ȘCOALĂ DOCTORALĂ INTERDISCIPLINARĂ

Facultatea de Inginerie Electrică și Știința Calculatoarelor

Alexandre REKERAHO

Provocări de securitate cibernetică pentru rețelele inteligente de energie regenerabilă bazate pe IoT

REZUMAT

Supervizor științific

Prof. Dr. Daniel Tudor COTFAS

BRAȘOV, 2025

Rezumat

Integrarea rețelelor inteligente de energie regenerabilă bazate pe IoT, în special a sistemelor solare fotovoltaice (PV), a revoluționat monitorizarea de la distanță, automatizarea și eficiența operațională. Cu toate acestea, această transformare digitală introduce vulnerabilități de securitate cibernetică, expunând dispozitivele IoT, canalele de transmisie a datelor și platformele bazate pe cloud la diverse amenințări cibernetice. Această cercetare abordează aceste provocări prin dezvoltarea unui cadru cuprinzător, sigur și proactiv de securitate cibernetică adaptat rețelelor inteligente de energie solară bazate pe IoT.

În primul rând, acest studiu realizează o revizuire sistematică și o analiză critică a provocărilor de securitate în rețelele de energie regenerabilă bazate pe IoT. Acesta clasifică amenințările cibernetice, vulnerabilitățile, vectorii de atac și motivațiile adversarilor, oferind o înțelegere structurată a riscurilor de securitate în sistemele fotovoltaice solare bazate pe IoT. Cercetarea utilizează analiza Cyber Kill Chain pentru a evalua potențialele scenarii de atac. Ea evaluează în mod critic mecanismele de securitate existente, inclusiv protocoalele de criptare, schemele de autentificare, sistemele de detectare a intruziunilor, blockchain și apărarea bazată pe învățarea automată. Analiza identifică lacune în abordările actuale, în special lipsa unei strategii de securitate unificate, ceea ce subliniază necesitatea unui cadru integrat de securitate cibernetică.

În al doilea rând, cercetarea dezvoltă un caz de utilizare a unui sistem inteligent de energie solară bazat pe IoT care să servească drept platformă experimentală pentru analiza securității cibernetice și modelarea amenințărilor. Arhitectura include module fotovoltaice, senzori IoT, controlere industriale, straturi de transmisie a datelor, analize bazate pe cloud și interfețe de monitorizare la distanță. Folosind acest caz de utilizare, studiul realizează modelarea structurată a amenințărilor și evaluarea riscurilor prin aplicarea metodologiilor STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) și DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability). Acest cadru clasifică sistematic și prioritizează amenințările cibernetice care afectează diverse componente ale sistemului solar inteligent bazat pe IoT, cuantificând gravitatea acestor amenințări. În plus față de analiza securității la nivel de sistem, vulnerabilitățile de securitate la nivel de dispozitiv au fost examinate prin efectuarea unei evaluări a vulnerabilității firmware a dispozitivelor IoT încorporate în sistemele de energie solară. Evaluarea controlerului logic programabil (PLC) identifică firmware neacoperit, implementări criptografice slabe, mecanisme de actualizare nesigure și vulnerabilități și expuneri comune (CVE) cunoscute public.

În al treilea rând, cercetarea proiectează și implementează o arhitectură sigură de monitorizare bazată pe IoT pentru a spori protecția datelor și comunicarea sigură. Soluția propusă protejează integritatea și confidențialitatea fluxurilor de date Internet of Things (IoT) prin încorporarea Transport Layer Security (TLS 1.2) pentru conectivitatea cloud și Advanced Encryption Standard (AES) pentru securitatea comunicațiilor locale. De asemenea, a fost dezvoltat un sistem de monitorizare la distanță în timp real care utilizează SystemLink Cloud, oferind capacități de monitorizare la distanță pentru rețelele solare inteligente bazate pe IoT.

În al patrulea rând, studiul introduce un sistem de securitate integrat în cloud pentru a îmbunătăți autentificarea și autorizarea, precum și procesarea securizată a datelor, în sistemele de energie regenerabilă bazate pe IoT. Sistemul utilizează Stream Analytics, Microsoft Azure IoT Hub, Power BI și Time Series Insights pentru procesarea sigură și în timp real a datelor. Sunt utilizate mecanisme îmbunătățite de autentificare a dispozitivelor, inclusiv politici de acces partajat (SAP) și autorizare pe bază de tokenuri SAS (Shared Access Signature), pentru a preveni accesul nedorit. Politicile RBAC (Role-based Access Control) sunt integrate pentru a aplica gestionarea granulară a permisiunilor în comunicațiile IoT-cloud.

În cele din urmă, cercetarea dezvoltă un cadru unificat de monitorizare a securității cibernetice și de răspuns la incidente pentru a asigura corelarea proactivă a evenimentelor de securitate, detectarea anomaliilor în timp real și descoperirea automată a activelor. Cadrul integrează securitatea Information și Event Management (SIEM) cu monitorizarea securității IoT/OT, permițând o vizibilitate multidomeniu a securității. Sunt încorporate tehnici avansate de corelare a evenimentelor pentru a detecta atacurile cibernetice în mai multe etape care acoperă domeniile IT și OT, în timp ce analiza pasivă a traficului de rețea îmbunătățește detectarea amenințărilor în sistemele de control industrial (ICS). Descoperirea automată a activelor și vizibilitatea continuă a dispozitivelor IoT conectate consolidează și mai mult postura de securitate a sistemului și îi sporesc reziliența cibernetică.

Soluțiile de securitate propuse sunt validate experimental utilizând date reale ale sistemului de control industrial (ICS) și scenarii de testare a securității cibernetice IT. Rezultatele demonstrează capacități îmbunătățite de detectare a amenințărilor, comunicații IoT-cloud securizate și protecție îmbunătățită împotriva amenințărilor cibernetice în rețelele inteligente de energie solară bazate pe IoT.

Această cercetare contribuie la avansarea securității cibernetice în rețelele de energie regenerabilă bazate pe IoT prin furnizarea unei arhitecturi de securitate cu mai multe straturi, monitorizarea proactivă a amenințărilor și cadre de securitate bazate pe conformitate. Direcțiile viitoare de cercetare includ explorarea în continuare a criptografiei post-cuantice, a gestionării identității bazate pe blockchain, a arhitecturilor de încredere zero și a conformității cu standardele internaționale de securitate cibernetică pentru a spori reziliența securității infrastructurilor inteligente de energie regenerabilă bazate pe IoT.

Tabla de conținut

Rezumat 2

1. Introducere 6

1.1. Necesitatea și justificarea tezei 6

1.2. Scopul și obiectivele tezei 6

1.3. Metodologie de cercetare și analiză bibliometrică 7

1.4. Structura și conținutul tezei 8

2. Securitatea cibernetică în rețelele inteligente de energie solară bazate pe IoT 10

2.1. Provocări de securitate cibernetică și strategii de atenuare în sistemele solare inteligente bazate pe IoT 10

2.2. Concluzie 12

3. Securitatea cibernetică Amenințare Modelare pentrun bazate pe IoT inteligente sisteme solare 15

3.1. Metodologie integrată de modelare a amenințărilor și arhitectură de sistem 15

3.2. Analiza amenințărilor și evaluarea riscurilor pentru sistemele de energie solară bazate pe IoT Smart 17

3.3. Nivel dispozitiv securitate: O analiză aprofundată a vulnerabilităților firmware-ului 20

3.4. Concluzie 20

4. Dezvoltarea unui sistem de monitorizare securizat pentru rețele de energie solară bazate pe IoT 24

4.1. Arhitectură și proiectare sistemului 24

4.2. Implementarea unui sistem securizat de monitorizare a energiei solare bazat pe IoT 25

4.3. Rezultate și Discuții 27

4.4. Concluzie 28

5. Soluții de monitorizare și securitate bazate pe cloud pentru sistemele de energie solară bazate pe IoT 30

6. Dezvoltarea monitorizării, detectării și răspunsului proactiv la amenințări: Integrarea SIEM și a securității OT în sisteme de energie solară bazate pe IoT 33

6.1. Arhitectură de securitate pentru monitorizarea integrată a amenințărilor cibernetice IT-OT 33

6.2. Integrarea monitorizării securității IT și OT pentru monitorizarea unificată a amenințărilor, detectarea și gestionarea incidentelor 34

6.3. Validarea și evaluarea securității sistemului integrat de monitorizare a amenințărilor IT-OT 35

7. Concluzii finale 39

7.1. Concluzii 39

7.2. Contribuții originale 47

7.3. Valorificarea rezultatelor cercetării 49

7.4. Noi direcții de cercetări 51

Bibliografie 52

1. Introducere

1.1. Necesitatea și justificarea tezei

Creșterea globală a cererii de energie și impactul negativ asupra mediului al arderii combustibililor fosili impun trecerea la surse de energie regenerabile, cum ar fi energia solară fotovoltaică (PV), eoliană, hidroelectrică, geotermală și biomasa[1], [2], [3], [4], [5] . Sistemele de energie regenerabilă (SER) oferă alternative mai curate și mai durabile, reducând semnificativ emisiile de gaze cu efect de seră și consolidând independența energetică, creșterea economică și crearea de locuri de muncă, în special în zonele izolate [6], [7], [8], [9], [10], [11]. Adoptarea pe scară largă a sistemelor fotovoltaice solare este determinată de durabilitatea acestora, de resursele solare abundente și de progresele tehnologice rapide, previziunile indicând contribuții substanțiale la nevoile energetice globale până la mijlocul secolului[12], [13], [14].

Integrarea tehnologiilor internetului obiectelor (IoT) în SER a avansat semnificativ gestionarea și eficiența operațională. Sistemele bazate pe IoT facilitează colectarea datelor în timp real, întreținerea predictivă prin analize avansate, învățare automată și utilizarea optimizată a energiei[15], [16] ,[17], [18], [19]. Această conectivitate îmbunătățește SER cu rețelele inteligente, asigurând îmbunătățirea stabilității rețelei și a schimbului de energie.

Cu toate acestea, încorporarea IoT introduce, de asemenea, riscuri și vulnerabilități considerabile de securitate cibernetică, cum ar fi atacurile de tip denial-of-service (DoS), accesul neautorizat, încălcarea securității datelor și manipularea sistemului [20], [21], [22]. Aceste amenințări la adresa securității cibernetice prezintă riscuri semnificative pentru fiabilitatea, integritatea și confidențialitatea SER, în special în cazul instalațiilor solare bazate pe IoT. În plus, natura sistemelor inteligente de energie solară bazate pe IoT ca sisteme care implică atât tehnologia informației (IT), cât și tehnologia operațională (OT) agravează și mai mult aceste provocări prin extinderea suprafețelor potențiale de atac [23], [24], [25].

Deși cercetările existente au abordat probleme de securitate cibernetică, acestea se concentrează în principal pe vulnerabilități și atacuri specifice în cadrul anumitor componente, neexistând un cadru cuprinzător de securitate cibernetică adaptat în mod explicit sistemelor inteligente de energie solară bazate pe IoT. În plus, majoritatea studiilor se concentrează pe scenarii generale de rețele inteligente, neglijând cerințele unice de securitate cibernetică ale sistemelor fotovoltaice. Abordând aceste lacune, această cercetare pune accentul pe dezvoltarea unui cadru de securitate cibernetică integrat și holistic care unifică securitatea IT și OT, sporind astfel reziliența și fiabilitatea generală a infrastructurilor de energie regenerabilă împotriva amenințărilor cibernetice în evoluție.

1.2. Scopul și obiectivele tezei

Scopul cercetării:

Această cercetare vizează dezvoltarea unui cadru unificat de securitate cibernetică pentru sistemele inteligente de energie solară bazate pe IoT. Cadrul va integra comunicarea securizată, detectarea avansată a amenințărilor, monitorizarea în timp real și capacitățile proactive de răspuns la incidente

pentru a spori securitatea, reziliența și integritatea rețelelor de energie regenerabilă. Prin abordarea vulnerabilităților unice ale sistemelor de energie solară bazate pe IoT, această cercetare urmărește să protejeze infrastructurile energetice critice împotriva amenințărilor cibernetice moderne, sprijinind în același timp eforturile globale pentru tranziții energetice durabile.

Obiective specifice:

Pentru a atinge obiectivul principal, cercetarea este ghidată de următoarele obiective:

O1. Să analizeze amenințările și vulnerabilitățile la adresa securității cibernetice în sistemele inteligente de energie solară bazate pe IoT.

Q2. Modelarea amenințărilor pentru dezvoltarea sistemului fotovoltaic solar inteligent bazat pe IoT

O3. Proiectarea și implementarea unui sistem de monitorizare inteligent și securizat pentru rețelele de energie solară bazate pe IoT.

O4. Dezvoltarea unui cadru unificat și proactiv de monitorizare, detectare și gestionare a incidentelor de securitate cibernetică prin integrarea soluțiilor de securitate SIEM și OT.

O5. Evaluarea și validarea eficacității cadrului de securitate propus utilizând date din lumea reală.

Această cercetare și-a atins obiective și contribuie la avansarea securității cibernetice în SER bazate pe IoT. Cadrul propus asigură comunicarea securizată a datelor, monitorizarea în timp real și gestionarea proactivă a amenințărilor cibernetice, a energia solare, îmbunătățind reziliența, disponibilitatea și securitatea rețelelor inteligente. Această lucrare abordează provocările imediate de securitate cibernetică ale sistemelor de energie solară bazate pe IoT. Ea sprijină obiectivele mai largi ale tranzițiilor energetice durabile și ale atenuării schimbărilor climatice prin protejarea infrastructurilor energetice critice împotriva amenințărilor cibernetice în evoluție.

1.3. Metodologie de cercetare și analiză bibliometrică

Cercetarea prezentată în această teză de doctorat, intitulată "Cybersecurity Challenges for IoT-Based Smart Renewable Energy Networks", se concentrează pe sistemele inteligente de energie solară bazate pe IoT. Metodologia de cercetare abordează sistematic provocările de securitate cibernetică în acest domeniu. Metodologia este organizată în următoarele etape-cheie:

1. Identificarea problemei de cercetare
2. Definirea domeniului de aplicare și a direcției de cercetare
3. Documentație și analiză critică
4. Dezvoltarea unei soluții integrate de securitate cibernetică
5. Realizarea practică și validarea ei
6. Stabilirea de noi direcții de cercetare

Pentru a stabili relevanța subiectului de cercetare și a oferi o analiză de ultimă oră a sistemelor de energie regenerabilă bazate pe IoT, a fost efectuată o revizuire sistematică a literaturii de specialitate.

Strategia de căutare a fost concepută cu atenție și pusă în aplicare în conformitate cu orientările PRISMA, astfel cum sunt descrise în referința [26] și a urmat criteriile de căutare științifică furnizate în referințe [27] și [28].

1.4. Structura și conținutul tezei

Această teză de doctorat este structurată în șapte capitole, fiecare abordând aspecte critice ale securizării rețelelor de energie regenerabilă activate de IoT. Cercetarea urmează o progresie logică, începând cu identificarea problemei și contextul teoretic, avansând spre dezvoltarea și implementarea cadrelor de securitate și încheind cu validarea, diseminarea și direcțiile viitoare de cercetare. Teza își propune să ofere perspective noi prin integrarea modelării amenințărilor, a comunicării sigure, securitate bazată pe cloud și mecanisme de monitorizare proactivă pentru a spori reziliența și securitatea acestor sisteme.

Capitolul 1: Introducere: Acest capitol stabilește contextul și motivația cercetării, prezentând necesitatea și justificarea securității cibernetice în sistemele inteligente de energie solară bazate pe IoT. Acesta definește scopul și obiectivele cercetării, prezintă metodologia de cercetare și include o analiză bibliometrică pentru a demonstra importanța științifică a cercetării. Capitolul se încheie cu o prezentare generală a structurii tezei.

Capitolul 2: Securitatea cibernetică în rețelele inteligente de energie solară bazate pe IoT: Acest capitol analizează în mod cuprinzător provocările, vulnerabilitățile și riscurile legate de securitatea cibernetică în sistemele inteligente de energie solară bazate pe IoT. Se discută despre amenințările cibernetice care vizează rețelele energetice bazate pe IoT și impactul lor potențial asupra fiabilității sistemului, integrității datelor și securității operaționale. Contramăsurile de securitate existente sunt analizate critic pentru a identifica lacunele în implementările actuale de securitate.

Capitolul 3: Modelarea amenințărilor la adresa securității cibernetice pentru sistemele inteligente de energie solară bazate pe IoT: Acest capitol introduce sistematic tehnici de modelare a amenințărilor pentru a analiza potențialele riscuri cibernetice în rețelele solare bazate pe IoT. Modelul de amenințare STRIDE este aplicat pentru a identifica și clasifica amenințările care afectează dispozitivele IoT, protocoalele de comunicare și fluxurile de date. În plus, modelul de evaluare a riscurilor DREAD este utilizat pentru a cuantifica gravitatea acestor riscuri, oferind o evaluare structurată pentru sistem. Este examinat un scenariu de utilizare, demonstrând modul în care modelarea amenințărilor poate identifica în mod proactiv vulnerabilitățile și poate sprijini dezvoltarea de contramăsuri. În plus față de analiza securității la nivel de sistem, acest capitol examinează vulnerabilitățile de securitate la nivel de dispozitiv prin efectuarea unei evaluări a vulnerabilității firmware a dispozitivelor IoT integrate în sistemele de energie solară.

Capitolul 4: Dezvoltarea unui sistem de monitorizare securizat pentru rețelele de energie solară bazate pe IoT: Acest capitol se concentrează pe dezvoltarea și implementarea mecanismelor de securitate pentru a spori reziliența sistemelor inteligente de energie solară. Acesta prezintă o arhitectură de monitorizare securizată care integrează criptarea AES pentru securitatea datelor, Transport Layer Security (TLS) pentru comunicarea securizată și mecanisme de autentificare pentru a preveni accesul

neautorizat. Capitolul demonstrează modul în care monitorizarea la distanță în timp real îmbunătățește fiabilitatea sistemului într-o rețea solară bazată pe IoT.

Capitolul 5: Soluții de monitorizare și securitate bazate pe cloud pentru sistemele de energie solară bazate pe IoT: Acest capitol explorează integrarea serviciilor cloud pentru a permite monitorizarea securizată de la distanță, gestionarea datelor și analizele avansate pentru rețelele de energie solară bazate pe IoT. Acesta detaliază implementarea serviciilor Microsoft Azure IoT (IoT Hub, Stream Analytics, Power BI și Time Series Insights). Se implementează mecanisme de securitate bazate pe cloud, cum ar fi autentificarea dispozitivelor, autorizarea, criptarea TLS, controlul accesului și autentificarea bazată pe roluri.

