Academia de Studii Economice din Bucureşti
Şcoala doctorală Informatică Economică

TEZĂ DE ABILITARE

Utilizarea analizei de securitate pentru a îmbunătăţi soluţiile Internet of Things şi securitatea platformelor mobile şi embedded

Candidat
conf. dr. Marius POPA

Bucureşti 2023

Rezumat

Industria 5.0 schimbă rolul industriei în societate, abordând provocările sociale și de mediu actuale cu prioritate față de abordările tradiționale centrate pe eficiență și productivitate. Conform [8], Industria 5.0 completează versiunea 4.0 prin adăugarea de beneficii pentru angajați și pentru societate conform următoarelor aspecte:

- Creșterea profesionalismului prin abilități evoluate și programe de formare pentru angajați.
- Implementarea modelelor circulare de producție pentru conservarea resurselor naturale.
- Furnizarea de soluții la schimbările climatice.

Pentru a obține beneficiile enumerate mai sus, Industria 5.0 presupune dezvoltarea de programe de cercetare și inovare. Potrivit Comisiei Europene, o Europă digitală este una dintre prioritățile implementării Industriei 5.0, conform [8]. Prin urmare, utilizarea tehnologiilor digitale ar trebui să urmărească:

- Bunăstarea angajaților.
- Îmbunătățirea abilităților digitale ale angajaților.
- Prosperitatea socială.

Majoritatea companiilor sunt încă implicate în industria 4.0. Abordarea Industriei 5.0 este încă la nivel strategic, dar există câteva modalități de a evidenția sau chiar de a demonstra practic cum ar putea arăta acea abordare prin analizarea, investigarea și atingerea aplicațiilor propuse pentru viitoarea industrie.

Utilizarea cunoștințelor și instrumentelor TIC (Tehnologia Informației și a Comunicațiilor) este un element cheie pentru a implementa Industria 5.0. Pandemia COVID-19 a demonstrat rolul tehnologiei digitale în protejarea angajaților și asigurarea continuității afacerii prin intermediul platformelor de lucru și colaborare la distanță. Materializarea beneficiilor Industriei 5.0 va fi posibilă pe baza TIC și a transformărilor digitale care urmează să fie realizate.

Teza conține trei secțiuni având ca subiect principal provocările și soluțiile de securitate TIC în domeniul Internet of Things (IoT), în special pentru a pregăti implementarea următoarei versiuni ale Industriei 5.0:

1. Utilizarea IoT pentru evidenţierea posibilelor aplicații pentru Industria 5.0.
2. Probleme de securitate, provocări și abordări în IoT.
3. Asigurarea calității securității în timpul ciclului de viață de dezvoltare software, în special pentru etapa de implementare a unei aplicaţii securizate.

Elementul comun al acestor trei secțiuni este securitatea abordată în etapele de implementare si mentenanţă ale ingineriei software, cât și la nivel de proiectare pentru diferite arhitecturi și platforme.

Capitolul 2 prezintă mai multe soluții în domeniul Industriei 5.0 ca implementări care vizează aspecte privind poluarea aerului, votul electronic și controlul de la distanță al diferitelor dispozitive sau vehicule. Cunoștințele și instrumentele TIC sunt utilizate pentru a proiecta, dezvolta și implementa soluțiile propuse, precum și rezolvarea problemelor de securitate asociate acestor aplicații. Implementările de securitate iau în considerare ghidurile de implementare existente, cele mai bune practici și standarde pentru a asigura fiabilitatea și robustețea soluțiilor propuse.

Lucrarea [5] se concentrează pe rezolvarea sau atenuarea riscurilor care amenință sănătatea populaţiei legate de poluarea aerului în orașe. Este investigat un posibil sistem de monitorizare a poluării în timp real și este proiectată și implementată un Proof of Concept (PoC) pentru a oferi contramăsuri în timp real bazate pe analize predictive. PoC-ul interpretează și analizează datele colectate din sistemul de monitorizare implementat pe o infrastructură IoT. De asemenea, soluția propusă este integrată cu sistemele existente pentru adoptarea celor mai bune decizii decizii privind reducerea poluării aerului şi aducerea lor în intervalele de siguranță. Astfel, orașele devin inteligente prin comportamentul în timp real adaptat condițiilor de mediu existente.

