107] V. N. G. Raju, K. P. Lakshmi, V. M. Jain, A. Kalidindi, and V. Padma, “Study the Influence of Normalization/Transformation process on the Accuracy of Supervised Classification,” in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2020, pp. 729–735.
[108] D. Singh and B. Singh, “Investigating the impact of data normalization on classification performance,” *Appl. Soft Comput.*, vol. 97, p. 105524, Dec. 2020.
[109] S. Raschka, “Model Evaluation, Model Selection, and Algorithm Selection in Machine Learning.” arXiv, Nov-2020.

[110] T. O'Malley, E. Bursztein, J. Long, F. Chollet, H. Jin, and L. Invernizzi, "KerasTuner," 2019. [Online]. Available: https://github.com/keras-team/keras-tuner. [Accessed: 21-Jan-2026].
[111] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: a simple way to prevent neural networks from overfitting," *J Mach Learn Res*, vol. 15, no. 1, pp. 1929–1958, Jan. 2014.
[112] D. P. Kingma and J. Lei Ba, "Adam: A Method for Stochastic Optimization," in *3rd International Conference on Learning Representations (ICLR)*, 2015, vol. 5.
[113] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 (General Data Protection Regulation," Regulation L 119, Apr. 2016.
[114] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards and Technology." Special Publication 500-292; NIST: Gaithersburg, MD, USA, 2011.
[115] J. Bian, A. A. Arafat, H. Xiong, J. Li, L. Li, H. Chen, J. Wang, D. Dou, and Z. Guo, "Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8364–8386, June 2022.
[116] D. Panchal, P. Verma, I. Baran, D. Musgrove, and D. Lu, "Reusable MLOps: Reusable Deployment, Reusable Infrastructure and Hot-Swappable Machine Learning models and services." arXiv, 19-Feb-2024.
[117] A. Marda, S. Kulkarni, and K. Vaidhyanathan, "SWITCH: An Exemplar for Evaluating Self-Adaptive ML-Enabled Systems," in *Proceedings of the 19th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, 2024, pp. 143–149.
[118] G. Andresini, F. Pendlebury, F. Pierazzi, C. Loglisci, A. Appice, and L. Cavallaro, "INSOMNIA: Towards Concept-Drift Robustness in Network Intrusion Detection," in *Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security*, 2021, pp. 111–122.
[119] "Pricing Calculator | Microsoft Azure." [Online]. Available: https://azure.microsoft.com/en-us/pricing/calculator/. [Accessed: 30-Jan-2026].
[120] O. F. Olaitan, O. N. Akatakpo, C. O. Victor, C. J. Emejulu, T. M. Ayoola, D. E. Olayiwola, and A. A. Ajibola, "Secure and Resilient Industrial IoT Architectures for Smart Manufacturing: A Comprehensive Review," *J. Eng. Res. Rep.*, vol. 27, no. 6, pp. 331–344, June 2025.
[121] "On the Latency, Rate, and Reliability Tradeoff in Wireless Networked Control Systems for IIoT | IEEE Journals & Magazine | IEEE Xplore." [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9134368. [Accessed: 17-Mar-2026].
[122] J. Iyengar and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport," Internet Engineering Task Force, Request for Comments RFC 9000, May 2021.
[123] G. Pettorru and M. Martalò, "A Persistent and Secure Publish-Subscriber Architecture for Low-Latency IoT Communications," *IEEE Trans. Netw. Serv. Manag.*, vol. 23, pp. 729–739, 2026.