Capitolul 6: Dezvoltarea sistemelor proactive de monitorizare, detectare și răspuns la amenințări: Integrarea SIEM și a securității OT în sistemele de energie solară bazate pe IoT: Acest capitol prezintă dezvoltarea unui cadru unificat de monitorizare proactivă a securității cibernetice și de gestionare a incidentelor, care integrează soluții de gestionare a informațiilor și evenimentelor de securitate și de securitate OT. Cercetarea utilizează SIEM și Defender pentru IoT pentru a permite detectarea anomaliilor în timp real, informații despre amenințări și corelarea evenimentelor de securitate în straturile IT, IoT și OT. Pentru a măsura eficacitatea mecanismelor de securitate în atenuarea amenințărilor la adresa securității cibernetice, se efectuează un proces de validare folosind date reale din ICS și IT tradiționale. Rezultatele experimentale demonstrează modul în care monitorizarea unificată a securității îmbunătățește detectarea proactivă a amenințărilor și răspunsul automat la incidente în sistemele inteligente de energie solară bazate pe IoT.

Capitolul 7: Concluzii finale, contribuții originale, valorificarea rezultatelor cercetării și noi direcții de cercetare: Acest capitol rezumă concluziile, evidențiind contribuțiile cheie la securizarea rețelelor de energie regenerabilă bazate pe IoT. Contribuțiile originale ale autorului subliniază modul în care soluțiile de securitate cibernetică propuse sporesc securitatea, reziliența și monitorizarea sistemelor energetice inteligente. În plus, capitolul discută diseminarea rezultatelor prin publicații științifice, conferințe și potențiale aplicații industriale. În cele din urmă, sunt prezentate direcțiile viitoare de cercetare, identificând domeniile în care se pot face progrese suplimentare în acest domeniu.

2. Securitatea cibernetică în rețelele inteligente de energie solară bazate pe IoT

2.1. Provocări de securitate cibernetică și strategii de atenuare în sistemele solare inteligente bazate pe IoT

Tabelul 1 rezumă cercetările existente privind diverse amenințări cibernetice, inclusiv atacurile de tip Denial of Service, atacurile de tip False Data Injection, atacurile cu parolă, atacurile de tip Replay și atacurile Man-in-the-Middle, împreună cu contramăsurile actuale ale acestora. Cercetările anterioare au identificat mai multe măsuri-cheie de securitate cibernetică pentru a spori reziliența sistemelor fotovoltaice inteligente bazate pe IoT. IDS și IPS sunt esențiale pentru monitorizarea și protejarea acestor sisteme prin detectarea și blocarea breșelor de securitate. IDS asigură detectarea amenințărilor în timp real prin tehnici bazate pe semnături și anomalii, în timp ce IPS asigură o apărare proactivă prin prevenirea activităților suspecte. Actualizările periodice ale acestor sisteme sunt esențiale pentru a face față evoluției amenințărilor cibernetice. Controlul accesului și mecanismele de autentificare a utilizatorilor, inclusiv autentificarea cu mai mulți factori (MFA) și accesul bazat pe roluri, contribuie, de asemenea, la restricționarea accesului neautorizat. Criptarea datelor este vitală pentru protejarea cantității mari de date generate de sistemele fotovoltaice bazate pe IoT, asigurând conformitatea cu reglementările privind confidențialitatea fără a compromite performanța sistemului. Tehnicile de învățare automată (ML) au fost, de asemenea, aplicate pentru a detecta atacuri specifice. Alte măsuri necesare includ actualizări periodice ale software-ului și gestionarea patch-urilor pentru a aborda vulnerabilitățile și segmentarea rețelei pentru a izola componentele sistemului și pentru a limita potențialele atacuri.

Tabelul 1. Amenințări cibernetice și contramăsuri actuale în sistemele energetice bazate pe IoT

Atac	Ținte	**Contramăsuri**	Referință
Atac FDI	PV (fotovoltaic)	ML-artificial neural network	[29]
Atac FDI	Rețea inteligentă	Margin Setting Algorithm (MSA).	[30]
Atac FDI	PV (fotovoltaic)	Artificial Neural Network	[29]
Atac DoS	Surse de energie distribuite (DER)	Virtual Synchrophasor Network	[31]
Atac FDI	Smart grids	IDS, DLP, and SIEM	[32]
Atac FDI	Microrețele DC	recurrent neural network	[33]
Atac FDI	Rețea inteligentă	Deep belief networks	[34]

Atac de tip Man-in-the-Middle (MitM)	SCADA PV	Utilizarea criptării	[35]
Atac FDI		Verificarea integrității datelor	
Atac DoS	Sistems fotovoltaic	Data-driven method for detection	[25]
Atac FDI		Deep neural networks, vector autoregressive model	
Atac DoS	Nanorețea	IPS and IDS	[36]
Atac FDI		-Use of TLS -Encryption technique	
Atac de rejucare	DER, Sistems fotovoltaic	Utilization of FTP-SSL protocols and sTELNET	[37]
Atac de tip Man-in-the-Middle (MitM)		Criptarea datelor	
Atac de tip Man-in-the-Middle (MitM)	Surse de energie distribuite (DER)	PKI Intelligence-driven algorithms Encrypting communication	[38]
Atac prin parolă		MFA Single sign-on	
Atac de tip Man-in-the-Middle (MitM)	Prosumator Nanorețea	Cheie SSH	[39]
Atac DoS		Snort, Zeek IDS	
Atac FDI	Sistems fotovoltaic	Detectarea amenințărilor bazată pe rețele neuronale	[40]
		Sanitizarea parametrilor de acces	
		Sistem de detectare a intruziunilor (IDS)	
Atac de rejucare	Rețea inteligentă	Algoritmul HMAC-MD5	[41]

Atac de tip Man-in-the-Middle (MitM)	DC Microgrids	Algoritm ML cu optimizare Gray Wolf	[42]
Atac FDI	DC Microrețele	-circuite oscilatoare pasive -Relee diferențiale de curent	[43]

Deși cercetările anterioare au abordat în mod semnificativ amenințările la adresa securității cibernetice, acestea se concentrează în principal pe atenuarea atacurilor specifice care vizează vulnerabilitățile dispozitivelor individuale din cadrul sistemului. Această abordare nu oferă o strategie cuprinzătoare de abordare a provocărilor mai ample de securitate cibernetică cu care se confruntă sistemele energetice fotovoltaice bazate pe IoT. În plus, o mare parte din cercetările actuale se concentrează pe sectorul rețelelor inteligente, trecând adesea cu vederea nevoile specifice de securitate cibernetică ale SER, cum ar fi instalațiile de energie solară, care sunt din ce în ce mai adoptate la nivel mondial. Această lacună evidențiază necesitatea unei abordări mai holistice care integrează securitatea IT și OT, abordează provocările unice ale sistemelor de energie solară bazate pe IoT și oferă protecție de la un capăt la altul împotriva amenințărilor cibernetice în continuă evoluție. Abordarea acestui decalaj este esențială pentru a asigura reziliența și fiabilitatea infrastructurilor de energie regenerabilă în fața amenințărilor cibernetice în creștere.

2.2. Concluzie

Analiza critică din acest capitol a determinat provocările de securitate cibernetică asociate cu rețelele inteligente de energie solară bazate pe IoT, concentrându-se pe vulnerabilități, vectori de atac și contramăsuri actuale. Capitolul a analizat sistematic arhitectura cu două straturi a nanorețelelor și microrețele, subliniind interacțiunea dintre componentele fizice și cibernetice și a identificat riscurile critice de securitate care decurg din această interconectare.

Capitolul a explorat, de asemenea, motivațiile din spatele atacurilor cibernetice asupra sistemelor fotovoltaice, de la câștiguri financiare la spionaj și activism ideologic, și a clasificat diverșii vectori de atac pe care îi exploatează actorii rău intenționați. Prin examinarea unor amenințări specifice, cum ar fi atacurile DoS și DDoS, FDI, MitM și ransomware, capitolul a analizat modul în care aceste amenințări pot perturba producția de energie, pot cauza pierderi financiare și pot destabiliza funcționarea rețelei. În plus, capitolul a analizat eficacitatea măsurilor de securitate actuale, inclusiv IPS și IDS, mecanismele de control al accesului, învățarea automată, criptarea datelor și segmentarea rețelei în atenuarea acestor amenințări.

Următoarele sunt principalele contribuții extrase din acest capitol:

1. Identificarea vulnerabilităților sistemelor ciber-fizice:

- Structura și componentele atât ale nanorețelelor, cât și ale microrețelelor sunt clasificate, punându-se accentul pe arhitectura lor cu două straturi (fizic și cibernetic). Au fost identificate vulnerabilitățile inerente acestor sisteme, în special în protocoalele de comunicare, firmware-ul și software-ul utilizate în sistemele fotovoltaice bazate pe IoT.

Analiza privind potențialul de manipulare fizică și de atacuri de la distanță evidențiază necesitatea unor măsuri de securitate puternice pentru a proteja atât aspectele cibernetice, cât și cele fizice ale acestor sisteme.

2. Analiza motivelor și vectorilor de atac pentru sistemele fotovoltaice bazate pe IoT:

- A fost realizată o clasificare a vectorilor de atac în atacuri la distanță, fizice, interne și în lanțul de aprovizionare, oferind o înțelegere detaliată a modului în care atacatorii exploatează punctele slabe ale sistemelor fotovoltaice bazate pe IoT. Aceasta a furnizat raționamentul din spatele atacurilor cibernetice asupra sistemelor fotovoltaice, inclusiv motive economice, de spionaj și ideologice. Analiza modelului Cyber Kill Chain, în special în ceea ce privește sistemele fotovoltaice, oferă o metodă sistematică pentru înțelegerea și contracararea amenințărilor persistente avansate (APT).

3. Examinarea amenințărilor cibernetice specifice în sistemele fotovoltaice bazate pe IoT:

- Au fost evaluate amenințările cibernetice, cum ar fi atacurile MitM, DoD și DDoS, FDI și ransomware, analizându-se impactul lor potențial asupra sistemelor fotovoltaice, inclusiv întreruperile producției de energie, pierderile economice și riscurile pentru stabilitatea rețelei.

4. Analiza măsurilor actuale de securitate pentru sistemele fotovoltaice bazate pe IoT:

- Au fost analizate contramăsurile actuale de atenuare a amenințărilor cibernetice în sistemele fotovoltaice bazate pe IoT. Primul tip de contramăsuri, IPS și IDS Sisteme pentru monitorizarea operațiunilor sistemului și a traficului de rețea pentru a detecta și a răspunde la încălcările securității. Tehnicile de control al accesului, inclusiv RBA și MFA sunt determinate ca fiind esențiale pentru restricționarea accesului neautorizat. În plus, criptarea datelor poate fi utilizată ca măsură esențială pentru protejarea informațiilor sensibile în timpul transmiterii și stocării. În plus, importanța gestionării consecvente a patch-urilor și a actualizării software-ului pentru a aborda vulnerabilitățile este examinată împreună cu segmentarea rețelei, care ajută la limitarea atacurilor prin divizarea rețelei în rețele mai mici, izolate. În cele din urmă, tehnicile de învățare automată, sensibilizarea continuă cu privire la Securitate formarea părților interesate și evaluarea securității furnizorilor pot oferi o poziție de securitate cuprinzătoare.

5. Lacune în cercetare:

- Deși cercetările existente au făcut progrese semnificative în abordarea amenințărilor cibernetice specifice, capitolul identifică o lacună critică în literatura de specialitate: lipsa unei abordări holistice a securității cibernetice în sistemele de energie regenerabilă bazate pe IoT. Majoritatea studiilor se concentrează pe vulnerabilități sau dispozitive individuale, trecând adesea cu vederea natura interconectată a acestor sisteme. Rezultatele acestui capitol au fost publicate în [44].

Capitolul contribuie în mod direct la atingerea obiectivului O1 (analiza amenințărilor la adresa securității

cibernetice și a vulnerabilităților în sistemele inteligente de energie solară bazate pe IoT) prin efectuarea unei evaluări sistematice a amenințărilor și vulnerabilităților cibernetice. Analiza prezentată aici constituie baza pentru abordarea de modelare a amenințărilor introdusă în capitolul 3.

3. Securitatea cibernetică Amenințare Modelare pentrun bazate pe IoT inteligente sisteme solare

3.1. Metodologie integrată de modelare a amenințărilor și arhitectură de sistem

Acest capitol prezintă o abordare cuprinzătoare a modelării amenințărilor în sistemele fotovoltaice solare inteligente bazate pe IoT pentru a identifica, evalua și prioritiza în mod proactiv riscurile de securitate cibernetică. Modelarea amenințărilor devine esențială pentru securizarea infrastructurilor energetice odată cu extinderea suprafeței de atac introdusă de dispozitivele IoT, serviciile cloud și componentele interconectate.

Modelarea amenințărilor este necesară din cauza complexității crescânde a amenințărilor cibernetice care vizează sistemele solare inteligente. Aceste sisteme sunt formate din diverse componente - senzori IoT, noduri IoT, gateway-uri de teren, platforme cloud și zone de acces de la distanță - care sunt vulnerabile la diferite tipuri de atacuri. Modelarea amenințărilor permite analiza structurată a acestor vulnerabilități înainte ca acestea să poată fi exploatate.

Cazul de utilizare al sistemului inteligent de energie solară bazat pe IoT dezvoltat este prezentat în figura 1. Arhitectura sistemului include următoarele straturi interconectate:

Stratul fizic: Module fotovoltaice și senzori de mediu/electrici.

Nivelul nodului IoT: dispozitiv myRIO-1900 pentru procesarea și controlul local al datelor. Stratul de comunicare: Gateway-uri de teren IoT și interfețe de rețea.

Cloud Layer: Azure IoT Hub, Stream Analytics și Power BI pentru stocarea, analiza și vizualizarea datelor.

Zona utilizatorului la distanță: Tablouri de bord bazate pe web pentru monitorizarea la distanță în timp real

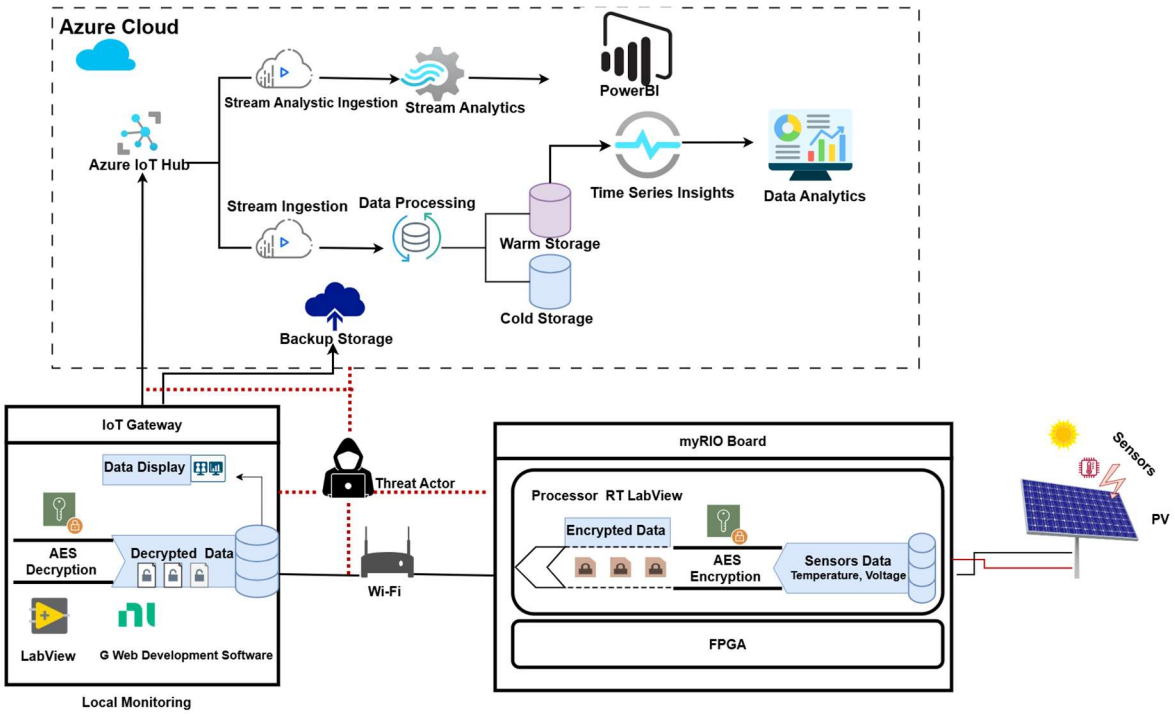

Figura 1. Arhitectura sistemului pentru cazul de utilizare Sistem inteligent de energie solară.

Pentru a identifica și evalua sistematic riscurile potențiale, această cercetare utilizează două metodologii:

Modelul STRIDE: Utilizat pentru a clasifica amenințările în șase categorii - falsificare, manipulare, repudiere, divulgare de informații, negare de serviciu și ridicare de privilegii[45]. Procesul STRIDE de analiză a amenințărilor este vizualizat în figura 2, ilustrând modul în care amenințările sunt identificate sistematic în diferite straturi ale sistemului.

Modelul DREAD: Aplicat pentru a evalua fiecare amenințare identificată pe baza potențialului de pagubă, a reproductibilității, a exploatabilității, a utilizatorilor afectați și a posibilității de descoperire, atribuind un scor de risc pentru stabilirea priorităților[46]. Modelul DREAD evaluează cantitativ fiecare amenințare identificată pe baza unui sistem de notare de la 1 (scăzut) la 10 (critic). Acest lucru permite prioritizarea structurată.

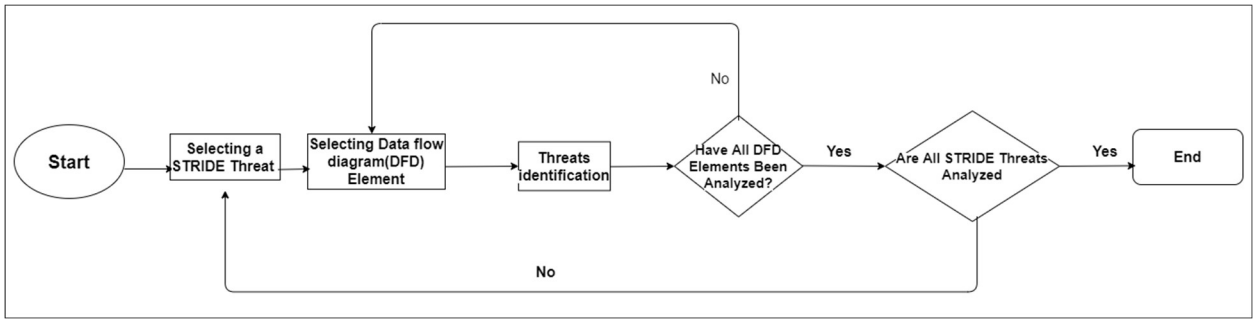

Figura 2. Diagrama de flux a procesului de analiză a amenințărilor STRIDE.