Contribuțiile autorului cu privire la cercetarea acestui subiect includ următoarele elemente:

- Investigații privind poluarea aerului afectează zonele urbane și populația.
- Investigarea soluțiilor TIC aflate în exploatare şi utilizate pentru atenuarea cauzelor și efectelor poluării aerului.
- Cercetări cu privire la caracteristica „smart city” în contextul poluării aerului.
- Cercetări ale tehnologiilor și platformelor critice care vor fi utilizate pentru dezvoltarea unei soluții bazate pe TIC de monitorizare a poluării.
- Cercetări legate de măsurătorile poluării aerului și modul în care acestea sunt utilizate în cadrul infrastructurii unui oraș inteligent.
- Definirea arhitecturii soluției propuse pe baza tehnologiilor și platformelor actuale și a metricilor vizate care vor fi utilizate pentru analiza calitativă.
- Prelucrarea și interpretarea datelor colectate din exploatarea soluției propuse pentru a utiliza eficient resursele orașului.
- Analiza și interpretarea datelor colectate de la senzori reali implementați și comparații analitice efectuate la momente diferite pentru aceleași surse de date.

Soluția propusă în [7] contribuie la stabilitatea socială, oferind tuturor cetățenilor posibilitatea de a face parte dintr-un model de guvernanță participativă. În plus, acest tip de aplicație este folosit ca suport pentru luarea deciziilor în cadrul diferitelor organizații. Provocările de implementare sunt semnificative în ceea ce privește anonimatul alegătorului și asigurarea securităţii. PoC-ul propus folosește o infrastructură IoT distribuită și descentralizată bazată pe semnături oarbe și tehnologie blockchain pentru a implementa un anumit sistem de vot.

Contribuțiile de cercetare ale autorului vizează următoarele aspecte:

- Analiza sistemelor de vot electronic existente.
- Metodologia de dezvoltare a unei soluții bazate pe TIC pentru vot electronic.
- Analiza schemelor criptografice existente ca fiind cele mai potrivite pentru a fi incluse într-o soluție de vot electronic.

- Proiectarea unor caracteristici funcţionale ale PoC pe baza analizei sistemelor existente.
- Dezvoltarea software a unor mmodule funcţionale ale PoC de vot electronic.
- Validarea PoC prin verificarea funcționalităților, cerințelor de resurse și sincronizarea datelor în componentele PoC atât la nivel hardware, cât și la nivel software.

Utilizarea Inteligenței Artificiale (IA) ca parte a implementării Industriei 5.0 este evidențiată de lucrare [6]. Două PoC-uri sunt dezvoltate pentru a obține beneficiile tehnologiei Machine Learning (ML) utilizată pentru dispozitivele IoT embedded, ca modalitate specială de a proiecta, implementa și implementa Edge ML. Există mai multe constrângeri și limitări cu privire la dispozitivele IoT embedded care trebuie rezolvate atunci când este dezvoltat un sistem bazat pe Edge ML. PoC-urile se referă la următoarele câmpuri de aplicație:

- Robot bazat pe Edge ML operat la distanţă pentru a identifica scurgerile de gaz.
- Vehicule aeriene/drone fără pilot dotate cu inferență de tip Edge ML ce implementează operații de calcul vizual

Dezvoltarea unui astfel de sistem este iterativă și cea mai potrivită versiune este selectată în funcție de performanța prestabilită.

În sfera de aplicare a [6], contribuțiile autorului în cercetarea domeniului sunt legate de:

- Metodologie de aplicare a algoritmilor de machine learning în decizii automate și procese de visual computing dezvoltate în cadrul dispozitivelor încorporate IoT, roboți sau UAV-uri/drone.
- Investigații asupra soluțiilor existente pentru aplicarea IA în cadrul platformelor IoT și UAV.
- Definirea cerințelor pe baza analizei efectuate asupra soluțiilor existente.
- Validarea modelelor de machine learning propuse.
- Analiza performanței modelelor de învățare bazate pe IA.

