Universitatea Transilvania din Braşov
Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor
Departamentul de Electronică şi Calculatoare

MEMORIU ȘTIINȚIFIC

asupra tezei de doctorat intitulate

"Addressing Cybersecurity Challenges in IoT/IIoT-based Remote Engineering Systems"

elaborată de Drd. Ing. Emmanuel TUYISHIME

Subsemnatul Petru Adrian Cotfas, profesor universitar în cadrul Departamentului de Electronică și Calculatoare al Facultății de Inginerie Electrică și Știința Calculatoarelor, Universitatea Transilvania din Brașov, în calitate de conducător științific al tezei de doctorat intitulate "Addressing Cybersecurity Challenges in IoT/IIoT-based Remote Engineering Systems", elaborată de doctorandul ing. Emmanuel Tuyishime, pe baza cunoașterii activităților științifice desfășurate de doctorand și a analizei atente a conținutului tezei, formulez următoarele aprecieri:

- Tema abordată se încadrează în activitățile actuale de dezvoltare și cercetare științifică din domeniul ingineriei electronice, telecomunicațiilor și tehnologiilor informaționale, vizând sistemele inginerești la distanță de tip IoT/IIoT din punctul de vedere al provocărilor de securitate cibernetică. Dezvoltarea puternică a rețelelor de comunicații, a tehnologiilor de calcul în „nori" (cloud computing) și a celor de tip IoT/IIoT, mai ales odată cu apariția Industriei 4.0, a permis intensificarea interacțiunii de la distanță cu procesele fizice și cu infrastructura inginerească, realizată prin intermediul rețelelor distribuite. Totuși, această interacțiune a crescut expunerea acestora la amenințări cibernetice. Teza se concentrează pe abordarea acestor provocări prin proiectarea, implementarea și testarea experimentală a unor mecanisme complementare de securitate cibernetică pentru sistemele de inginerie la distanță bazate pe IoT/IIoT. Au fost considerate trei direcții de cercetare, și anume: controlul accesului centrat pe identitate, detectarea intruziunilor eficientă din punctul de vedere al resurselor și arhitecturile de implementare orientate spre reziliență.
- Teza de doctorat are o structură logică și coerentă, fiind organizată în șapte capitole și șase anexe ce conțin linkuri către resursele publicate pe GitHub. Lucrarea se întinde pe 125 de pagini și conține 23 de tabele, 56 de figuri, 2 algoritmi și o listă de 324 de titluri bibliografice.
- Studiile efectuate și textul tezei sunt originale, aducând contribuții valoroase atât din punct de vedere teoretic, cât și aplicativ.

- Primul capitol prezintă contextul și motivația realizării studiilor doctorale, discutând problemele de securitate cibernetică apărute odată cu adoptarea rapidă a ingineriei la distanță și introducând lacunele identificate în domeniu. Pe baza acestor lacune/nișe s-au stabilit scopul și obiectivele cercetării. Metodologia propusă în acest capitol se bazează pe metodologia *Experimental Computer Science and Engineering (ECSE)*, care pune accent pe proiectarea, implementarea, evaluarea experimentală și rafinarea iterativă a sistemelor software și ciber-fizice.
- Capitolul al doilea este dedicat unui studiu bibliografic privind sistemele inginerești la distanță din domeniile educațional și industrial. Sunt discutate aspecte legate de arhitecturile utilizate pentru realizarea laboratoarelor și a sistemelor de monitorizare și control la distanță, considerând tehnologiile, protocoalele de comunicație și caracteristicile operaționale. Toate acestea sunt analizate din punctul de vedere al securității cibernetice, realizându-se o sinteză inter-domenii pentru identificarea riscurilor și vulnerabilităților arhitecturale comune, a zonelor de amenințare și a provocărilor de securitate nerezolvate.
- Modelul și arhitectura *Zero Trust* aplicate în mediile de inginerie la distanță sunt discutate în capitolul al treilea. În acest capitol sunt prezentate proiectarea, implementarea și validarea experimentală a unei arhitecturi de control al accesului centrate pe identitate, cu aplicabilitate în domeniul laboratoarelor la distanță
- Capitolul al patrulea este dedicat utilizării tehnicilor de învățare automată pentru detecția intruziunilor în medii de comunicații bazate pe protocolul MQTT, cu resurse limitate. S-a avut în vedere o metodă de selecție a unui număr mic, dar reprezentativ, de caracteristici, pe baza pragului diferenței dintre momentele statistice.
- Dezvoltarea și implementarea unei arhitecturi modulare pentru detectarea intruziunilor în timp real în IoT/IIoT, care integrează o componentă de *edge computing* bazată pe învățare automată și o componentă de monitorizare a securității bazată pe *cloud computing*, cu integrarea mediului Microsoft Sentinel, sunt prezentate în capitolul al cincilea. Este introdus și un mecanism de comutare a modelului de detectare a intruziunilor în timpul rulării, fără întreruperea monitorizării traficului.
- Capitolul al șaselea prezintă o extindere a arhitecturii propuse în capitolul al cincilea, orientată spre reziliență la nivelurile de *edge* și *fog computing*. Arhitectura hibridă propusă pentru detectarea intruziunilor permite păstrarea stării operaționale și a unei latențe scăzute în condiții de atac cibernetic. Rezultatele obținute prin testarea soluției propuse în diverse scenarii de inundare MQTT și de injectare de pachete malformate, în mai multe configurații de implementare, arată că distribuirea inferenței între straturile de *edge* și de *fog* îmbunătățește capacitatea de răspuns a sistemului și păstrează stabilitatea controlului în timpul solicitării rețelei.
- Concluziile și contribuțiile principale sunt prezentate în ultimul capitol, care include și rezultatele obținute, precum și direcțiile viitoare de cercetare.
- Rezultatele obținute pe parcursul studiilor doctorale au fost diseminate prin publicații științifice în jurnale indexate ISI și în conferințe indexate BDI, după cum urmează: șapte articole indexate ISI (șase în reviste și unul la conferințe), cinci articole prezentate

la conferințe internaționale și indexate IEEE Xplore (trei), SciTePress (unul) și Springer (unul), precum și un capitol de carte publicat la editura Springer. Doctorandul este prim autor la cinci dintre acestea: două în reviste ISI (Q2) și trei la conferințe internaționale. Toate aceste publicații certifică valoarea și recunoașterea rezultatelor activității de cercetare desfășurate de doctorand. Standardele minimale ale comisiei de inginerie electronică, telecomunicații și tehnologii informaționale au fost îndeplinite cu succes.

În urma analizei efectuate, apreciez că teza elaborată de către ing. Emmanuel Tuyishime reprezintă o lucrare științifică relevantă și originală în domeniul de doctorat Inginerie Electronică, Telecomunicații și Tehnologii Informaționale. Prezentarea grafică și redactarea sunt corespunzătoare, iar lucrarea respectă cerințele tehnice și practice impuse unei teze de doctorat. Prin urmare, recomand susținerea ei publică în vederea obținerii titlului științific de doctor inginer.

Data:
23.10.2026

Conducător științific
Prof. Dr. Cotfas Petru Adrian