O diagramă a fluxului de date (DFD) [47] din figura 3 a fost elaborată pentru a ilustra modul în care datele circulă între aceste componente ale sistemului, evidențiind limitele critice de încredere și

potențialele riscuri de securitate. Și STRIDE a fost utilizat pentru a analiza riscurile de securitate în diferite zone ale sistemului, inclusiv zona utilizatorului local, zona serviciilor cloud și zona la distanță, pentru a clasifica mai bine riscurile din aceste zone.

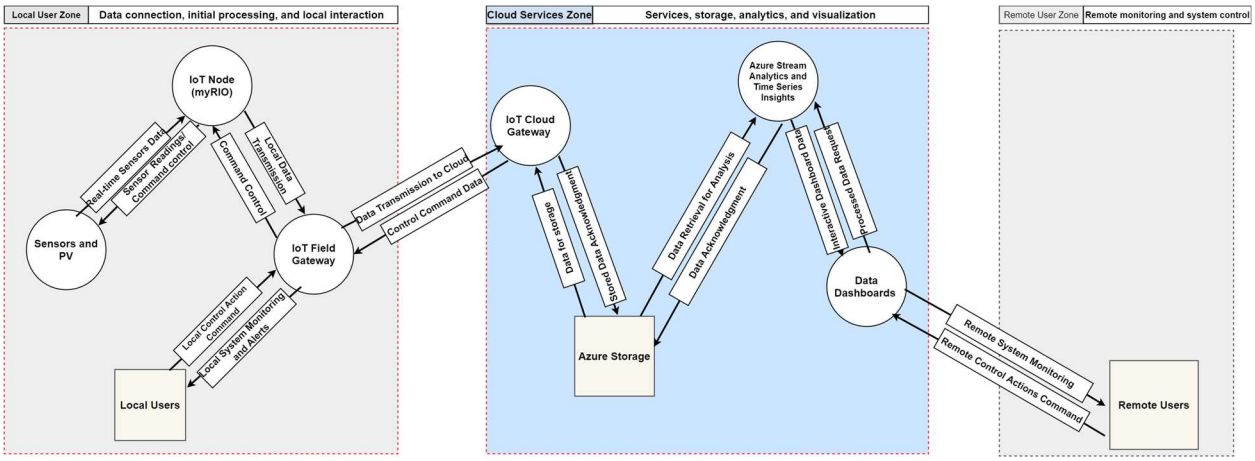

Figura 3. Diagrama fluxului de date pentru cazul de utilizare a sistemului.

3.2. Analiza amenințărilor și evaluarea riscurilor pentru sistemele de energie solară bazate pe IoT Smart

Această secțiune aplică metodologia de modelare a amenințărilor STRIDE pentru a analiza sistematic vulnerabilitățile din diferite zone ale sistemului, în special zona utilizatorului local, zona serviciilor cloud și zona utilizatorului la distanță. Pentru a cuantifica și prioritiza aceste amenințări de securitate identificate, acest studiu aplică modelul de evaluare a riscurilor DREAD. Fiecărei amenințări i s-a atribuit un scor numeric de la 1 (risc scăzut) la 10 (risc critic), Această metodologie clasifică riscurile în scăzute (1,0 - 3,9), medii (4,0 - 6,9), niveluri ridicate (7,0 - 8,9) și critice (9,0 - 10,0), facilitând stabilirea structurată a priorităților pentru atenuarea securității cibernetice.

Evaluarea DREAD a fost aplicată în toate cele trei zone operaționale, iar tabelul 2 ilustrează constatările pentru zona utilizatorilor locali. Amenințările prezintă riscuri semnificative pentru integritatea senzorilor, acuratețea datelor și mecanismele locale de autentificare a dispozitivelor.

Tabelul 2. Analiza de risc DREAD pentru zona utilizatorului local în sistemele inteligente de energie solară bazate pe IoT

Categoria de amenințare	Componentă	Amenințare identificată	D	R	E	A	D	Scorul de risc	Nivelul de risc
S	Sensors to IoT Node	Uzurparea identității senzorilor	9	8	9	8	7	8.2	Mare
S	Local User to IoT Gateway	Falsificarea utilizatorului	8	7	8	7	7	7.4	Mare

		pentru acces neautorizat							
T	IoT Node to IoT Gateway	Modificarea datelor între nodul IoT și gateway	8	7	8	7	7	7.4	Mare
T	Sensors	Manipularea fizică a senzorilor	9	8	9	8	7	8.2	Mare
R	Local User to IoT Node	Utilizatorii neagă efectuarea modificărilor în sistem	6	5	6	5	7	5.8	Mediu
I	IoT Node	Expunerea informațiilor sensibile	7	6	7	6	6	6.4	Mediu
I	Sensors to IoT Node	Interceptarea datelor senzorilor în timpul transmiterii	7	6	7	6	6	6.4	Mediu
D	IoT Gateway	Suprasolicitarea gateway-ului cu cereri	9	8	9	8	6	8	Mare
D	IoT Field Gateway	Atac DoS asupra gateway-ului de câmp IoT	8	7	8	7	6	7.2	Mare
E	Utilizator local	Utilizatorii obțin privilegii de acces neautorizate	10	9	10	9	7	9	Critic

În zona serviciilor cloud, tabelul 3 prezintă constatările analizei de risc DREAD.

Tabelul 3. Analiza de risc DREAD pentru zona de servicii cloud în sistemele inteligente de energie solară bazate pe IoT

Categoria de amenințare	Componentă	Amenințare identificată	D	R	E	A	D	Scorul de risc	Nivelul de risc
S	IoT Field Gateway to Cloud Gateway	Atacatorii falsifică gateway-ul de câmp IoT	9	8	9	8	7	8.2	Mare
T	Data Flow from IoT Field Gateway to Cloud Gateway	Interceptarea și modificarea datelor în timpul transmiterii	8	7	8	7	7	7.4	Mare
T	Cloud Storage	Modificare neautorizată a datelor stocate	9	8	9	8	8	8.4	Mare
I	IoT Field Gateway to Cloud Gateway	Expunerea datelor sensibile în timpul transmiterii necriptate	7	6	7	6	7	6.6	Mediu
I	Cloud Storage	Acces neautorizat la datele stocate în cloud	8	7	8	7	6	7.2	Mare
D	Stream Analytics	Suprasolicitarea serviciilor de analiză a fluxurilor de date	9	8	9	8	6	8	Mare
D	Cloud Gateway	Atac de tip Denial of Service asupra gateway-ului cloud	8	7	8	7	6	7.2	Mare
E	Cloud Dashboard and Admin Control	Escaladarea neautorizată a privilegiilor	10	9	10	9	7	9	Critic

De asemenea, s-a constatat că zona de utilizator la distanță este susceptibilă la atacuri de substituire a identității, modificări ale programelor malware și escaladarea privilegiilor. Dependența de mecanismele de control al accesului la distanță și de protocoalele de comunicare nesecurizate crește riscul de acces neautorizat, în cazul în care adversarii pot intercepta acreditările utilizatorilor, manipula

comenzile de control sau injecta software rău intenționat în sistem.

3.3. Nivel dispozitiv securitate: O analiză aprofundată a vulnerabilităților firmware-ului

Această secțiune prezintă o analiză aprofundată a vulnerabilităților firmware-ului pentru myRIO-1900 [48], o componentă critică în cadrul sistemului fotovoltaic solar inteligent bazat pe IoT. Evaluarea a scos la iveală puncte slabe de securitate semnificative, inclusiv firmware fără patch-uri, biblioteci învechite și implementări criptografice slabe care prezintă riscuri substanțiale pentru integritatea, confidențialitatea și disponibilitatea sistemului.

Au fost identificate un total de 117 vulnerabilități și expuneri comune (CVE) cunoscute, inclusiv defecte critice în componente precum wpasupplicant, OpenSSH, OpenVPN, OpenSSL și libcurl. Aceste vulnerabilități permit executarea potențială a codului de la distanță, escaladarea privilegiilor și manipularea datelor. Acest nivel de expunere face din dispozitiv un punct de intrare cu risc ridicat pentru atacatorii care vizează infrastructura solară inteligentă.

Analiza a identificat, de asemenea, deficiențe criptografice importante, inclusiv numeroase certificate expirate și auto-semnate și semnături digitale slabe, toate acestea expunând sistemul la atacuri MITM (man-in-the- middle) și acces neautorizat de la distanță. Gestionarea deficitară a certificatelor subminează în mod semnificativ canalele de comunicare securizate din cadrul sistemului.

Evaluarea suplimentară a protecțiilor binare ale firmware-ului a evidențiat lacune în măsurile esențiale de întărire. În timp ce unele protecții precum NX Bit și RELRO au fost implementate eficient, mecanisme critice precum Stack Canary și PIE au fost fie parțial aplicate, fie au lipsit cu desăvârșire. Aceste omisiuni cresc riscul de corupere a memoriei și de atacuri de tip buffer overflow, ceea ce ar putea permite compromiterea întregului sistem.

Aceste constatări evidențiază o lacună gravă în securitatea la nivel de dispozitiv care ar putea fi exploatată pentru compromiterea datelor, perturbarea funcțiilor de gestionare a energiei sau lansarea de atacuri persistente. Abordarea unor astfel de vulnerabilități prin actualizări în timp util ale firmware-ului, practici criptografice puternice și tehnici robuste de întărire binară este esențială pentru creșterea rezistenței și fiabilității sistemelor inteligente de energie solară bazate pe IoT.

3.4. Concluzie

A fost realizată o modelare a amenințărilor la adresa securității cibernetice și o evaluare a riscurilor pentru un anumit sistem energetic fotovoltaic solar bazat pe IoT. Acest proces a utilizat cadrele STRIDE și DREAD pentru identificarea, clasificarea și prioritizarea sistematică a potențialelor amenințări la adresa securității. Cercetarea s-a concentrat asupra problemelor unice de securitate declanșate de interdependența dispozitivelor IoT, a serviciilor cloud și a infrastructurii fotovoltaice, care formează împreună un sistem complex și interconectat.

A fost efectuată o analiză cuprinzătoare a amenințărilor în zona utilizatorului local, în zona serviciilor cloud și în zona utilizatorului de la distanță, investigând riscuri semnificative, cum ar fi falsificarea,

alterarea, informațiile dezvăluirea de informații, refuzul de serviciu și atacurile de ridicare a privilegiilor. Evaluarea cantitativă a riscurilor bazată pe DREAD a prioritizat în continuare aceste amenințări în funcție de impactul lor potențial, facilitând o strategie de securitate orientată către riscuri pentru sistemele fotovoltaice bazate pe IoT.

În plus față de modelarea amenințărilor la nivel de sistem, au fost luate în considerare considerațiile de securitate la nivel de dispozitiv. Vulnerabilitățile firmware-ului din dispozitivele IoT integrate au fost analizate pentru un PLC (myRIO) utilizat într-un sistem de energie solară. Evaluarea securității firmware-ului a evidențiat vulnerabilități critice nerezolvate (CVE), implementări criptografice slabe, certificate digitale expirate sau slabe și mecanisme inadecvate de întărire a firmware-ului, subliniind securitatea sporită la nivel de dispozitiv pentru a completa protecțiile sistemului mai larg. Principalele contribuții și constatări:

1. Caz de utilizare și arhitectură de sistem:
    - Analiza a utilizat un caz specific de utilizare a unui sistem energetic fotovoltaic bazat pe IoT, oferind un context realist și detaliat pentru identificarea amenințărilor și vulnerabilităților. Arhitectura sistemului a fost împărțită în trei zone principale: zona utilizatorului local, zona serviciilor cloud și zona utilizatorului la distanță, fiecare cu componente și funcționalități distincte. Această abordare structurată a permis o examinare focalizată a provocărilor de securitate inerente fiecărei zone.
2. Diagrama fluxului de date (DFD):
    - Diagrama fluxului de date (DFD) a fost utilizată pentru a cartografia vizual fluxul de date în cadrul sistemului, evidențiind punctele critice de interacțiune și definind limitele de încredere. DFD a servit drept instrument de bază pentru înțelegerea modului în care datele sunt prelucrate, transmise și stocate în cadrul sistemului, contribuind la identificarea atacurilor și vulnerabilităților potențiale. Prin clasificarea sistemului în trei zone - utilizator local, servicii cloud și utilizator la distanță - DFD a facilitat o analiză direcționată a amenințărilor specifice fiecărei zone.
3. Modelarea amenințărilor cu STRIDE:

- Modelul STRIDE a identificat și clasificat în mod metodic amenințările în șase dimensiuni-cheie. Acest cadru a permis o analiză detaliată a vulnerabilităților din zona utilizatorului local, zona serviciilor cloud și zona utilizatorului la distanță, evidențiind punctele critice în care sistemul este cel mai susceptibil la atacuri cibernetice.
- Analiza a arătat că fiecare zonă operațională prezintă provocări de securitate distincte. De exemplu, zona utilizatorilor locali este deosebit de vulnerabilă la spoofing (de exemplu, uzurparea identității senzorilor sau a utilizatorilor) și la alterare (de exemplu, modificarea neautorizată a datelor). În același timp, zona de servicii cloud se confruntă cu riscuri semnificative de negare a serviciului și de ridicare privilegiilor. Pe de altă parte, zona utilizatorilor la distanță este expusă unor amenințări precum accesul neautorizat și

interceptarea datelor în timpul interacțiunilor la distanță.

4. Evaluarea cantitativă a riscurilor cu DREAD:

- Pentru a completa clasificarea calitativă a amenințărilor furnizată de STRIDE, modelul DREAD a fost utilizat pentru a cuantifica gravitatea amenințărilor identificate pe baza a cinci criterii ale modelului DREAD. Tehnica cantitativă a facilitat prioritizarea riscurilor, asigurându-se că cele mai semnificative riscuri au fost abordate cu promptitudine.
- Evaluarea DREAD a arătat că amenințările cum ar fi falsificarea datelor, spoofing și ridicarea privilegiilor au fost printre cele mai grave, scorurile de risc ridicat indicând potențialul lor de a cauza daune semnificative sistemului.

5. Analiza vulnerabilității firmware-ului și securitatea la nivel de dispozitiv:

- A fost efectuată o evaluare cuprinzătoare a vulnerabilității firmware-ului controlerului logic programabil (PLC) myRIO-1900 pentru a identifica deficiențele de securitate la nivelul dispozitivului. Evaluarea a scos la iveală probleme critice, inclusiv componente software fără patch-uri, implementări criptografice slabe și mecanisme de actualizare nesigure, făcând dispozitivul susceptibil la infecții malware, modificări neautorizate și amenințări persistente.
- Analiza a detectat 117 vulnerabilități și expuneri comune (CVE) în firmware, clasificate în funcție de gravitate: 19 critice, 52 ridicate și 39 medii. Aceste vulnerabilități ar putea fi exploatate pentru a perturba funcționalitatea dispozitivului, pentru a obține acces neautorizat sau pentru a injecta cod rău intenționat în componente IoT esențiale, cum ar fi contoarele inteligente și invertoarele.
- Analiza certificatelor SSL a scos la iveală deficiențe de securitate semnificative, inclusiv 65 de certificate expirate, 138 de certificate cu semnături criptografice slabe și 90 de certificate auto-semnate. Astfel de deficiențe compromit comunicațiile criptate, crescând riscul atacurilor MITM și al amenințărilor legate de uzurparea identității.
- Evaluarea capacităților de întărire a firmware-ului a evidențiat lacune în mecanismele de atenuare a exploatărilor. În timp ce protecții precum bitul NX (No-eXecute) (100%) și RELRO (Read-Only Relocation) (91%) au fost bine implementate, altele, precum PIE (Position Independent Executable) (55%) și Stack Canary (3%), au arătat un spațiu semnificativ pentru îmbunătățire. Implementarea slabă a "stack canaries" expune firmware-ul la atacuri de tip buffer overflow și exploatări de corupere a memoriei.
- "Firmware security hardening" a fost evidențiat ca o strategie proactivă pentru menținerea igienei firmware-ului prin monitorizare continuă, remedierea periodică a vulnerabilităților și îmbunătățiri criptografice. Constatările subliniază necesitatea de a aplica politici criptografice stricte și de a îmbunătăți configurațiile de securitate pentru a consolida securitatea la nivel de dispozitiv în sistemele energetice fotovoltaice solare bazate pe IoT.
- Rezultatele evidențiază necesitatea critică a măsurilor de securitate la nivel de dispozitiv în rețelele solare bazate pe IoT. Analiza oferă o bază pentru îmbunătățiri viitoare, inclusiv

mecanisme sigure de pornire, verificarea integrității și procese automate de actualizare, consolidând cadrul mai larg de securitate cibernetică stabilit în această cercetare.

Constatările din acest capitol pregătesc terenul pentru dezvoltarea de contramăsuri specifice și de îmbunătățiri ale securității în capitolele următoare. Prin abordarea vulnerabilităților identificate și integrarea tehnologiilor avansate de securitate, sistemul poate fi mai bine protejat împotriva amenințărilor cibernetice în continuă evoluție. Rezultatele acestui capitol au fost publicate în [49].

Prin aplicarea unor metodologii structurate de modelare a amenințărilor, acest capitol contribuie în mod direct la atingerea obiectivului O2 (Realizarea unei modelări a amenințărilor pentru dezvoltarea unui sistem fotovoltaic solar inteligent bazat pe IoT). Rezultatele acestei analize pun bazele măsurilor de securitate dezvoltate în capitolul 4.

4. Dezvoltarea unui sistem de monitorizare securizat pentru rețele de energie solară bazate pe IoT

Capitolul 4 se bazează pe modelarea amenințărilor la adresa securității cibernetice și pe evaluarea riscurilor efectuate în capitolul 3, care a identificat vulnerabilități critice în sistemele inteligente de energie solară bazate pe IoT, cum ar fi falsificarea datelor, spoofing, denunțarea serviciului și divulgarea informațiilor. Acest capitol trece de la analiza amenințărilor la implementarea practică, concentrându-se pe proiectarea și implementarea unui sistem de monitorizare securizat pentru a aborda aceste vulnerabilități. Sistemul integrează tehnici avansate de criptare, protocoale de comunicare securizate și monitorizare bazată pe cloud pentru a spori reziliența rețelelor de energie solară bazate pe IoT împotriva amenințărilor cibernetice.