Capitolul 3 evidențiază diverse soluții de securitate aplicate în infrastructurile de tip IoT. Puterea IoT constă într-un număr mare de dispozitive care rămân conectate permanent. Securitatea în IoT este o mare provocare din cauza numărului foarte mare de dispozitive conectate și a volumelor imense de date trimise prin diferite canale și protocoale de comunicaţii. Dispozitivele IoT folosesc hardware, chipset-uri, sisteme de operare și firmware diferite și diferite protocoale, nivele de comunicare, utilizatori și dezvoltatori care introduc potențiale probleme de securitate. Pe lângă acestea, există încă incertitudine cu privire la cele mai bune practici de securitate și costurile asociate în domeniul IoT. Prin urmare, nu există o soluție de securitate care să se potrivească oricărei implementări IoT, deoarece riscurile de securitate sunt mai puțin cunoscute. Volumele mari de date colectate din infrastructurile IoT şi semantica diversă a acestora oferă îmbunătățiri ale muncii și vieții angajaților.

Lucrarea [1] analizează principalele protocoale de comunicaţie IoT cu infrastructurile Cloud şi potențiale riscuri de securitate. Pe lângă infrastructura IoT în sine, există și alte surse de probleme de securitate, cum ar fi protocoalele de comunicare IoT, Web of Data și accesul la Serviciile Cloud. O implementare necorespunzătoare a infrastructurii IoT va duce la probleme de securitate semnificative în cadrul organizației. Alegerea infrastructurii IoT potrivite împreună cu platformele de procesare asociate este un proces complex, care depinde de resursele financiare alocate

pentru aceasta și de nivelul de securitate vizat. Cunoștințele actuale despre securitatea IoT introduc riscuri potențiale de securitate din cauza unor probleme ascunse sau abordări particulare, chiar dacă infrastructura IoT a fost proiectată și implementată ca fiind una robustă.

Contribuțiile autorului la cercetarea domeniului abordează următoarele aspecte:

- Investigații privind provocările reale de securitate din cadrul unei infrastructuri IoT și riscurile expuse mediului de execuţie de către acest tip de platforme.
- Investigații asupra riscurilor reale de securitate introduse de protocoalele de comunicații utilizate în infrastructurile IoT.
- Abordarea provocărilor de securitate IoT prin alegerea și ajustarea protocoalelor de comunicare adecvate pentru a asigura o securitate minimă vizată într-o infrastructură IoT.
- Analizarea complexității unei infrastructuri IoT ca factor generator de noi provocări de securitate.

Problemele de securitate a plăților și posibilele soluții implementate pentru tranzacțiile financiare sunt prezentate în [3]. Arhitectura și implementarea propuse materializează avantajele în ceea ce privește securitatea plăților prin utilizarea tehnologiilor bazate pe tehnologii Oracle (de exemplu, Java Card) combinate cu standarde robuste și confirmate furnizate de organizații profesionale și comerciale (de exemplu, EMVCo, Global Platform) și tehnologie blockchain implementată pe diferite arhitecturi hardware. Lucrarea abordează provocările de securitate ale implementării sistemului de plată electronică și oferă soluții care să fie aplicate în aplicațiile mobile.

Contribuțiile autorului pentru cercetarea securităţii tranzacțiilor de plată bazate pe carduri inteligente vizează următoarele:

- Investigații asupra sistemelor aflate în exploatare şi bazate pe carduri inteligente având diverse obiective şi fără a fi limitate la plăți.
- Investigații asupra diferitelor tipuri de tranzacții bazate pe carduri inteligente și posibile vulnerabilități de securitate introduse de acestea.
- Analiza modalităților de securizare a tranzacțiilor de plată prin utilizarea diferitelor mecanisme de autentificare a datelor.
- Analizarea robusteței tehnologiilor existente pentru a fi utilizate la dezvoltarea sistemelor bazate pe carduri inteligente.
- Proiectarea și implementarea componentelor pentru un sistem de plată bazat pe carduri inteligente care utilizează tehnologia blockchain.

Un PoC sub formă de aplicație mobilă este prezentat în [11] pentru a evidenția modalități de colectare și utilizare a datelor importante privind activitatea de asigurare prin cercetarea piaței și a implementărilor tehnice. Conținutul implică componente hardware și software specifice industriei auto pentru a fi integrate într-o infrastructură IoT pentru colectarea în timp real a datelor specifice auto. Provocările de securitate sunt semnificative deoarece accesul la datele vehiculului și controlul acestora trebuie limitat doar la părțile autorizate.