Sistemul de monitorizare securizat abordează trei provocări cheie: asigurarea integrității și confidențialității datelor prin intermediul Standardului avansat de criptare (AES), permiterea monitorizării securizate de la distanță utilizând HTTPS și platforma SystemLink Cloud și asigurarea scalabilității și flexibilității prin utilizarea nodului IoT myRIO-1900, programarea labview și software-ul G Web Development Software pentru crearea de interfețe web ușor de utilizat.

4.1. Arhitectură și proiectare sistemului

Arhitectura sistemului integrează o instalație fotovoltaică echipată cu senzori pentru a colecta date precum tensiunea și temperatura. Datele sunt transmise prin Wi-Fi de la nodul IoT myRIO-1900 la un computer local care acționează ca gateway IoT. Pentru monitorizarea de la distanță, sistemul utilizează SystemLink Cloud, care permite accesarea datelor în siguranță din orice locație. Inițial, sistemul a fost vulnerabil la atacurile Man-in-the-Middle (MitM), după cum a demonstrat interceptarea datelor necriptate prin intermediul testelor de securitate. Această vulnerabilitate a fost atenuată prin implementarea criptării AES pentru transmiterea datelor și HTTPS pentru comunicarea securizată cu cloud-ul.

Arhitectura sistemului securizat de monitorizare a energiei solare bazat pe IoT este ilustrată în figura 4, care prezintă integrarea configurației fotovoltaice, a senzorilor, a plăcii myRIO-1900, a gateway-ului IoT și a SystemLink, platforma IoT Cloud. Această concepție asigură transmiterea fără întreruperi a datelor și accesul securizat de la distanță, permițând în același timp scalabilitatea și adaptabilitatea la diferite configurații.

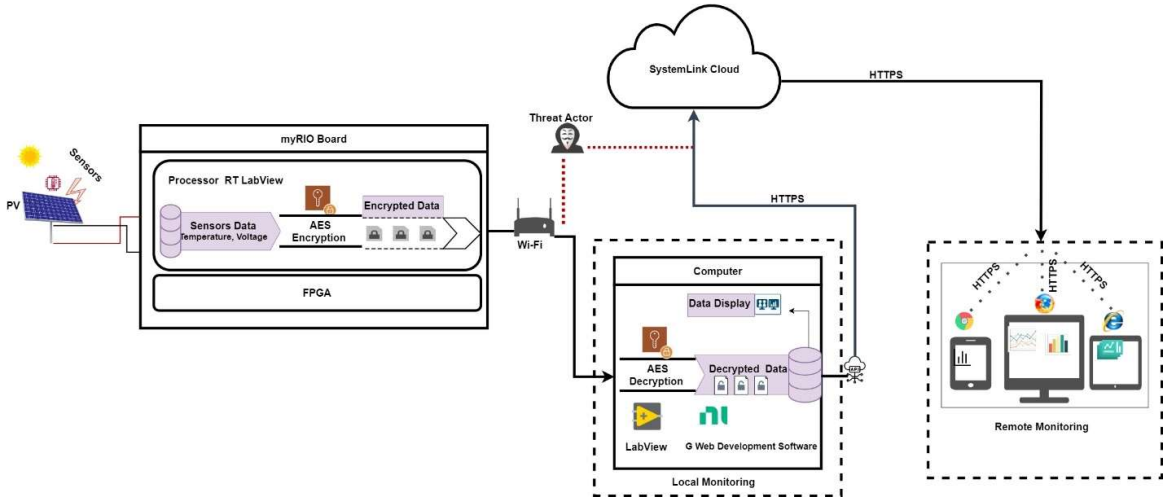

Figura 4. Arhitectura sistemului securizat de monitorizare a energiei solare bazat pe IoT.

4.2. Implementarea unui sistem securizat de monitorizare a energiei solare bazat pe IoT

Implementarea sistemului implică mai multe componente și tehnologii cheie. Placa myRIO- 1900, un microcontroler flexibil, servește drept nod IoT pentru achiziția și procesarea datelor în timp real. Procesorul său dual-core ARM Cortex-A9 și FPGA permit gestionarea eficientă a sarcinilor complexe, în timp ce capacitățile sale Wi-Fi integrate facilitează comunicarea wireless cu gateway-ul IoT.

Platforma SystemLink Cloud este utilizată pentru vizualizarea datelor în timp real și monitorizarea la distanță. Figura 5 ilustrează fluxul de lucru pentru transmiterea datelor și integrarea cu SystemLink Cloud, prezentând procesul de autentificare, transmiterea datelor și etapele de verificare. Această platformă oferă o soluție centralizată și rentabilă pentru gestionarea și monitorizarea sistemului de energie solară din orice locație.

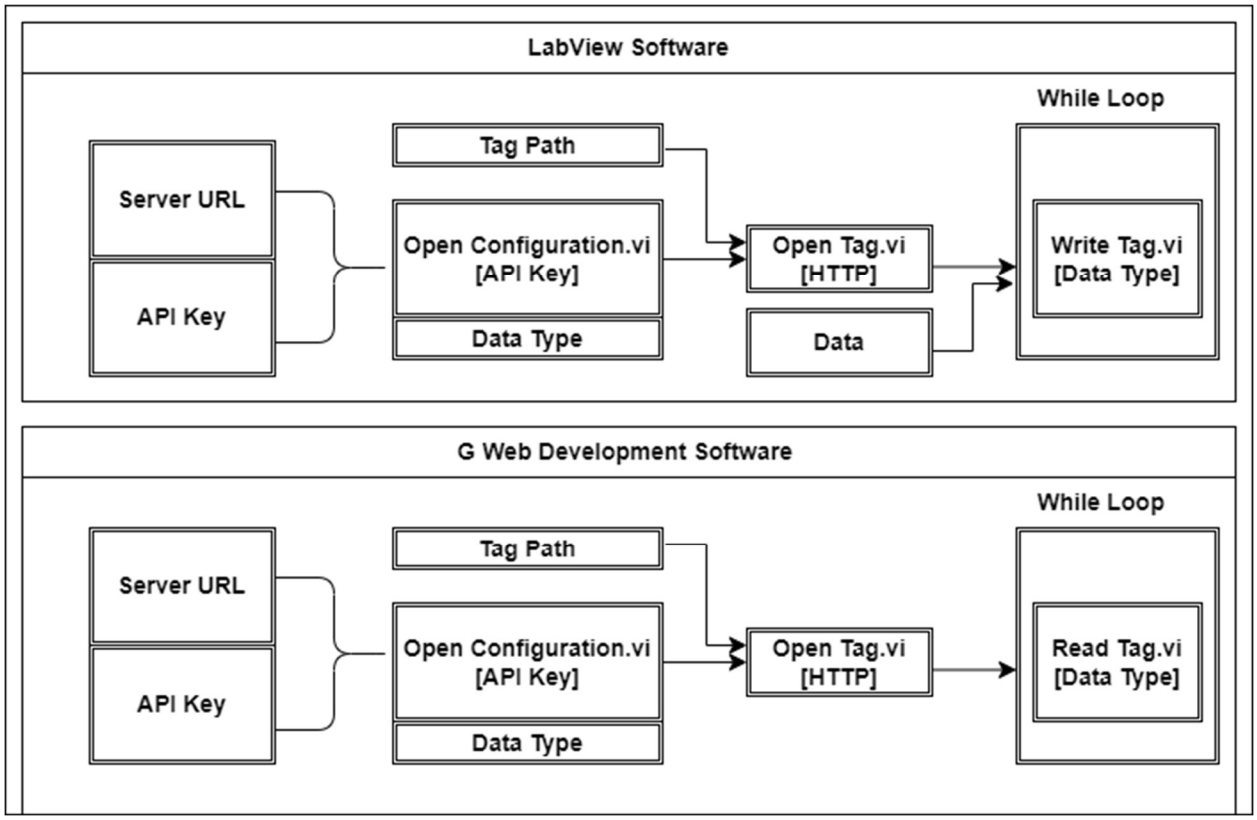

Figura 5. Conectivitatea SystemLink Cloud.

Standardul avansat de criptare (AES) a fost implementat în programul LabVIEW pentru a cripta datele senzorilor în timpul transmisiei, asigurând integritatea și confidențialitatea datelor. Procesul de decriptare la gateway-ul IoT a fost efectuat, demonstrând modul în care datele criptate sunt readuse la formatul lor original de text clar. Figura 6 prezintă reprezentarea pseudocodului AES. Aceasta arată toate etapele de criptare și decriptare AES.

```
function AES_Encrypt(plaintext, key):
    round_keys = KeyExpansion(key)
    state = AddRoundKey(plaintext, round_keys[0])

    for round in 1 to Nr-1:
        state = SubBytes(state)
        state = ShiftRows(state)
        state = MixColumns(state)
        state = AddRoundKey(state, round_keys[round])

    state = SubBytes(state)
    state = ShiftRows(state)
    state = AddRoundKey(state, round_keys[Nr])

    return state

function AES_Decrypt(ciphertext, key):
    round_keys = KeyExpansion(key)
    state = AddRoundKey(ciphertext, round_keys[Nr])

    for round in (Nr-1) down to 1:
        state = InvShiftRows(state)
        state = InvSubBytes(state)
        state = AddRoundKey(state, round_keys[round])
        state = InvMixColumns(state)

    state = InvShiftRows(state)
    state = InvSubBytes(state)
    state = AddRoundKey(state, round_keys[0])

    return state
```

Figura 6. Pseudocodul standardului avansat de criptare.

4.3. Rezultate și Discuții

Au fost efectuate experimente simulând atacuri cibernetice reale pentru a evalua eficacitatea sistemului de monitorizare securizat dezvoltat pentru rețelele de energie solară bazate pe IoT. Testele inițiale cu ajutorul Wireshark au arătat că, înainte de criptare, parametrii datelor fotovoltaice, cum ar fi tensiunea și temperatura, au fost transmise în text clar prin Wi-Fi. Acest lucru a expus sistemul la mai multe riscuri de securitate, inclusiv ascultare, manipularea datelor, control neautorizat și atacuri de reluare. AES cu o cheie de 256 de biți a fost implementat în mediul de programare LabVIEW al sistemului pentru a cripta datele senzorilor înainte de transmitere. Datele criptate au fost decriptate utilizând aceeași cheie simetrică la gateway-ul de teren IoT. Procesul confirmă integritatea și confidențialitatea procesului de comunicare. Alte teste de securitate au confirmat că datele transmise au fost complet criptate și nu au putut fi citite de utilizatori neautorizați.

În plus, au fost implementate capabilități de monitorizare de la distanță utilizând platforma SystemLink Cloud, permițând accesul în timp real la datele sistemului fotovoltaic printr-o conexiune securizată HTTPS. Inspecția traficului a confirmat utilizarea TLS 1.2 în timpul comunicării de la browser la cloud, asigurând criptarea și confidențialitatea de la un capăt la altul. Rezultatele experimentale validează faptul că mecanismele de criptare și transmisie securizată aplicate atenuează în mod eficient multiplele amenințări cibernetice identificate în modelarea anterioară a amenințărilor. Integrarea tehnicilor puternice criptografice , protocoalelor sigure, și monitorizării bazate

pe cloud demonstrează o abordare practică și scalabilă pentru îmbunătățirea securității cibernetice a sistemelor de energie regenerabilă bazate pe IoT.

4.4. Concluzie

În capitolul 4, se face tranziția de la analiza amenințărilor prezentată în capitolul 3 la implementarea practică a unui sistem de monitorizare securizat, adaptat pentru a aborda amenințările identificate în sistemele inteligente de energie fotovoltaică. Acest capitol aduce contribuții semnificative la securitatea cibernetică a IoT prin demonstrarea modului în care tehnicile avansate de criptare, protocoalele de comunicare securizate și monitorizarea bazată pe cloud pot fi integrate pentru a spori fiabilitatea și securitatea sistemelor de energie regenerabilă.

Principalele contribuții:

1. Abordarea amenințărilor identificate din capitolul 3:
    - Implementarea criptării AES: Pentru a atenua falsificarea și divulgarea informațiilor, sistemul criptează datele senzorilor înainte de transmitere, asigurând integritatea și confidențialitatea datelor.
    - Utilizarea protocolului HTTPS: Pentru a proteja împotriva falsificării și accesului neautorizat, sistemul utilizează HTTPS pentru comunicarea securizată între utilizatorii de la distanță și platforma cloud.
    - Îmbunătățirea monitorizării la distanță prin utilizarea SystemLink Cloud: Îmbunătățește monitorizarea de la distanță menținând în același timp securitatea, oferind o interfață securizată, bazată pe web, pentru vizualizarea datelor în timp real.
2. Arhitectura sistemului:
    - Arhitectura sistemului s-a concentrat pe asigurarea scalabilității, flexibilității și adaptabilității la configurații și senzori sau dispozitive suplimentare. Implementarea unei arhitecturi de sistem centrată pe placa myRIO-1900. MyRIO acționează ca nod IoT pentru procesarea în timp real și achiziția de date de la senzori.
    - În ceea ce privește soluțiile software, LabVIEW a fost utilizat pentru achiziția de date, criptare și decriptare, asigurând integrarea fără probleme a măsurilor de securitate. G Software de dezvoltare web: Acest software permite crearea unei interfețe web ușor de utilizat pentru monitorizarea de la distanță, găzduită pe SystemLink Cloud.
    - Această arhitectură asigură siguranță, scalabilitate, flexibilitate și adaptabilitate la configurații și senzori sau dispozitive suplimentare.
3. Implementarea standardului avansat de criptare (AES-256):
    - O securitate criptografică de nivel înalt este obținută prin implementarea standardului avansat de criptare (AES-256) între nodul IoT și gateway-ul IoT. Acest lucru asigură

rezistența la accesul neautorizat și la atacurile de manipulare

4. Simularea testelor de securitate:
    - Transmiterea datelor: Inițial vulnerabil la atacurile MitM, ceea ce duce la interceptarea și expunerea datelor sensibile.
    - Transmiterea criptată a datelor: După implementarea criptării AES-256, datele transmise prin Wi-Fi au fost complet criptate, ceea ce le face ilizibile pentru actorii amenințători.
    - Validarea protocoalelor de criptare și de comunicare securizată a confirmat eficacitatea acestora în abordarea riscurilor descrise în capitolul 3.
5. Implementarea unei interfețe de monitorizare la distanță și de utilizare bazată pe web cu SystemLink Cloud:
    - Sistemul facilitează monitorizarea de la distanță a sistemului fotovoltaic, oferind operatorilor acces în timp real la datele parametrilor fotovoltaici, inclusiv temperatura și tensiunea.
    - Utilizează HTTPS pentru a asigura comunicații sigure între utilizatorii de la distanță și platforma cloud, protejând împotriva ascultării și accesului neautorizat.
    - Interfața web, dezvoltată cu ajutorul software-ului G Web Development, oferă interfață ușor de utilizat pentru vizualizarea performanței sistemului, îmbunătățind accesibilitatea și ușurința în utilizare.

Constatările și contribuțiile din acest capitol pun bazele unor cercetări ulterioare privind îmbunătățirea securității cibernetice a sistemelor de energie solară bazate pe IoT. Rezultatele acestui capitol au fost publicate în [50]

Prin implementarea unui sistem de monitorizare sigur și inteligent, acest capitol contribuie în mod direct la atingerea obiectivului O3 (proiectarea și implementarea unui sistem de monitorizare sigur și inteligent pentru rețelele de energie solară bazate pe IoT). În plus, prin validarea experimentală a mecanismelor de securitate implementate, acest capitol sprijină obiectivul O5. Constatările din acest capitol constituie baza pentru îmbunătățirile de securitate discutate în capitolul 5.

5. Soluții de monitorizare și securitate bazate pe cloud pentru sistemele de energie solară bazate pe IoT

Capitolul 5 prezintă proiectarea și integrarea unui sistem de monitorizare sigur, bazat pe cloud, pentru rețelele de energie solară bazate pe IoT. Bazându-se pe cadrul de modelare a amenințărilor stabilit în capitolul 3 și pe măsurile de securitate implementate în capitolul 4, acest capitol face legătura între modelarea teoretică și aplicarea practică. Metodologia de cercetare a implicat integrarea serviciilor cloud Microsoft Azure - Azure IoT Hub, Stream Analytics, Power BI și Time Series Insights - într-un prototip funcțional. Acest lucru a permis achiziția de date în timp real, comunicarea securizată, monitorizarea de la distanță și analizele avansate pentru sistemele fotovoltaice.

Implementarea a utilizat LabVIEW pentru programarea sistemului de achiziție de date în timp real, conectat la senzori prin intermediul unui nodul IoT myRIO. Datele au fost transmise în siguranță de la nodul IoT la gateway-ul de teren IoT utilizând Advanced Encryption Standard și de la dispozitivele IoT la cloud-ul Azure utilizând Transport Layer Security (TLS) 1.2. Pentru a atenua amenințările de spoofing și de acces neautorizat, sistemul a impus autentificarea dispozitivelor prin Azure IoT Hub, token-uri SAS (Shared Access Signature) și controlul accesului pe bază de rol (RBAC). Stream Analytics și Power BI au fost utilizate pentru filtrarea, prelucrarea și vizualizarea datelor de telemetrie, în timp ce Time Series Insights a fost utilizat pentru stocarea la scară largă și analiza seriilor de timp, utilizând atât stocarea la cald, cât și la rece pentru păstrarea datelor la un cost eficient și scalabil. Figura 7 ilustrează programul LabVIEW pentru achiziția de date și integrarea cu Azure IoT Hub, arătând modul în care datele senzorilor sunt prelucrate și transmise în siguranță către cloud.

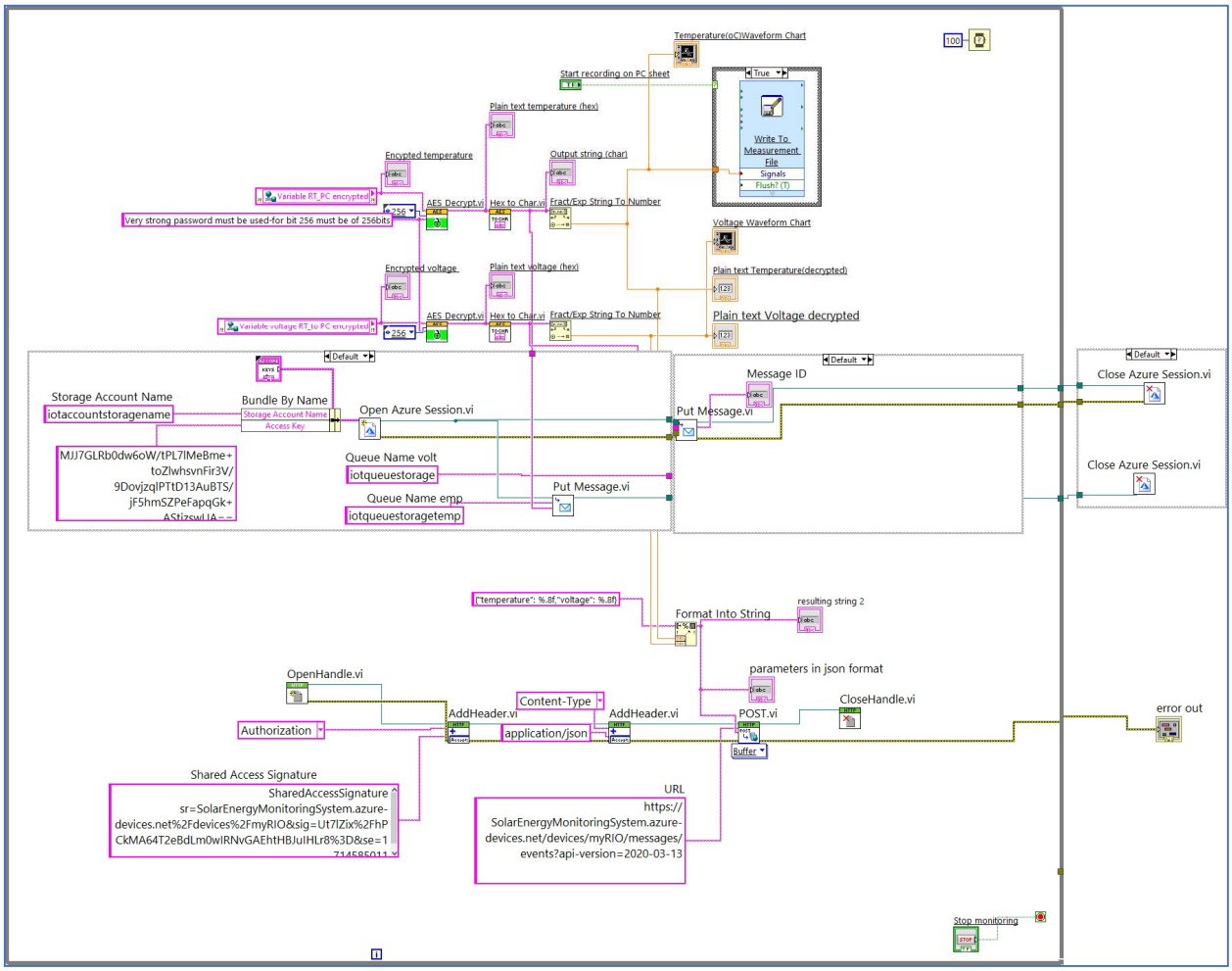

Figura 7. Program LabVIEW pentru achiziția de date și integrarea cu Azure IoT Hub.

Experimentele au demonstrat capacitatea sistemului de monitorizare în timp real și de detectare a anomaliilor. Indicatorii cheie de telemetrie, cum ar fi tensiunea și temperatura, au fost vizualizați și analizați în tablourile de bord Cloud. Metrici precum numărul de mesaje trimise, utilizarea cotelor și tendințele conectivității dispozitivelor au confirmat scalabilitatea și performanța sistemului. Combinația dintre analiza în timp real (prin Power BI) și analiza tendințelor istorice (prin Time Series Insights) facilitează luarea deciziilor proactive și optimizarea sistemului pe termen lung.

Capitolul concluzionează că integrarea în cloud îmbunătățește semnificativ scalabilitatea, disponibilitatea și securitatea rețelelor de energie solară bazate pe IoT. Arhitectura propusă a abordat cu succes amenințările, inclusiv spoofing, divulgarea informațiilor, falsificarea și ridicarea privilegiilor. Această contribuție oferă un cadru robust și real pentru monitorizarea sigură bazată pe cloud în aplicațiile de energie regenerabilă

Contribuții la cercetare pentru capitolul 5:

1. Integrare în cloud pentru sistemele de energie solară bazate pe IoT:

- Integrarea cu succes a Azure Stream Analytics, Azure IoT Hub, Power BI și Time Series Insights pentru a crea un sistem de monitorizare scalabil și eficient bazat pe cloud pentru rețelele de

energie solară.

- A permis procesarea, vizualizarea și analizarea datelor în timp real, oferind informații utile pentru optimizarea sistemului și luarea deciziilor.

2. Mecanisme avansate de securitate:

- Implementarea Transport Layer Security (TLS) pentru a garanta că transmiterea datelor între gateway-ul de teren IoT și platforma cloud rămâne criptată și securizată, reducând astfel probabilitatea de falsificare și acces neautorizat la informații.
- Conceperea și implementarea mecanismelor de autentificare și autorizare a dispozitivelor, inclusiv SharedAcces partajat Signature (SAS) token-uri și RBAC, pentru a preveni atacurile de tip spoofing și elevation of privilege.

3. Scalabilitate și reziliență:

- S-a proiectat un sistem capabil să se adapteze la complexitatea în creștere a rețelelor de energie solară bazate pe IoT, asigurând disponibilitate ridicată și fiabilitate prin backup-uri în timp real și soluții de stocare redundante.
- Sistemul a fost consolidat împotriva atacurilor cibernetice prin includerea mai multor niveluri de securitate, cum ar fi autentificarea, controlul accesului și criptarea.

Acest capitol contribuie la obiectivul O3 (Proiectarea și implementarea unui sistem de monitorizare inteligent, sigur și securizat pentru rețelele de energie solară bazate pe IoT).

6. Dezvoltarea monitorizării, detectării și răspunsului proactiv la amenințări: Integrarea SIEM și a securității OT în sisteme de energie solară bazate pe IoT

6.1. Arhitectură de securitate pentru monitorizarea integrată a amenințărilor cibernetice IT-OT

Acest capitol prezintă o arhitectură unificată de securitate cibernetică adaptată pentru sistemele de energie solară bazate pe IoT, cu scopul de a aborda amenințările complexe care rezultă din integrarea mediilor IT și OT. Cadrul propus permite monitorizarea centralizată, detectarea în timp real și răspunsul automat prin combinarea capacităților SIEM [51] pentru IT cu soluția de monitorizare OT fără agent.

Așa cum este ilustrat în figura 8, arhitectura asigură o coordonare perfectă între straturile IT și OT, susținută de tehnologii precum învățarea automată, analiza comportamentală și fluxurile de informații privind amenințările. Aceste componente lucrează împreună pentru a detecta anomalii, a corela evenimente între domenii și a declanșa răspunsuri automate prin intermediul unor programe predefinite. Această arhitectură consolidează poziția de securitate a sistemelor solare inteligente, oferind o abordare flexibilă, inteligentă și proactivă a monitorizării amenințărilor și a răspunsului în medii convergente.

Caracteristicile cheie includ:

- Monitorizare unificată și detectarea amenințărilor
- Integrarea informațiilor privind amenințările
- Descoperirea cuprinzătoare a activelor
- Corelarea evenimentelor și detectarea anomaliilor în rețelele IT și OT
- Răspuns automatizat la incidente
- Scalabilitate și adaptabilitate
- Gestionarea vulnerabilității

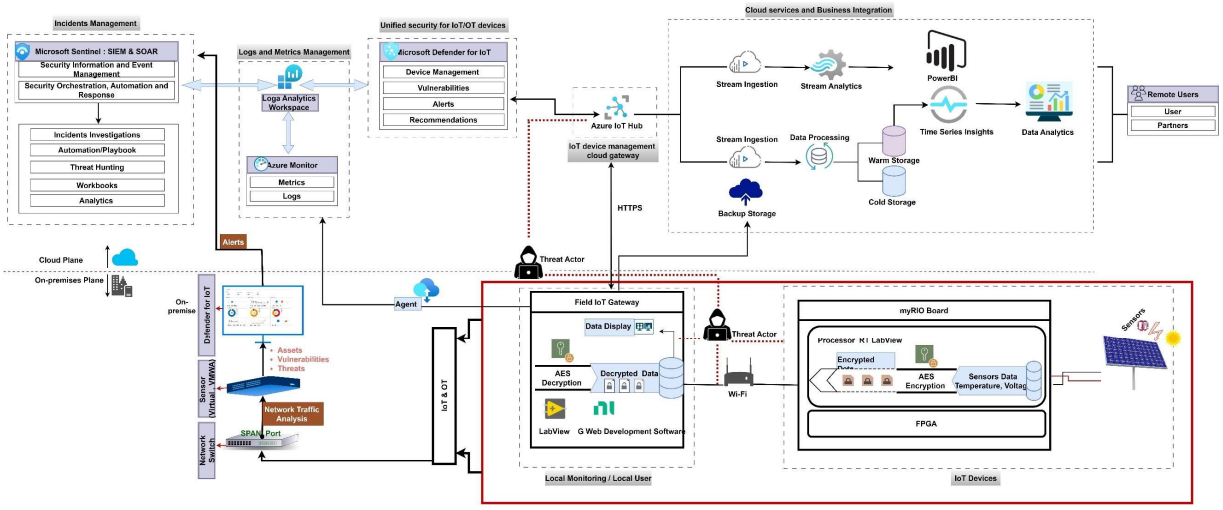

Figura 8. Arhitectură de securitate pentru monitorizarea proactivă și detectarea unificată a amenințărilor IT/OT în sistemele de energie solară bazate pe IoT.

6.2. Integrarea monitorizării securității IT și OT pentru monitorizarea unificată a amenințărilor, detectarea și gestionarea incidentelor

Această secțiune se concentrează pe convergența monitorizării securității IT și OT într-o singură platformă unificată pentru a spori vizibilitatea, corelarea amenințărilor și răspunsul la incidente în cadrul sistemului de energie solară bazat pe IoT. Cu jurnalele de securitate IT și sistemul de monitorizare a securității IoT/OT deja implementate, integrarea în platforma SIEM centralizată a permis detectarea holistică a amenințărilor în ambele domenii.

SIEM este utilizat drept nucleu pentru agregarea alertelor de la serviciile cloud, punctele finale, dispozitivele de rețea și activele industriale. În timp ce SIEM-urile tradiționale preluau deja jurnalele IT care acopereau autentificarea, detectarea programelor malware și activitățile din cloud, amenințările industriale nu erau monitorizate anterior. Pentru a elimina acest decalaj, alertele de la soluțiile de securitate IoT/OT au fost transmise către SIEM, permițând corelarea anomaliilor OT (de exemplu, atacuri spefice PLC, utilizarea abuzivă a protocolului) cu vectorii de atac IT (de exemplu, conturile de utilizator compromise).

Un beneficiu al acestei integrări a fost detectarea atacurilor cibernetice-fizice care vizează ambele medii. De exemplu, o stație de lucru compromisă a unui operator IT legată de activitatea suspectă a unui controler OT ar putea fi identificată și investigată rapid. Mai mult, sistemul a fost utilizat pentru detectarea avansată a amenințărilor și pentru investigații criminalistice, oferind o analiză structurată pe interdomenii.

Regulile de detecție personalizate din cadrul SIEM au permis corelarea incidentelor IT și OT, în timp ce fluxurile de informații despre amenințări au asigurat semnalarea în timp real a comunicațiilor dispozitivelor IoT și OT cu IP-uri malițioase.

Această abordare unificată a avut ca rezultat o vizibilitate unică a amenințărilor IT și OT, asigurând

detectarea, investigarea și răspunsul raționalizate. Figura 9 ilustrează capacitățile unificate de monitorizare proactivă a amenințărilor, detectare și gestionare a incidentelor. În ansamblu, această integrare a eliminat un decalaj critic între operațiunile de securitate IT și OT, oferind un cadru de apărare proactiv capabil să identifice, să coreleze și să răspundă la amenințări care acoperă întreaga infrastructură energetică fotovoltaică solară inteligentă.

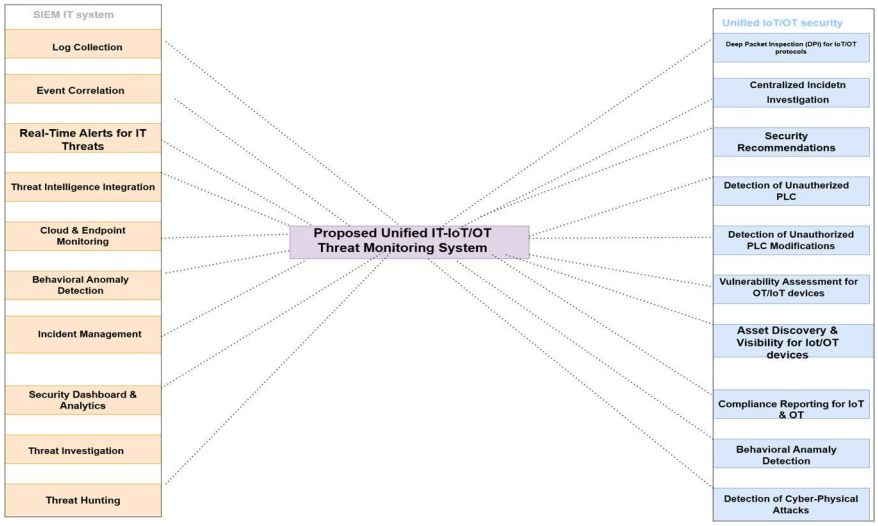

Figura 9. Funcționalități unificate de monitorizare proactivă a amenințărilor, de detectare și de gestionare a incidentelor.

6.3. Validarea și evaluarea securității sistemului integrat de monitorizare a amenințărilor IT-OT

În urma implementării sistemului integrat de monitorizare a amenințărilor IT-OT, a fost efectuată o validare cuprinzătoare pentru a evalua eficacitatea acestuia în detectarea amenințărilor în timp real, corelarea incidentelor și analiza interdomeniilor. Capacitățile sistemului au fost evaluate atât prin monitorizarea în timp real a evenimentelor de securitate, cât și prin testarea cu scenarii reale de atac ICS și IT care conțin elemente industriale și IT. Acest lucru a permis extinderea sistemului prin testarea acestuia pe sisteme complexe.

Procesul de validare a demonstrat că sistemul poate detecta și corela cu succes amenințările care acoperă rețelele IT tradiționale și OT industriale. Jurnalele de la punctele finale, autentificările utilizatorilor, resursele cloud și traficul din rețeaua industrială au fost colectate și analizate într-o platformă SIEM unificată, permițând o vizibilitate completă a securității.

Sistemul a valorificat atât detecția bazată pe jurnale (din mediile IT), cât și monitorizarea pasivă a traficului (din rețelele OT) pentru a asigura o monitorizare robustă, în timp real, și răspunsul la incidente. Analizele comportamentale, regulile de detecție personalizate și fluxurile de informații privind amenințările au fost utilizate pentru a semnala activitățile anormale și modelele de atac cunoscute.

Principalele scenarii de atac detectate cu succes în timpul validării au inclus:

- Brute Force Attacks - Autentificările repetate eșuate de la IP-uri neautorizate au fost

detectate cu ajutorul regulilor de corelare SIEM și investigate

- Port Scanning & Reconnaissance - Senzorul de monitorizare OT a semnalat încercările rău intenționate de a sonda porturile și serviciile rețelei industriale.
- Activitate de phishing - Detectată prin crearea de reguli suspecte pentru căsuța de primire și indicatori de domeniu legați de campanii de phishing cunoscute și investigate
- Detectarea programelor malware - Identificate prin anomalii comportamentale și indicatori de compromitere (IoC) cunoscuți din surse de informații despre amenințări.
- Triton Malware Detection - Detectarea critică a comunicațiilor PLC neautorizate caracteristice malware-ului Triton/Trisis.
- Deconectarea PLC sau schimbarea modului de operare - Semnalizate ca alerte majore, semnalând un potențial sabotaj sau o configurație greșită.
- Amenințări din interior - Au fost identificate tentative de acces la distanță (de exemplu, sesiuni SSH) și modele de deplasare laterală
- Desfășurarea de resurse/dispozitive rău intenționate - Aprovizionarea neautorizată și activitatea de la noi dispozitive sau VM-uri au fost înregistrate și investigate.
- Conexiuni neautorizate ale dispozitivelor - Descoperite prin inventarul dinamic al activelor IoT/OT și analiza abaterilor de referință.
- Dispozitive vulnerabile - Dispozitivele cu servicii învechite sau expuse au fost marcate automat pentru reducerea riscurilor.

Cadrul de monitorizare integrat a îmbunătățit semnificativ acuratețea detectării amenințărilor și timpii de răspuns la incidente, comparativ cu SIEM-urile tradiționale. Acesta a permis analiza centralizată, pe mai multe niveluri și investigarea în timp real, sprijinind atât căutarea proactivă a amenințărilor, cât și fluxurile de lucru eficiente de răspuns.

Validarea folosind seturi reale de date ICS a confirmat aplicabilitatea practică a sistemului în medii industriale, în timp ce configurațiile conectate la cloud au extins în continuare scalabilitatea și capacitățile de partajare a informațiilor.

Contribuții ale capitolului:

1. Cadru de securitate unificat:

- Capitolul prezintă un cadru de securitate unificat care integrează monitorizarea securității IT și OT, oferind o viziune holistică a sistemului de energie solară bazat pe IoT. Această integrare asigură faptul că amenințările care provin dintr-un strat IT al unui domeniu nu se propagă nedetectate în straturile OT nedetectate, îmbunătățind astfel postura generală de securitate.

2. Detectarea și răspunsul îmbunătățit la amenințări:

- Soluția propusă îmbunătățește semnificativ capacitățile de detectare a amenințărilor prin

combinarea monitorizării bazate pe jurnale SIEM cu analiza pasivă a traficului de rețea Microsoft Defender for IoT. Această abordare dublă detectează amenințările sofisticate, inclusiv atacurile prin forță brută, tentativele de phishing, intruziunile malware (de exemplu, Triton) și scanarea neautorizată a porturilor. De asemenea, sistemul reduce timpul mediu de detectare (MTTD) și timpul mediu de răspuns (MTTR), permițând un răspuns mai rapid și mai eficient la incidente.

3. Monitorizare în timp real și analiză comportamentală:

- Capitolul demonstrează eficiența monitorizării în timp real și a analizei comportamentale în identificarea anomaliilor și a abaterilor de la tiparele operaționale standard. Prin învățarea continuă a comportamentului normal al rețelei, sistemul poate detecta amenințări de tip zero-day și adversari discreți pe care metodele tradiționale de detectare bazate pe semnături le-ar putea rata.