Contribuțiile autorului cu privire la cercetarea autovehiculelor conectate (connected cars) vizează următoarele elemente:

- Investigaţii ale monitorizării și comunicării autovehiculului pe baza datelor de localizare.
- Investigații asupra hardware-ului și software-ului existent şi specializat pentru accesul la datele auto.
- Analiza oportunităților tehnice pentru diferite companii de a utiliza datele colectate de la o mașină pentru a optimiza costurile operaționale ale unui parc auto.
- Proiectarea arhitecturii PoC și a componentelor funcționale ale unei aplicații mobile pentru gestionarea datelor auto în cadrul unei infrastructuri IoT Cloud.
- Deschiderea unor noi direcții viitoare de dezvoltare prin adăugarea de componente IA în arhitectura PoC propusă.

Capitolul 4 evidențiază cunoștințele și instrumentele necesare pentru implementarea soluțiilor fiabile și sigure similare celor prezentate în capitolele 2 și 3. O implementare defectuoasă a soluției software este principala cauză a vulnerabilităților provenite din proiectarea soluției, componente hardware și software cu riscuri de securitate, canale de comunicaţie sau dezvoltarea software deficitară din punct de vedere al securităţii. O listă de erori de implementare se transformă în listă de vulnerabilități, deoarece întotdeauna există un actor care urmăreşte să exploateze erorile pentru a obține informații despre software. Capitolul 4 se concentrează pe ingineria software, deoarece calitatea software determină nivelul de securitate software. Standardele de implementare software sigură și principiile dezvoltării software încurajează dezvoltatorii de software să urmeze un set comun de reguli și ghiduri de implementare pentru a îmbunătăți calitatea software. Abordarea calității software operează pe două niveluri:

- Metode și tehnici pentru a avea un proces de inginerie software care să conducă la o calitate înaltă a software.
- Definirea de indicatori pentru a evalua atât procesul de inginerie, cât și calitatea software.

Lucrarea [9] oferă cadrul de definire a unor metrici privind calitatea instrumentelor de dezvoltare sau a containerelor structurate, cum ar fi fișierele de cod sursă. Unele analize sunt efectuate pentru evaluarea ortogonalității pe baza unui sistem de măsurare a ortogonalității. Rezultatele sunt folosite pentru a detecta posibile probleme de codare de securitate sau pentru a îmbunătăți calitatea aplicaţiilor utilitare și a instrumentelor utilizate în timpul ciclului de dezvoltare software.

Contribuțiile autorului la cercetarea pentru dezvoltarea sistemului de evaluare a calității datelor includ:

- Investigații asupra containerelor de stocare a datelor definite ca entități structurate.
- Definirea atributelor de calitate a datelor gestionate ca entități structurate.
- Identificarea caracteristicilor cheie ale metricilor bazate pe agregare incluse în evaluarea ortogonalității entităților structurate.
- Definirea domeniului de aplicare a sistemului de evaluare a ortogonalității în cadrul ciclului de viață al dezvoltării software.
- Definirea indicatorilor de ortogonalitate ale datelor stocate de fișierele de cod sursă ca entități structurate.
- Validarea sistemului de evaluare a ortogonalității prin analiza rezultatelor experimentale prin considerarea a mai multor scenarii.

Dezvoltatorii de software care aplică cele mai bune practici și principiile de implementare software conform cerințelor soluției determină creșterea calității software. Evaluarea și îmbunătățirea abilităților tehnice ale dezvoltatorilor sunt prezentate în [2]. De regulă, un dezvoltator de software mai experimentat adaugă mai multă complexitate și securitate implementării. Provocarea este de a îmbunătăți resursa umană prin transferarea cât mai curând posibil a expertizei dezvoltatorilor mai experimentați către cei începători. Lucrarea prezintă modul în care se realizează această educație de inginerie software pornind de la studiile universitare ale viitorilor specialiști în domeniul TIC.