4. Validarea cu date din lumea reală:

- Eficacitatea sistemului este validată utilizând seturi de date reale ICS PCAP, demonstrând capacitatea acestuia de a detecta și de a răspunde la amenințări sofisticate în scenarii reale. Această validare asigură că soluția propusă este solidă din punct de vedere teoretic și aplicabilă în practică în mediile industriale.

5. Descoperirea automată a activelor și gestionarea vulnerabilităților:

- Capitolul evidențiază capacitatea sistemului de a descoperi automat și de a inventaria activele OT, oferind vizibilitate continuă în rețea. Această caracteristică este esențială pentru identificarea dispozitivelor neautorizate, a configurațiilor greșite și a vulnerabilităților potențiale, permițând reducerea proactivă a riscurilor.

6. Integrare cu SIEM bazat pe cloud:

- Integrarea monitorizării securității OT cu o platformă SIEM bazată pe cloud sporește scalabilitatea și adaptabilitatea sistemului. Această integrare permite gestionarea centralizată a incidentelor de securitate, analiza avansată și corelarea evenimentelor de securitate IT și OT, oferind o imagine mai cuprinzătoare a peisajului amenințărilor.

7. Mecanisme proactive de apărare:

- Soluția propusă pune accentul pe mecanismele de apărare proactive, cum ar fi răspunsul automat la incidente, vânătoarea de amenințări și integrarea fluxurilor de informații despre amenințări. Aceste mecanisme asigură faptul că echipele de securitate pot detecta și răspunde la amenințări înainte ca acestea să se transforme în incidente la scară largă.

Prin implementarea unui cadru proactiv de securitate cibernetică, acest capitol a abordat obiectivul O4 (Dezvoltarea unui cadru unificat proactiv de monitorizare, detectare și gestionare a incidentelor de securitate cibernetică prin integrarea soluțiilor de securitate SIEM și OT). În plus, prin validarea în lumea reală cu ajutorul sistemului de control industrial (ICS) și al datelor IT, acest capitol contribuie, de asemenea,

la obiectivul O5 (evaluarea și validarea eficacității cadrului de securitate propus cu ajutorul datelor din lumea reală).

7. Concluzii finale

7.1. Concluzii

Această cercetare doctorală a fost efectuată pentru a analiza provocările de securitate cibernetică și a dezvolta soluții de securitate robuste pentru rețelele inteligente de energie solară bazate pe IoT. Pe măsură ce IoT, integrarea în cloud și monitorizarea în timp real devin fundamentale pentru sistemele moderne de energie regenerabilă, acestea introduc vulnerabilități semnificative de securitate cibernetică care prezintă riscuri pentru fiabilitatea sistemului, integritatea datelor și securitatea operațională. Abordarea acestor provocări necesită mecanisme de securitate proactive pentru a asigura confidențialitatea, integritatea și disponibilitatea (CIA) infrastructurilor energetice.

Cercetarea a fost structurată pentru a atinge cinci obiective-cheie:

- O1. Să analizeze amenințările și vulnerabilitățile la adresa securității cibernetice în sistemele inteligente de energie solară bazate pe IoT.
- O2. Realizarea modelării amenințărilor pentru dezvoltarea unui sistem solar fotovoltaic inteligent bazat pe IoT Sistem solar fotovoltaic inteligent bazat pe IoT
- O3. Proiectarea și implementarea unui sistem de monitorizare inteligent și securizat pentru rețelele de energie solară bazate pe IoT.
- O4. Dezvoltarea unui cadru unificat și proactiv de monitorizare, detectare și gestionare a incidentelor de securitate cibernetică prin integrarea soluțiilor de securitate SIEM și OT.
- O5. Evaluarea și validarea eficacității cadrului de securitate propus utilizând date din lumea reală.

Prin investigație teoretică, implementare practică și evaluare experimentală, această cercetare oferă o abordare cuprinzătoare a securității cibernetice care îmbunătățește comunicarea sigură, criptarea avansată, autentificarea dispozitivelor, autorizarea, controlul accesului, detectarea amenințărilor în timp real, apărarea cibernetică proactivă și mecanismele de răspuns la incidente în rețelele inteligente de energie solară bazate pe IoT. Integrarea monitorizării securității IT bazate pe SIEM și a monitorizării centralizate a securității OT asigură o arhitectură de securitate cibernetică unificată, permițând detectarea anomaliilor în timp real, corelarea evenimentelor de securitate și răspunsul automat la incidente pentru a proteja infrastructurile energetice critice de amenințările cibernetice.

În cele ce urmează se prezintă un rezumat al modului în care a fost atins fiecare obiectiv de cercetare, subliniindu-se contribuțiile aduse domeniului securității cibernetice pentru sistemele de energie regenerabilă bazate pe IoT.

O1: Analiza amenințărilor la adresa securității cibernetice și a vulnerabilităților în sistemele de energie solară bazate pe IoT

Pentru a atinge obiectivul O1, această cercetare a efectuat o analiză cuprinzătoare a amenințărilor la adresa securității cibernetice și a vulnerabilităților care afectează sistemele inteligente de energie solară bazate pe IoT. Investigația s-a concentrat pe înțelegerea motivației din spatele atacurilor

cibernetice, identificarea vectorilor de atac, analiza modelelor de atac cibernetic și evaluarea amenințărilor la adresa securității cibernetice, a vulnerabilităților și a contramăsurilor existente. Acest obiectiv a fost abordat în principal în capitolele 2 și 3:

A. Analiza amenințărilor la adresa securității cibernetice și a vulnerabilității (capitolul 2):

Capitolul 2 a oferit o examinare aprofundată a riscurilor de securitate cibernetică în sistemele inteligente de energie solară bazate pe IoT, acoperind multiple aspecte pentru a construi o bază solidă pentru soluțiile de securitate din capitolele următoare.

Unul dintre primele aspecte analizate a fost motivația din spatele atacurilor cibernetice asupra rețelelor de energie solară bazate pe IoT. Atacatorii vizează aceste sisteme din diverse motive, inclusiv câștiguri financiare prin atacuri ransomware, întreruperea aprovizionării cu energie ca parte a războiului cibernetic și spionajului care vizează accesul la date critice privind producția de energie. În unele cazuri, atacatorii exploatează vulnerabilitățile din sistemele energetice bazate pe IoT pentru a recruta dispozitive în botnet-uri, lansând atacuri cibernetice la scară largă asupra altor ținte. Dependența tot mai mare de monitorizarea și automatizarea de la distanță în rețelele inteligente de energie solară extinde și mai mult aria de atac, făcând aceste sisteme atractive pentru infractorii cibernetici.

În continuare, studiul a identificat principalii vectori de atac cibernetic exploatați de adversari. Mecanismele de autentificare slabe permit adesea accesul neautorizat la dispozitivele IoT, ducând la manipularea datelor sau la preluarea controlului asupra sistemului. Canalele de comunicare nesigure fac ca transmisiile de date să fie vulnerabile la interceptare și falsificare, ceea ce face ca atacurile MITM să constituie o preocupare. Vulnerabilitățile firmware și software "unpatched" oferă atacatorilor un punct de intrare pentru compromiterea dispozitivelor, în timp ce configurațiile greșite ale cloud-ului expun datele sensibile ale sistemului. În plus, amenințările la adresa securității fizice, cum ar fi manipularea hardware, pot compromite integritatea sistemelor IoT implementate. Pentru a evalua sistematic aceste riscuri de securitate, cercetarea a aplicat modele de atacuri cibernetice care clasifică și analizează amenințările cibernetice în rețelele solare inteligente bazate pe IoT. Modelul Cyber Kill Chain (CKC) a fost utilizat pentru a cartografia etapele unui atac, de la recunoașterea inițială la exploatarea și persistența sistemului. Aceste modele au asigurat o abordare metodică pentru identificarea și atenuarea riscurilor cibernetice în rețelele de energie solară bazate pe IoT.

Studiul a examinat apoi amenințările și vulnerabilitățile specifice de securitate cibernetică care afectează rețelele solare bazate pe IoT. Atacurile de tip Denial-of-Service (DoS) și Denial-of-Service distribuit (DDoS) au fost considerate unul dintre riscuri, în special din cauza puterii limitate de procesare a dispozitivelor IoT, ceea ce le face vulnerabile la epuizarea resurselor. Atacurile Replay și spoofing au fost identificate ca amenințări care ar putea manipula integritatea datelor în protocoalele de comunicare. Amenințările de tip malware și ransomware reprezintă un risc semnificativ pentru rețelele solare integrate în cloud, putând cripta datele operaționale și solicitând plata unei răscumpărări pentru restaurare. Atacurile bazate pe firmware au reprezentat un alt motiv de

îngrijorare, deoarece actualizările firmware compromise ar putea introduce coduri rău intenționate în sistemele de monitorizare a energiei solare. Studiul a evidențiat, de asemenea, riscul în creștere al botnet-urilor IoT, în care dispozitivele IoT compromise dintr-o rețea energetică inteligentă ar putea fi utilizate pentru a lansa atacuri cibernetice suplimentare.

Cercetarea a analizat în continuare contramăsurile de securitate cibernetică existente care au fost implementate în sistemele de energie regenerabilă bazate pe IoT și a evaluat eficacitatea acestora. Protocoalele de criptare, cum ar fi TLS, sunt utilizate pe scară largă pentru a proteja transmisiile de date, dar deficiențele de implementare lasă adesea vulnerabilități. Soluțiile de autentificare a dispozitivelor și de gestionare a identității îmbunătățesc controlul accesului, însă multe dispozitive IoT nu dispun de mecanisme puternice de autentificare. Sistemele de detectare și prevenire a intruziunilor (IDPS) oferă monitorizare în timp real, însă eficiența lor depinde de detectarea anomaliilor care nu sunt întotdeauna ușor de identificat. Studiul a explorat, de asemenea, tehnologii avansate de securitate, cum ar fi detectarea anomaliilor pe baza învățării automate și mecanismele de securitate blockchain. Algoritmii de învățare automată au fost din ce în ce mai utilizați pentru a detecta anomaliile cibernetice și pentru a prezice modelele de atac, îmbunătățind detectarea proactivă a amenințărilor. Tehnologia blockchain oferă un sistem descentralizat și abordare rezistentă la falsificare pentru securizarea datelor IoT și autentificarea dispozitivelor, oferind un mecanism mai robust pentru a contracara accesul neautorizat și manipularea datelor. Aceste tehnologii emergente au fost evaluate în funcție de rolul lor potențial în consolidarea apărărilor de securitate cibernetică în sistemele de energie solară bazate pe IoT.

Deși cercetările anterioare au adus contribuții semnificative la abordarea amenințărilor la adresa securității cibernetice, acestea se concentrează în principal pe atenuarea atacurilor specifice, cum ar fi programele malware sau accesul neautorizat, vizând vulnerabilitățile dispozitivelor individuale din cadrul sistemului. Această abordare nu oferă o strategie cuprinzătoare de abordare a provocărilor mai ample de securitate cibernetică cu care se confruntă sistemele inteligente de energie regenerabilă bazate pe IoT. În plus, o mare parte din cercetările actuale se concentrează pe sectorul rețelelor inteligente, trecând adesea cu vederea nevoile specifice de securitate cibernetică ale sistemelor de energie regenerabilă, cum ar instalațiile de energie solară, care sunt adoptate din ce în ce mai mult la nivel mondial. Această lacună evidențiază necesitatea unei abordări mai holistice care să integreze securitatea IT și OT, să abordeze provocările unice ale sistemelor de energie solară bazate pe IoT și să ofere protecție de la un capăt la altul împotriva amenințărilor cibernetice în continuă evoluție. Abordarea acestei lacune este esențială pentru a asigura reziliența și fiabilitatea infrastructurilor de energie regenerabilă în fața amenințărilor cibernetice în creștere. Aceste lacune au motivat dezvoltarea unor soluții de securitate mai cuprinzătoare în capitolele următoare, asigurând protecția infrastructurilor inteligente de energie solară bazate pe IoT împotriva amenințărilor cibernetice în continuă evoluție.

O2. Realizarea modelării amenințărilor pentru dezvoltarea unui sistem solar fotovoltaic inteligent bazat pe IoT Sistem solar fotovoltaic inteligent bazat pe IoT

A. Modelarea structurată a amenințărilor și evaluarea riscurilor (capitolul 3)

Pentru a atinge obiectivul O2, această cercetare analizează sistematic și cuantifică riscurile de securitate cibernetică în sistemele inteligente de energie solară bazate pe IoT. Cercetarea a dezvoltat un exemplu de utilizare a sistemului din lumea reală, care a servit drept bază pentru realizarea unei modelări structurate a amenințărilor și a unei evaluări a riscurilor. Cazul de utilizare reprezintă o rețea funcțională de energie solară inteligentă bazată pe IoT, care încorporează dispozitive IoT, gestionarea datelor bazată pe cloud, protocoale de comunicare și capacități de monitorizare de la distanță

Pe baza acestui caz de utilizare, cercetarea a aplicat metodologii structurate de modelare a amenințărilor pentru a clasifica și evalua riscurile de securitate cibernetică. Modelul de amenințare STRIDE a fost utilizat pentru a clasifica sistematic potențialele amenințări care afectează dispozitivele IoT, comunicarea datelor și sistemele de gestionare a energiei integrate în cloud. STRIDE clasifică amenințările în Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service și Elevation of Privilege, permițând o structurată pentru identificarea punctelor slabe de securitate în cadrul cazului de utilizare a sistemului. Pentru a rafina și mai mult analiza riscurilor, a fost aplicat modelul DREAD de evaluare a riscurilor pentru a cuantifica gravitatea amenințărilor identificate. Modelul evaluează riscurile în funcție de potențialul de pagubă, reproductibilitate, exploatabilitate, utilizatori afectați și posibilitate de descoperire, oferind o strategie de prioritizare pentru atenuarea riscurilor de securitate. Prin atribuirea de scoruri fiecărei categorii de amenințări, cercetarea a stabilit o abordare bazată pe riscuri pentru securizarea sistemului de energie solară bazat pe IoT, asigurându-se că cele mai critice amenințări au fost prioritizate pentru atenuare.

În plus față de analiza securității la nivel de sistem, acest capitol examinează vulnerabilitățile de securitate la nivel de dispozitiv prin efectuarea unei evaluări a vulnerabilităților firmware ale dispozitivelor IoT integrate în sistemele de energie solară. Evaluarea controlerului logic programabil (PLC) myRIO-1900 identifică firmware neacoperit, implementări criptografice slabe, mecanisme de actualizare nesigure și vulnerabilități și expuneri comune (CVE) cunoscute public. În plus, au fost identificate dispozitive digitale slabe sau expirate sunt evaluate certificatele și tehnicile insuficiente de întărire a firmware-ului, expunând dispozitivele IoT la infecții malware, modificări neautorizate și amenințări de securitate persistente.

În plus față de analiza de securitate la nivel de sistem, vulnerabilitățile de securitate la nivel de dispozitiv au fost examinate prin efectuarea unei evaluări a vulnerabilităților firmware ale dispozitivelor IoT integrate în sistemele de energie solară. Evaluarea controlerului logic programabil (PLC) identifică firmware-ul fără patch-uri, implementări criptografice slabe, mecanisme de actualizare nesigure și vulnerabilități și expuneri comune (CVE) cunoscute public. În plus, sunt evaluate certificatele digitale slabe sau expirate și tehnicile insuficiente de întărire a firmware-ului, care expun dispozitivele IoT la infecții malware, modificări neautorizate și amenințări de securitate persistente.

Această abordare structurată nu numai că a îmbunătățit înțelegerea riscurilor de securitate cibernetică, dar a și pus bazele mecanismelor de securitate dezvoltate în capitolele următoare. Prin integrarea modelării amenințărilor cu un caz de utilizare a sistemului, această cercetare a stabilit cu

succes o metodologie structurată de evaluare a riscurilor de securitate cibernetică adaptată pentru rețelele inteligente de energie solară bazate pe IoT, asigurând că soluțiile de securitate au fost dezvoltate ca răspuns la provocări, mai degrabă decât să se bazeze exclusiv pe literatura de specialitate.

O3: Proiectarea și implementarea unui sistem de monitorizare sigur și inteligent pentru rețelele de energie solară bazate pe IoT

Pentru a atinge obiectivul O2, această cercetare s-a axat pe proiectarea și punerea în aplicare a unui sistem de monitorizare sigur și inteligent care îmbunătățește securitatea cibernetică, integritatea și capacitățile în rețelele de energie solară bazate pe IoT. Mecanismele de securitate dezvoltate au vizat atenuarea amenințărilor și vulnerabilităților identificate în obiectivul O1, în special a celor clasificate prin modelul de amenințare STRIDE. Prin abordarea spoofing-ului, a falsificării, a repudierii, a divulgării de informații, a refuzului de serviciu și a ridicării privilegiilor, măsurile de securitate implementate în acest studiu au urmărit să reducă riscurile asociate fiecărei categorii. Acest obiectiv a fost abordat în principal în capitolele 4 și 5.

A.Dezvoltarea unui sistem de monitorizare securizat (capitolul 4)

Sistemul de monitorizare securizat dezvoltat în cadrul acestei cercetări a fost conceput pentru a proteja comunicarea dintre dispozitivele IoT și serviciile cloud, pentru a asigura confidențialitatea datelor și pentru a preveni accesul neautorizat la componentele esențiale ale infrastructurii. Acesta a răspuns direct amenințărilor STRIDE, asigurând că vulnerabilitățile identificate în capitolul 3 au fost atenuate prin mecanisme de securitate adaptate rețelelor solare activate de IoT.

Unul dintre principalele mecanisme de securitate implementate a fost criptarea AES (Advanced Encryption Standard), care a securizat comunicarea dintre nodurile IoT și gateway-ul de teren IoT. Astfel, au fost abordate amenințările legate de divulgarea și falsificarea informațiilor, asigurându-se că datele schimbate în cadrul rețelei IoT rămân confidențiale și protejate împotriva interceptării neautorizate. Mecanismul de criptare a asigurat că datele transmise între senzori, controlere și gateway-ul de teren au rămas sigure, împiedicând atacatorii să exploateze pachetele de date interceptate.

Pentru a spori și mai mult securitatea comunicațiilor, a fost implementat Transport Layer Security (TLS) pentru criptarea de la un capăt la altul între gateway-ul de teren IoT și serviciile cloud. În timp ce AES a securizat transmiterea locală a datelor, TLS a oferit un nivel suplimentar de securitate pentru comunicațiile la distanță, atenuând atacurile MITM (Man-in-the-Middle) și prevenind accesul neautorizat la datele transmise. Combinația dintre AES la nivelul rețelei IoT și TLS pentru integrarea în cloud a asigurat multi-criptare stratificată în întregul sistem. În plus, aceasta protejează împotriva atacurilor de falsificare. Implementarea unor metode sigure de transmitere a datelor a asigurat că datele senzorilor nu pot fi modificate în tranzit, abordând riscurile de manipulare identificate prin analiza STRIDE. Aceste îmbunătățiri ale securității au asigurat că, chiar dacă un atacator a interceptat comunicarea, acesta nu va putea modifica datele fără a fi detectat.

Prin punerea în aplicare a acestor mecanisme de securitate, sistemul de monitorizare securizat a

atenuat cu succes riscurile multiple de securitate cibernetică identificate prin modelarea STRIDE, asigurând controlul amenințărilor de tip spoofing, manipulare, repudiere, divulgare de informații și refuz de serviciu.

B. Îmbunătățiri ale securității bazate pe cloud și integrarea monitorizării (capitolul 5)

Pentru a extinde capacitățile de securitate ale sistemului inteligent de monitorizare a energiei solare bazat pe IoT, capitolul 5 s-a axat pe integrarea mecanismelor de securitate bazate pe cloud pentru a asigura comunicarea sigură, autentificarea și controlul accesului între dispozitivele IoT și serviciile cloud. Cercetarea a valorificat serviciile Microsoft Azure IoT, implementând controale de securitate pentru a îmbunătăți protecția datelor, autorizarea și monitorizarea de la distanță în rețelele de energie solară bazate pe IoT.

1. Azure IoT Hub și integrarea în cloud:
    - Integrarea Azure IoT Hub, Stream Analytics, Power BI și Time Series Insights a facilitat conectivitatea sigură și transmiterea datelor, permițând sistemelor inteligente de energie solară bazate pe IoT să interacționeze cu serviciile bazate pe cloud.
    - Azure IoT Hub a servit drept hub central pentru comunicarea dispozitivelor, în timp ce Stream Analytics a procesat fluxuri de date în timp real, Power BI a oferit vizualizare interactivă, iar Time Series Insights a oferit analize avansate pentru datele din seriile de timp.
    - Această integrare a permis monitorizarea, procesarea și vizualizarea datelor în timp real, oferind informații utile pentru optimizarea sistemului și luarea deciziilor.
2. SAS tokens (Shared Access Signature):
    - SAS tokens au fost utilizate pentru autorizare și controlul accesului, permițând un control fin asupra comunicării dispozitivelor IoT cu cloud-ul.
    - Politicile de acces limitate în timp și în funcție de permisiuni au asigurat că numai dispozitivele autentificate pot trimite și primi date, reducând riscurile de acces neautorizat.
3. Transport Layer Security (TLS):
    - Criptarea TLS a fost implementată pentru a proteja transmisia de date între gateway-ul de teren IoT și serviciile cloud, prevenind atacurile MITM, interceptarea și manipularea.
    - Aceasta a completat criptarea AES utilizată între nodurile IoT și gateway-ul de teren IoT, creând o strategie de criptare stratificată care a protejat datele de la punctul de colectare până la infrastructura cloud
4. Autentificarea dispozitivelor și controlul accesului:
    - Politicile de autentificare a dispozitivelor și mecanismele de control al accesului au asigurat că numai dispozitivele IoT înregistrate și autentificate pot comunica cu cloud-

ul, reducând riscul de injectare neautorizată a datelor sau de falsificare a dispozitivelor.

- Controlul accesului pe bază de rol (RBAC) și politicile de acces partajat (SAP) au fost puse în aplicare pentru a defini roluri și permisiuni specifice, respectând principiul privilegiului minim.

***O4**: Dezvoltarea unui cadru unificat proactiv de monitorizare, detectare și gestionare a incidentelor de securitate cibernetică:*

Pentru a atinge obiectivul O4, această cercetare a dezvoltat un cadru unificat de monitorizare, detectare și gestionare a incidentelor de securitate cibernetică prin integrarea soluțiilor de securitate SIEM (Security Information and Event Management) și OT (Operational Technology) pentru rețelele inteligente de energie solară bazate pe IoT. Cadrul a fost conceput pentru a aborda limitările abordărilor tradiționale de securitate, asigurând detectarea amenințărilor în timp real, corelarea incidentelor și mecanisme de răspuns proactiv în mediile IoT, cloud și OT. Acest obiectiv a fost abordat în principal în capitolul 6.

A. Monitorizarea proactivă a securității cibernetice și gestionarea incidentelor (capitolul 6)

Cercetarea a introdus o strategie proactivă de monitorizare a securității cibernetice și de răspuns care combină monitorizarea securității IT bazată pe SIEM cu monitorizarea centralizată a securității OT, permițând o postură de securitate cuprinzătoare și unificată. Cadrul a utilizat Sentinel SIEM pentru monitorizarea securității IT și Microsoft Defender pentru IoT pentru monitorizarea securității OT, asigurând detectarea, analiza și atenuarea continuă a amenințărilor din straturile IT, IoT și OT.

Pentru a stabili o abordare de monitorizare centralizată, au fost implementate analize de securitate bazate pe SIEM pentru a colecta, corela și analiza evenimentele de securitate de la dispozitivele IoT și serviciile cloud. Acest lucru a permis sistemului să detecteze comportamente anormale, să identifice potențiale amenințări și să declanșeze alerte pe baza unor reguli de securitate predefinite. SIEM a jucat un rol cheie în agregarea jurnalelor de securitate, analizarea modelelor și corelarea indicatorilor de amenințare, asigurând detectarea incidentelor de securitate în timp real.

În paralel, Defender for IoT a fost implementat pentru monitorizarea securității OT, oferind o vizibilitate profundă asupra traficului de rețea industrială, comunicațiilor dispozitivelor și amenințărilor specifice protocolului. Defender for IoT a permis sistemului să identifice amenințările cibernetice care vizează dispozitivele de teren, controlerele industriale și infrastructurile de energie solară bazate pe SCADA, completând monitorizarea securității IT bazată pe SIEM.

Pentru a permite un răspuns proactiv la incidente, cadrul a implementat mecanisme automate de alertă și de corelare a evenimentelor de securitate, asigurându-se că indicatorii de amenințare detectați în mediile IT, IoT și OT sunt legați de scenariile potențiale de atac. Această abordare a îmbunătățit capacitatea sistemului de a detecta atacurile cibernetice în mai multe etape, în care atacatorii ar putea încerca să treacă de la rețelele IT la sistemele OT sau să exploateze vulnerabilitățile din infrastructura IoT.

Integrarea SIEM și a monitorizării securității OT a oferit o viziune unificată asupra amenințărilor la adresa securității cibernetice, asigurând detectarea și atenuarea promptă a incidentelor care afectează rețelele inteligente de energie solară bazate pe IoT. De asemenea, cadrul a îmbunătățit cunoașterea situației, permițând echipelor de securitate să identifice și să răspundă amenințărilor cibernetice înainte ca acestea să perturbe operațiunile energetice.

O5: Evaluarea și validarea eficacității cadrului de securitate propus utilizând date din lumea reală

Pentru a atinge obiectivul O5, această cercetare a efectuat experimente de evaluare și validare pentru a măsura eficacitatea cadrului propus de monitorizare, detectare și gestionare a incidentelor de securitate cibernetică pentru rețelele inteligente de energie solară bazate pe IoT. Pe lângă datele din sistemul de caz de utilizare implementat, procesul de validare a implicat date din lumea reală ale sistemului de control industrial (ICS) și date IT, asigurându-se că mecanismele de securitate implementate în capitolele anterioare au fost testate în medii practice. Acest obiectiv a fost abordat în principal în capitolul 6.

Evaluarea și validarea cadrului de securitate (capitolul 6):

Procesul de validare a urmărit să demonstreze capacitatea cadrului de securitate cibernetică de a detecta, analiza și răspunde la amenințările cibernetice care vizează sistemele inteligente de energie solară bazate pe IoT. Evaluarea experimentală s-a axat pe:

- Evaluarea eficacității monitorizării securității IT bazate pe SIEM, în special în detectarea evenimentelor anormale, a tentativelor de acces neautorizat și a tiparelor de atacuri cibernetice în cadrul sistemelor IoT integrate în cloud.
- Validarea monitorizării securității OT utilizând Defender for IoT, asigurându-se că anomaliile de rețea, amenințările bazate pe protocol și activitățile suspecte ale dispozitivelor au fost identificate cu exactitate în mediile de control industrial.
- Măsurarea impactului corelării integrate a evenimentelor de securitate, determinând cât de bine cadrul a legat indicatorii de amenințare între straturile IT, IoT și OT pentru a detecta atacurile cibernetice în mai multe etape.

Pentru a asigura o validare realistă, cercetarea a utilizat date reale din rețele industriale și jurnale de evenimente de securitate, reproducând potențiale scenarii de atacuri cibernetice cu care s-ar putea confrunta sistemele de energie solară bazate pe IoT. Această abordare a permis o evaluare empirică a capacității sistemului de a detecta amenințările de securitate cibernetică cunoscute și emergente.

Rezultatele evaluării au confirmat că cadrul de securitate cibernetică propus a detectat și a atenuat în mod eficient amenințările la adresa securității în rețelele inteligente de energie solară bazate pe IoT. Procesul de validare a demonstrat mai multe capacități-cheie în monitorizarea securității IT bazată pe SIEM și monitorizarea securității OT utilizând Defender for IoT, asigurând detectarea în timp real, corelarea evenimentelor de securitate și răspunsul la potențialele amenințări cibernetice.

Una dintre capacitățile notabile identificate a fost descoperirea automată a dispozitivelor sistemului

de control industrial (ICS), inclusiv controlerele logice programabile (PLC), unitățile terminale la distanță (RTU) și alte componente OT din cadrul rețelei. Această caracteristică permis cadrului de securitate să cartografieze arhitectura rețelei industriale, oferind o vizibilitate sporită a dispozitivelor conectate, a fluxurilor de comunicare și a vulnerabilităților potențiale în infrastructurile de energie solară bazate pe IoT.

În plus, evaluarea a confirmat că monitorizarea securității bazată pe SIEM a demonstrat o acuratețe ridicată în detectarea tentativelor de acces neautorizat, a atacurilor prin forța brută și a incidentelor de exfiltrare a datelor. Defender for IoT a identificat cu succes amenințările specifice OT, inclusiv traficul de rețea malițios, modelele de comunicare anormale și utilizarea necorespunzătoare a protocolului în dispozitivele industriale.

Integrarea monitorizării securității IT și OT a îmbunătățit semnificativ detectarea atacurilor cibernetice în mai multe etape, în care adversarii au încercat să treacă de la rețelele IT la mediile OT. Mecanismele de corelare a evenimentelor din cadrul sistemului SIEM au permis echipelor de securitate să urmărească modelele de atac în diferite straturi ale infrastructurii, îmbunătățind cunoașterea situației și timpul de răspuns.

În plus, capacitatea de a detecta comportamente anormale în dispozitivele ICS a consolidat monitorizarea proactivă a amenințărilor, asigurând că abaterile de la liniile de bază operaționale normale au fost identificate și atenuate rapid. Acest lucru a contribuit la reducerea riscului de perturbări cibernetice ale sistemelor inteligente de energie solară.

Experimentele de validare au demonstrat că mecanismele de securitate implementate pe parcursul cercetării au îmbunătățit în mod eficient reziliența securității cibernetice a rețelelor inteligente de energie solară bazate pe IoT, abordând vulnerabilitățile cheie identificate în obiectivul O1 și validând soluțiile dezvoltate în obiectivele O2 și O3.

7.2. Contribuții originale

Această cercetare doctorală aduce mai multe contribuții originale la securitatea cibernetică pentru rețelele inteligente de energie regenerabilă bazate pe IoT, în special în securizarea sistemelor de energie solară bazate pe IoT. Contribuțiile sunt structurate după cum urmează:

A. Sistematizarea cunoștințelor și revizuirea critică

1. S-a efectuat o analiză cuprinzătoare și o sistematizare a provocărilor de securitate cibernetică care afectează rețelele inteligente de energie regenerabilă bazate pe IoT, concentrându-se în special pe sistemele solare fotovoltaice (PV).
2. S-a clasificat și analizat amenințările cibernetice, vulnerabilitățile, vectorii de atac și motivațiile, oferind o înțelegere structurată a riscurilor de securitate în sistemele solare inteligente bazate pe IoT.
3. S-a aplicat analiza Cyber Kill Chain la rețelele PV, demonstrând modul în care adversarii pot exploata vulnerabilitățile în diferite etape ale unui atac.

4. S-a analizat critic măsurile de securitate existente, inclusiv protocoalele de criptare, mecanismele de autentificare, detectarea intruziunilor, blockchain și apărarea bazată pe învățarea automată, identificând limitările acestora în protejarea sistemelor inteligente de energie regenerabilă.
5. Au fost identificate lacune în cercetarea privind strategiile integrate de securitate IT-IoT/OT, subliniind unui cadru unificat de securitate cibernetică adaptat rețelelor solare bazate pe IoT.

B.Modelarea amenințărilor și evaluarea riscurilor pentru sistemele de energie solară bazate pe IoT

1. S-a dezvoltat o abordare îmbunătățită de modelare a amenințărilor utilizând metodologiile STRIDE și DREAD pentru a clasifica sistematic și a prioritiza amenințările informatice care vizează sistemele fotovoltaice inteligente bazate pe IoT.
2. S-a realizat un cadru de evaluare a riscurilor care integrează riscurile de securitate pentru a cuantifica potențialele amenințări la adresa securității cibernetice pentru cazul de utilizare dezvoltat al sistemului de energie solară bazat pe IoT.
3. Vulnerabilitățile de securitate la nivel de dispozitiv au fost examinate prin efectuarea unei evaluări a vulnerabilităților firmware ale dispozitivelor IoT integrate în sistemele de energie solară. Logica programabilă (PLC) identifică firmware neacoperit, implementări criptografice slabe, mecanisme de actualizare nesigure și vulnerabilități și expuneri comune (CVE) cunoscute public. În plus, sunt evaluate certificatele digitale slabe sau expirate și tehnicile insuficiente de întărire a firmware-ului, expunând dispozitivele IoT la infecții malware, modificări neautorizate și amenințări de securitate persistente.

B.Arhitectură sigură de monitorizare bazată pe IoT pentru rețele solare inteligente

1. S-a proiectat și implementat o arhitectură de sistem de monitorizare securizată pentru rețelele fotovoltaice inteligente bazate pe IoT, asigurând protecția datelor de la un capăt la altul, de la dispozitivele IoT la cloud.
2. AES (Advanced Encryption Standard) integrat pentru securitatea datelor și TLS 1.2 (Transport Layer Security) pentru comunicarea în cloud, asigurând confidențialitatea și integritatea datelor senzorilor prin atenuarea amenințărilor identificate prin metodologia STRIDE.
3. S-a dezvoltat un sistem de monitorizare la distanță în timp real folosind SystemLink Cloud, îmbunătățind vizualizarea sigură și analiza datelor pentru rețelele inteligente de energie solară.

C.Soluții de securitate bazate pe cloud pentru sistemele de energie regenerabilă bazate pe IoT

1. S-a proiectat servicii integrate în cloud utilizând serviciile Microsoft Azure IoT (IoT Hub, Stream Analytics, Power BI și Time Series Insights) pentru procesarea sigură și în timp real a datelor.
2. S-a implementat autentificarea dispozitivelor, politicile de acces partajat (SAP) și autorizarea pe bază de tokenuri SAS (Shared Access Signature) pentru a spori securitatea în mediile IoT bazate pe cloud.

3. Politici integrate de control al accesului pe bază de rol (RBAC) pentru aplicarea unui management strict al permisiunilor în comunicațiile IoT-cloud.

D.Monitorizare proactivă unificată a securității cibernetice și gestionarea incidentelor. S-a dezvoltat un cadru unificat de securitate cibernetică, integrând SIEM și monitorizarea securității IoT/OT pentru detectarea amenințărilor în timp real și răspunsul la incidente.

1. Au fost dezvoltate tehnici avansate de corelare a evenimentelor pentru detectarea atacurilor cibernetice în mai multe etape care acoperă domeniile IT și OT . ????
2. S-a implementat o analiza pasivă a traficului de rețea pentru dispozitivele OT, îmbunătățind detectarea și atenuarea amenințărilor cibernetice care vizează sistemele de control industrial
3. S-au dezvoltat mecanisme de detectare a anomaliilor în timp real folosind învățarea automată și informații despre amenințări pentru a identifica proactiv incidentele de securitate cibernetică.
4. Descoperirea și vizibilitatea automată a activelor, asigurând monitorizarea continuă a tuturor dispozitivelor IoT conectate.

7.3. Valorificarea rezultatelor cercetării

Rezultatele cercetării au fost diseminate prin 13 publicații, inclusiv în reviste ISI cu impact ridicat, prezentări la conferințe internaționale și capitole de carte. Aceste eforturi au sporit vizibilitatea și impactul cercetării.

A. Lucrarii publicate în reviste cotate ISI

1. **Rekeraho, A**., Cotfas, D.T., Cotfas, P.A. et al. Cybersecurity challenges in IoT-based smart renewable energy. Int. J. Inf. Secur. 23, 101–117 (2024). https://doi.org/10.1007/s10207-023-00732-9

   Factor de impact al revistei: 2,4 (2023), Q2.

2. 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

   Factor de impact: 2,5 (2023). Q1

3. **Rekeraho A**, Cotfas DT, Cotfas PA, Tuyishime E, Balan TC, Acheampong R. Enhancing Security for IoT-Based Smart Renewable Energy Remote Monitoring Systems. Electronics. 2024; 13(4):756. https://doi.org/10.3390/electronics13040756

   Factor de impact: 2,6 (2023), Q2

4. Acheampong, R., Popovici, D.-M., Balan, T., **Rekeraho, A**., & Ramos, M. S. (2025). Enhancing Security and Authenticity in Immersive Environments. *Information*, *16*(3), 191. https://doi.org/10.3390/info16030191

   Factor de impact: 2.4 (2023),Q2

5. Acheampong, R., Balan, T.C., Popovici, DM., **Rekeraho, A**. (2023). Embracing XR System Without Compromising on Security and Privacy. In: De Paolis, L.T., Arpaia, P.,

Sacco, M. (eds) Extended Reality. XR Salento 2023. Lecture Notes in Computer Science, vol 14218. Springer, Cham. https://doi.org/10.1007/978-3-031-43401-3_7

Lucrare de conferință indexată ISI: WOS:001156975100007

6. **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
   Factor de impact: 3.3 (2023), Q2
7. Acheampong Rebecca, Dorin-Mircea Popovici, Titus Balan, Emmanuel Tuyishemi, **Alexandre Rekeraho**, Gheorghe Daniel Voinea. "Balancing Usabiity, User Experience, Security and Privacy: Multidimensional Approach". International Journal of Information Security, (2025)- Accepted for publication, Factor de impact al revistei: 2,5 (2023), Q2.