Contribuțiile autorului la cercetarea impactului existent al Industriei 4.0 asupra transferului de cunoștințe acoperă următoarele aspecte:

- Investigații asupra impactului cunoștințelor și instrumentelor TIC existente asupra educației în domeniul ingineriei software.
- Eșantionarea celor mai relevanți indicatori de cod sursă pentru evaluarea calității codului.
- Definirea sistemului de evaluare a codului sursă prin luarea în considerare a unor constrângeri derivate din particularitățile educației de inginerie software.
- Analiza impactului sistemului de evaluare asupra activităților educaționale efective desfășurate în domeniul TIC.

Lucrarea [10] se concentrează mai mult pe cerințele de securitate ale procesului de dezvoltare software. Dezvoltatorii de software trebuie să fie conștienți și să acorde atenție vulnerabilităților de securitate adăugate accidental pe durata proiectăii soluției şi implementării software. Lucrarea evidențiază cele mai bune practici și principiile de codificare care trebuie aplicate pentru o calitate sporită a securității software. În plus, oferă câteva exemple puncte de pornire în care sunt aplicate astfel de tehnici de proiectare şi implementare.

Contribuțiile de cercetare ale autorului în domeniul securității codului sursă privesc următoarele elemente:

- Investigații asupra cerințelor de securitate pe durata dezvoltării software.
- Analizarea celor mai bune practici actuale privind includerea caracteristicilor de securitate a codului sursă într-o aplicație software.
- Specificarea de vulnerabilități de cod sursă pentru software-ul neconform și metode și tehnici de soluţionare a acestor riscuri de securitate.
- Modalități de îmbunătățire a calității software-ului prin eliminarea vulnerabilităților în timpul ciclului de viață al dezvoltării software.

O viziune mai complexă despre calitatea implementării este prezentată în lucrarea [4]. În implementările reale, setul de tehnologii utilizate este destul de mare și implementarea în cod sursă a soluției trebuie să se adapteze la infrastructura și regulile acelor tehnologii. Arhitectura soluției este eterogenă și diferite componente și tehnologii trebuie sincronizate. O implementare a unui canal de comunicaţie securizat este oferită ca exemplu la nivel industrial.

Contribuțiile autorului la cercetarea calităţii procesului de implementare în cod sursă a cerinţelor unei aplicaţii se evidenţiază astfel:

- Investigații asupra tendințelor TIC actuale în contextul Industriei 4.0.

- Analiza cerințelor Industriei 4.0 pentru a fi implementate într-o soluție IoT pentru o industrie foarte specializată, având abordări informaționale și tehnologice specifice.
- Definirea arhitecturii prototip de soluție IoT cu multiple particularități privind echipamentul tehnic și mediul de producție provocator.
- Specificarea de elemente de securitate soluției propuse pentru a îmbunătăți comunicarea dintre echipamentele fizice de producție și datele specifice producției gestionate de o infrastructură IoT Cloud.
- Definirea metodologiei de securitate cu privire la securitatea soluției împreună cu gestionarea eficientă a datelor legate de activitățile de producție.
- Implementări module funcţionale pentru asigurarea securităţii soluției propuse pentru a dovedi fezabilitatea.

Subiectele de cercetare de mai sus îmbunătățesc abilitățile, experiențele, cunoștințele și procesele în domenii precum educația, cercetarea și inovarea, precum și îmbunătățirea abilităților și competențelor profesionale.

În ceea ce privește domeniul educaţional, transferul tehnologic este îmbunătățit prin actualizarea continuă a temelor de predare, folosind resursele didactice electronice actuale, stimulând feedback-ul elevilor și transparența procesului de predare, activând învățarea și stimulând climatul academic.

Cercetarea, inovarea și transferul de tehnologie implică construirea de relații puternice între diferite echipe cercetare și dezvoltare interdisciplinare pentru a facilita transferul de tehnologie în diferite domenii interesate de aplicarea rezultatelor cercetării. Participarea în programe academice de nivel înalt, precum stagiile de doctorat, asigură creșterea calității resurselor umane domeniul TIC.

Cunoștințele și abilitățile profesionale sunt îmbunătățite prin participarea la programe academice și stagiilor de formare profesională bazate pe curricula în conformitate cu noile tendințe de piață și tehnologii implementate în industria TIC.

Toate elementele de mai sus contribuie la dezvoltarea profesională, asigurând o înaltă calitate a experienței profesionale și a competențelor tehnice așteptate de industria TIC.

Bibliografie

[1] Alin ZAMFIROIU, Bogdan IANCU, Cătălin BOJA, Tiberiu GEORGESCU, Cosmin CARTAS, Marius POPA, Cristian TOMA, *IoT Communication Security Issues for Companies: Challenges, Protocols and The Web of Data*, Proceedings of the International Conference on Business Excellence, Vol. 14, Issue 1, 2020, pp. 1109–1120, WOS 000556549000104, EISSN 2558-9652, https://doi.org/10.2478/picbe-2020-0104

[2] Cătălin BOJA, Mădălina ZURINI, Marius POPA, Cristian TOMA, *Code Quality Metrics Evaluation Platform in Software Engineering Education*, Proceedings of the 16th International Conference on Informatics in Economy (IE 2017), 2017, ASE Publishing House, Bucharest, pp. 283 – 290, WOS 000418463600046, ISSN 2284-7472, ISSN-L 2247-1480

[3] Cristian TOMA, Marius POPA, *EMV/Bitcoin Payment Transactions and Dynamic Data Authentication With Smart Java Cards*, Proceedings of the 14th International Conference on Informatics in Economy (IE 2015) – Section 3: Mobile-Embedded and Multimedia Solutions, 2015, ASE Publishing House, Bucharest, pp. 141 – 151, WOS 000362796900024, ISSN 2284-7472, ISSN-L 2247-1480

[4] Cristian TOMA, Marius POPA, *IoT Security Approaches in Oil & Gas Solution Industry 4.0*, Informatica Economica, Vol. 22, Issue 3, 2018, pp. 46 - 61, ISSN:1453-1305

[5] Cristian TOMA, Marius POPA, Alin ZAMFIROIU, Andrei ALEXANDRU, *IoT Solution for Smart Cities' Pollution Monitoring and the Security Challenges*, Sensors, Vol. 19, Issue 15, 2019, Article Number 3401, WOS 000483198900156, ISSN 1424-8220, https://doi.org/10.3390/s19153401

[6] Cristian TOMA, Marius POPA, Bogdan IANCU, Mihai DOINEA, Andreea PASCU, Filip IOAN-DUTESCU, *Edge Machine Learning for the Automated Decision and Visual Computing of the Robots, IoT Embedded Devices or UAV-Drones*, Electronics, Vol. 11, Issue 21, 2022, Article Number 3507, WOS 000883410100001, EISSN 2079-9292, https://doi.org/10.3390/electronics11213507

[7] Cristian TOMA, Marius POPA, Cătălin BOJA, Cristian CIUREA, Mihai DOINEA, *Secure and Anonymous Voting D-App with IoT Embedded Device Using Blockchain Technology*, Electronics 2022, Vol. 11, Issue 12, Article Number 1895, WOS 000818504700001, EISSN 2079-9292, https://doi.org/10.3390/electronics11121895

[8] Industry 5.0, European Commission, available on-line https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en

[9] Ion IVAN, Daniel MILODIN, Marius POPA, *Orthogonality Metrics of the Structured Entities*, Proceedings of the Romanian Academy, Series A: Mathematics, Physics, Technical Sciences, Information Science, vol. 11, Issue 3, 2010, pp. 269 – 276, WOS 000208624600011, ISSN 1454-9069

[10] Marius POPA, *Security Characteristics of the Program Coding*, Conference Proceedings – The 11th International Conference on Informatics in Economy – Section: Audit and Project Management, 2012, ASE Publishing House, Bucharest, pp. 211 – 215, WOS 000313136800040, ISSN 2284-7472, ISSN-L 2247-1480

[11] Marius POPA, Cosmin CARTAS, *OBD2 IoT Device Proof of Concept for the Insurance Companies Connected Cars*, Proceedings of the 15th International Conference on Informatics in Economy (IE 2016) – Section 2: Mobile-Embedded and Multimedia Solutions, 2016, ASE Publishing House, Bucharest, pp. 103 – 107, WOS 000386192300017, ISSN 2284-7472, ISSN-L 2247-1480