B. Lucrarii publicate în revistele BDI

1. **A. Rekeraho**, T. Balan, D. T. Cotfas, P. A. Cotfas, R. Acheampong and C. Musuroi, "Sandbox Integrated Gateway for the Discovery of Cybersecurity Vulnerabilities," 2022 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 2022, pp. 1-4, doi: 10.1109/ISETC56213.2022.10010327.
2. E. Tuyishime, F. Radu, P. Cotfas, D. Cotfas, T. Balan and **A. Rekeraho** , "Online Laboratory Access Control with Zero Trust Approach: Twingate Use Case," 2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 2024, pp. 1-7, doi: 10.1109/ECAI61503.2024.10607562.
3. R. Acheampong, T. C. Bălan, D. -M. Popovici and **A. Rekeraho** , "Security Scenarios Automation and Deployment in Virtual Environment using Ansible," *2022 14th International Conference on Communications (COMM)*, Bucharest, Romania, 2022, pp. 1-7, doi: 10.1109/COMM54429.2022.9817150.
4. D. Tudor Cotfas, P. A. Cotfas, **A. Rekeraho** and M. Madhiarasan, "Photovoltaic Mini-Panel and Thermoelectric Generator Under Concentrated Light," *2022 International Symposium on Electronics and Telecommunications (ISETC)*, Timisoara, Romania, 2022, pp. 1-4, doi: 10.1109/ISETC56213.2022.10010280.
5. Rebecca Acheampong, Bogdan Valentin Floricescu, Ionut Alexandru Oprea, **Alexandre Rekeraho**, Vladut Gabriel Anghel, Gabriel Danciu, Ioana Corina Bogdan, George Stefan Ionesc. Scalable Secure Platform for XR, EEITE 2025 Conference-Accepted for publication

C. Capitol de carte

1. 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

D. Proiect de cercetare (membru)

Numele proiectului	Rol	Perioada de punere în aplicare
Platformă scalabilă pentru inovații privind teleprezența imersivă în timp real SPIRIT: GENBA SAVR: Platformă sigură de realitate virtuală Manager de proiect Prof. Gabriel Danciu	Asistent de cercetare, Universitatea Transilvania din Brașov	Octombrie 2024- Aprilie 2025

7.4. Noi direcții de cercetări

Această cercetare a adus contribuții semnificative pentru securitatea cibernetică a rețelelor inteligente de energie regenerabilă bazate pe IoT. Cu toate acestea, sunt necesare cercetări suplimentare pentru a aborda provocările emergente și pentru a consolida mecanismele de securitate. Următoarele direcții de cercetare sunt propuse pentru activitatea viitoare:

1.Criptografie post-cuantum pentru rețelele de energie regenerabilă bazate pe IoT

Investigarea și implementarea unor algoritmi criptografici post-cuantici ușori și eficienți din punct de vedere energetic pentru a proteja sistemele de energie regenerabilă bazate pe IoT împotriva amenințării în evoluție a calculului cuantic.

2.Arhitecturi Zero-Trust pentru gestionarea îmbunătățită a identității și accesului

Proiectarea și implementarea arhitecturilor Zero-Trust pentru a consolida gestionarea identității și controlul accesului în sistemele de energie regenerabilă bazate pe IoT.

3. Autentificarea identității și controlul accesului bazate pe Blockchain

Explorarea utilizării tehnologiei blockchain pentru autentificarea descentralizată a identității și controlul accesului în sistemele distribuite de energie regenerabilă bazate pe IoT.

4.Tehnici de prelucrare a datelor care protejează confidențialitatea

Dezvoltarea de tehnici de procesare a datelor care protejează confidențialitatea, cum ar fi criptarea homomorfă, confidențialitatea diferențială și învățarea federată, pentru a permite partajarea sigură a datelor între dispozitivele IoT, serviciile cloud și centrele de control.

5. Implicațiile etice, juridice și politice ale securității cibernetice

Investigarea implicațiilor etice, juridice și politice ale securității cibernetice în infrastructurile inteligente de energie regenerabilă.

Bibliografie

[1] Q. Hassan *et al.*, "The renewable energy role in the global energy Transformations," *Renewable Energy Focus*, vol. 48, p. 100545, Mar. 2024, doi: 10.1016/j.ref.2024.100545.

[2] D. Gayen, R. Chatterjee și S. Roy, "A review on environmental impacts of renewable energy for sustainable development," *Int. J. Environ. Sci. Technol.*, vol. 21, nr. 5, pp. 5285-5310, mar. 2024, doi: 10.1007/s13762-023-05380-z.

[3] D. T. Cotfas, A. Enesca și P. A. Cotfas, "Enhancing the performance of the solar thermoelectric generator in unconcentrated and concentrated light", *Renewable Energy*, vol. 221, p. 119831, feb. 2024, doi: 10.1016/j.renene.2023.119831.

[4] G. M. Idroes, I. Hardi, Md. H. Rahman, M. Afjal, T. R. Noviandy și R. Idroes, "The dynamic impact of non-renewable and renewable energy on carbon dioxide emissions and ecological footprint in Indonesia", *Carbon Res.*, vol. 3, nr. 1, p. 35, apr. 2024, doi: 10.1007/s44246-024-00117-0.

[5] D. O. Obada *et al.*, "A review of renewable energy resources in Nigeria for climate change mitigation," *Case Studies in Chemical and Environmental Engineering*, vol. 9, p. 100669, Jun. 2024, doi: 10.1016/j.cscee.2024.100669.

[6] F. Belabbes, D. T. Cotfas, P. A. Cotfas și M. Medles, "Using the snake optimization metaheuristic algorithms to extract the photovoltaic cells parameters", *Energy Conversion and Management*, vol. 292, p. 117373, sep. 2023, doi: 10.1016/j.enconman.2023.117373.

[7] D. T. Cotfas și P. A. Cotfas, "EDUCATION FOR SUSTAINABILITY THROUGH RENEWABLE ENERGY," *INTED2023 Proceedings*, pp. 7639-7648, 2023, doi: 10.21125/inted.2023.2089.

[8] "Dampening energy security-related uncertainties in the United States: The role of green energy-technology investment and operation of transnational corporations - ScienceDirect". Accesat: Jun. 19, 2024. [Online]. Disponibil: https://www.sciencedirect.com/science/article/pii/S036054422303400X

[9] T. Bulavskaya și F. Reynès, "Job creation and economic impact of renewable energy in the Netherlands", *Renewable Energy*, vol. 119, pp. 528-538, apr. 2018, doi: 10.1016/j.renene.2017.09.039.

[10] E. T. Sayed *et al.*, "Renewable Energy and Energy Storage Systems", *Energies*, vol. 16, nr. 3, Art. no. 3, Jan. 2023, doi: 10.3390/en16031415.

[11] M. A. J. Quirapas Franco și A. Taeihagh, "Sustainable energy adoption in poor rural areas: A comparative case perspective from the Philippines", *Energy for Sustainable Development*, vol. 79, p. 101389, apr. 2024, doi: 10.1016/j.esd.2024.101389.

[12] Ch. M. S. Kumar *et al.*, "Solar energy: A promising renewable source for meeting energy demand in Indian agriculture applications", *Sustainable Energy Technologies and Assessments*, vol. 55,

p. 102905, feb. 2023, doi: 10.1016/j.seta.2022.102905.

[13] H. H. Pourasl, R. V. Barenji și V. M. Khojastehnezhad, "Solar energy status in the world: A comprehensive review", *Energy Reports*, vol. 10, pp. 3474-3493, nov. 2023, doi: 10.1016/j.egyr.2023.10.022.

[14] A. Mohammad și F. Mahjabeen, "Revolutionizing Solar Energy with AI-Driven Enhancements in Photovoltaic Technology," *BULLET : Jurnal Multidisiplin Ilmu*, vol. 2, nr. 4, Art. no. 4, aug. 2023.

[15] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt și B. Zakeri, "Internet of Things (IoT) and the Energy Sector", *Energies*, vol. 13, nr. 2, art. nr. 2, ianuarie 2020, doi: 10.3390/en13020494.

[16] Z. Lv, W. Liu și T. Xu, "Evaluating the impact of information and communication technology on renewable energy consumption: A spatial econometric approach", *Renewable Energy*, vol. 189,

pp. 1-12, apr. 2022, doi: 10.1016/j.renene.2022.03.005.

[17] M. S. Qureshi, S. Umar și M. U. Nawaz, "Machine Learning for Predictive Maintenance in Solar Farms", *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, nr. 3, Art. nr. 3, apr. 2024.

[18] R. K. Pachauri *et al.*, "Solar Photovoltaic System-Based Power Generation", în *Clean and Renewable Energy Production*, John Wiley & Sons, Ltd, 2024, pp. 267-286. doi: 10.1002/9781394174805.ch11.

[19] S. Umar, M. U. Nawaz și M. S. Qureshi, "Deep Learning Approaches for Crack Detection in Solar PV Panels," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 3, Art. no. 3, apr. 2024.

[20] F. Harrou, B. Taghezouit, B. Bouyeddou și Y. Sun, "Cybersecurity of photovoltaic systems: challenges, threats, and mitigation strategies: a short survey," *Front. Energy Res.*, vol. 11, sep. 2023, doi: 10.3389/fenrg.2023.1274451.

[21] A. A. Khan și O. A. Beg, "Cyber Vulnerabilities of Modern Power Systems," în *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*, H. Haes Alhelou, N. Hatziargyriou, and Z.

Y. Dong, Eds., Cham: Springer International Publishing, 2023, pp. 47-66. doi:

10.1007/978-3- 031-20360-2_2.

[22] "Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations." Accesat:

Jun. 19, 2024. [Online]. Disponibil: https://ieeexplore.ieee.org/abstract/document/9046835

[23] "Cyber-physical security framework for Photovoltaic Farms| IEEE Conference Publication|

IEEE Xplore." Accesat: May 19, 2024. [Online]. Disponibil: https://ieeexplore.ieee.org/abstract/document/9311533

[24] A. Karthikeyan, K. Karthikeyan și O. V. G. Swathika, "2 - Cyber-physical security in a stand- alone photovoltaic system for rural electrification", în *Next-Generation Cyber-Physical Microgrid Systems*, O. V. G. Swathika, K. Karthikeyan și S. Padmanaban, Eds., Elsevier, 2024, pp. 29-75. doi: 10.1016/B978-0-443-22187-3.00002-3.

[25] J. Ye *et al.*, "A Review of Cyber-Physical Security for Photovoltaic Systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, pp. 4879-4901, aug. 2022, doi: 10.1109/JESTPE.2021.3111728.

[26] D. Moher *et al.*, "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement", *Systematic Reviews*, vol. 4, nr. 1, p. 1, ianuarie 2015, doi: 10.1186/2046-4053-4-1.

[27] E. Ferrier, "LibGuides: Guide to Searching: Citation Searching". Accesat: Feb. 16, 2023. [Online].

Disponibil: https://libguides.brown.edu/searching/citation

[28] H. Kraus, "LibGuides: Topic: Căutarea sistematică pentru sinteza dovezilor: Searching Scopus". Accesat: Feb. 16, 2023. [Online]. Disponibil: https://guides.lib.uconn.edu/systematic_searching/scopus

[29] H. Riggs, S. Tufail, M. Khan, I. Parvez și A. I. Sarwat, "Detection of False Data Injection of PV Production," in *2021 IEEE Green Technologies Conference (GreenTech)*, Apr. 2021, pp. 7-12. doi: 10.1109/GreenTech48523.2021.00012.

[30] "A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids| IEEE Journals & Magazine| IEEE Xplore." Accesat: Jun. 20, 2024. [Online].

Disponibil: https://ieeexplore.ieee.org/abstract/document/8093999

[31] X. Zhong, I. Jayawardene, G. K. Venayagamoorthy și R. Brooks, "Denial of Service Attack on Tie-Line Bias Control in a Power System With PV Plant," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 1, no. 5, pp. 375-390, oct. 2017, doi: 10.1109/TETCI.2017.2739838.

[32] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi și H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges", *Computers & Electrical Engineering*, vol. 67, pp. 469-482, apr. 2018, doi: 10.1016/j.compeleceng.2018.01.015.

[33] M. R. Habibi, H. R. Baghaee, T. Dragičević și F. Blaabjerg, "Detection of False Data Injection Cyber-Attacks in DC Microgrids Based on Recurrent Neural Networks", *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5294-5310, oct. 2021, doi: 10.1109/JESTPE.2020.2968243.

[34] L. Wei, D. Gao și C. Luo, "False Data Injection Attacks Detection with Deep Belief Networks in

Smart Grid", în *2018 Chinese Automation Congress (CAC)*, Nov. 2018, pp. 2621-2625. doi: 10.1109/CAC.2018.8623514.

[35] S. Ferlito, S. Ippolito, C. Santagata, P. Schiattarella și G. Di Francia, "A Study on an IoT-Based SCADA System for Photovoltaic Utility Plants", *Electronics*, vol. 13, nr. 11, Art. nr. 11, Jan. 2024, doi: 10.3390/electronics13112065.

[36] P. J. Hueros-Barrios, Fco. J. Rodríguez, P. Martín, M. Gayo și I. Fernández, "Addressing cybersecurity threats in prosumer-based nanogrids with MQTT communication," in *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Jul. 2022,

pp. 1-6. doi: 10.1109/ICECET55527.2022.9872918.

[37] C. Carter, I. Onunkwo, P. Cordeiro și J. Johnson, "Cyber Security Assessment of Distributed Energy Resources", în *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC)*, iunie 2017, pp. 2135-2140. doi: 10.1109/PVSC.2017.8366503.

[38] D. Saleem, A. Sundararajan, A. Sanghvi, J. Rivera, A. I. Sarwat și B. Kroposki, "A Multidimensional Holistic Framework for the Security of Distributed Energy and Control Systems", *IEEE Systems Journal*, vol. 14, nr. 1, pp. 17-27, mar. 2020, doi: 10.1109/JSYST.2019.2919464.

[39] Y. Dafalla, B. Liu, D. A. Hahn, H. Wu, R. Ahmadi și A. G. Bardas, "Prosumer Nanogrids: A Cybersecurity Assessment", *IEEE Access*, vol. 8, pp. 131150-131164, 2020, doi: 10.1109/ACCESS.2020.3009611.

[40] Y. Dubasi, A. Khan, Q. Li și A. Mantooth, "Security Vulnerability and Mitigation in Photovoltaic Systems," in *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Jun. 2021, pp. 1-7. doi: 10.1109/PEDG51384.2021.9494252.

[41] L. Pavithra și D. Rekha, "Prevention of Replay Attack for Isolated Smart Grid," în *Next Generation Information Processing System*, P. Deshpande, A. Abraham, B. Iyer, și K. Ma, Eds., în Advances in Intelligent Systems and Computing. Singapore: Springer, 2021, pp. 251-258. doi: 10.1007/978-981-15-4851-2_27.

[42] M. Dehghani, T. Niknam, M. Ghiasi, N. Bayati și M. Savaghebi, "Cyber-Attack Detection in DC Microgrids Based on Deep Machine Learning and Wavelet Singular Values Approach", *Electronics*, vol. 10, nr. 16, Art. nr. 16, Jan. 2021, doi: 10.3390/electronics10161914.

[43] A. Ameli, A. Hooshyar, E. F. El-Saadany și A. M. Youssef, "An Intrusion Detection Method for Line Current Differential Relays," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 329-344, 2020, doi: 10.1109/TIFS.2019.2916331.

[44] A. Rekeraho, D. T. Cotfas, P. A. Cotfas, T. C. Bălan, E. Tuyishime și R. Acheampong, "Cybersecurity challenges in IoT-based smart renewable energy," *Int. J. Inf. Secur.*, Aug. 2023, doi: 10.1007/s10207-023-00732-9.

[45] O. Saßnick, T. Rosenstatter, C. Schäfer și S. Huber, "STRIDE-based Methodologies for Threat Modeling of Industrial Control Systems: A Review", în *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS)*, mai 2024, pp. 1-8. doi: 10.1109/ICPS59941.2024.10639949.

[46] L. Zhang, A. Taal, R. Cushing, C. de Laat și P. Grosso, "A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces," *Int. J. Inf. Secur.*, vol. 21, nr. 3, pp. 509-525, iun. 2022, doi: 10.1007/s10207-021-00566-3.

[47] Q. Li și Y.-L. Chen, "Data Flow Diagram", în *Modeling and Analysis of Enterprise and Information Systems: From Requirements to Realization*, Q. Li și Y.-L. Chen, Eds., Berlin, Heidelberg: Springer, 2009, pp. 85-97. doi: 10.1007/978-3-540-89556-5_4.

[48] S. Krishnaveni, M. Harsha Priya, S. Mallesh și Ch. Narendar, "A Smart Security Systems Using National Instruments myRIO," în *Confidential Computing: Hardware Based Memory Protection*,

V. Garcia Diaz și G. J. Rincón Aponte, Eds., Singapore: Springer Nature, 2022, pp. 187-

193. doi: 10.1007/978-981-19-3045-4_20.

[49] "Modelarea amenințărilor de securitate cibernetică pentru sistemele inteligente de energie solară integrate în IoT: Consolidarea rezilienței pentru sustenabilitatea energetică globală". Accesat: Apr. 02, 2025. [Online]. Disponibil: https://www.mdpi.com/2071-1050/17/6/2386

[50] A. Rekeraho, D. T. Cotfas, P. A. Cotfas, E. Tuyishime, T. C. Balan și R. Acheampong, "Enhancing Security for IoT-Based Smart Renewable Energy Remote Monitoring Systems", *Electronics*, vol. 13, no. 4, Art. no. 4, Jan. 2024, doi: 10.3390/electronics13040756.

[51] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas și A. Rekeraho, "Enhancing Cloud Security-Proactive Threat Monitoring and Detection Using a SIEM-Based Approach," *Applied Sciences*, vol. 13, nr. 22, Art. nr. 22, Jan. 2023, doi: 10.3390/app132212359.