MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___" _____ 2025

PREVENIREA ATACURILOR ASUPRA DISPOZITIVELOR IoT

Proiect de master

Student: _____ **Barajin Simion, SI-231M**

Coordonator: _____ **Alexandru Putere, lect. univ.**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2025

REZUMAT

În era digitală actuală, proliferarea dispozitivelor Internet of Things (IoT) a creat un ecosistem complex și interconectat, aducând atât oportunități remarcabile, cât și provocări semnificative în domeniul securității cibernetice. Această lucrare se concentrează pe explorarea și modelarea atacurilor asupra dispozitivelor IoT prin utilizarea sistemelor neuronale AI și a agenților AI, oferind o perspectivă inovatoare asupra vulnerabilităților și strategiilor de securitate în contextul IoT. Cercetarea abordează problematica din perspectiva dublă a atacatorului și a apărării, utilizând inteligența artificială ca instrument principal pentru simularea, analiza și prevenirea potențialelor amenințări cibernetice. Prin implementarea sistemelor neuronale avansate, studiul analizează patterns-urile complexe ale traficului de date și comportamentul dispozitivelor IoT, permițând identificarea anomaliilor și a potențialelor breșe de securitate înainte ca acestea să fie exploatate în atacuri reale. Agenții AI autonomi sunt utilizați pentru a simula diverse scenarii de atac, testând reziliența sistemelor IoT și identificând punctele vulnerabile care necesită consolidare. Această abordare permite dezvoltarea unor strategii de securitate mai eficiente și adaptabile, capabile să evolueze în paralel cu amenințările emergente. Metodologia cercetării implică crearea unor medii de testare controlate, unde diverse tipuri de dispozitive IoT sunt supuse unei game largi de atacuri simulate, de la simple tentative de compromitere până la scenarii complexe de atac distribuit. Rezultatele acestor simulări sunt analizate utilizând algoritmi avansați de machine learning, permițând identificarea pattern-urilor comune în atacurile reușite și dezvoltarea unor contramăsuri eficiente. Un accent deosebit este pus pe studiul atacurilor care exploatează vulnerabilitățile specifice arhitecturii IoT, cum ar fi resursele limitate ale dispozitivelor, protocoalele de comunicare nesecurizate sau configurațiile implicite slabe. Prin înțelegerea aprofundată a acestor vulnerabilități, cercetarea contribuie la dezvoltarea unor practici de securitate mai robuste și a unor standarde îmbunătățite pentru dispozitivele IoT. Utilizarea sistemelor neuronale AI în modelarea atacurilor permite, de asemenea, predicția și anticiparea unor potențiale vectori de atac care nu au fost încă observați în mediul real, oferind astfel un avantaj proactiv în lupta împotriva amenințărilor cibernetice. Implementarea agenților AI autonomi în acest context deschide noi perspective în testarea automată a securității și în dezvoltarea unor sisteme de apărare adaptive, capabile să răspundă în timp real la amenințările emergente. Rezultatele acestei cercetări au implicații semnificative atât pentru producătorii de dispozitive IoT, cât și pentru experții în securitate cibernetică, oferind insights valoroase pentru îmbunătățirea securității ecosistemului IoT în ansamblu. Prin combinarea expertizei în domeniul IoT cu cele mai recente avansări în inteligența artificială și securitatea cibernetică, această lucrare contribuie la dezvoltarea unor strategii de securitate mai eficiente și la crearea unui internet al lucrurilor mai sigur și mai rezistent la atacuri.

ABSTRACT

In the current digital era, the proliferation of Internet of Things (IoT) devices has created a complex and interconnected ecosystem, bringing both remarkable opportunities and significant challenges in cybersecurity. This research focuses on exploring and modeling attacks on IoT devices using AI neural systems and AI agents, providing an innovative perspective on vulnerabilities and security strategies in the IoT context. The research approaches the issue from both attacker and defense perspectives, using artificial intelligence as the primary tool for simulating, analyzing, and preventing potential cyber threats. Through the implementation of advanced neural systems, the study analyzes complex patterns of data traffic and IoT device behavior, enabling the identification of anomalies and potential security breaches before they are exploited in real attacks. Autonomous AI agents are used to simulate various attack scenarios, testing IoT systems' resilience and identifying vulnerable points requiring reinforcement. This approach enables the development of more efficient and adaptable security strategies capable of evolving alongside emerging threats. The research methodology involves creating controlled testing environments where various IoT devices are subjected to a wide range of simulated attacks, from simple compromise attempts to complex distributed attack scenarios. The results of these simulations are analyzed using advanced machine learning algorithms, allowing the identification of common patterns in successful attacks and the development of effective countermeasures. Special emphasis is placed on studying attacks that exploit IoT architecture-specific vulnerabilities, such as limited device resources, unsecured communication protocols, or weak default configurations. Through deep understanding of these vulnerabilities, the research contributes to developing more robust security practices and improved standards for IoT devices. The use of AI neural systems in attack modeling also allows the prediction and anticipation of potential attack vectors not yet observed in the real environment, thus providing a proactive advantage in the fight against cyber threats. The implementation of autonomous AI agents in this context opens new perspectives in automated security testing and the development of adaptive defense systems capable of responding in real-time to emerging threats. The results of this research have significant implications for both IoT device manufacturers and cybersecurity experts, providing valuable insights for improving the security of the IoT ecosystem as a whole. By combining expertise in IoT with the latest advances in artificial intelligence and cybersecurity, this work contributes to developing more effective security strategies and creating a safer and more attack-resistant Internet of Things.

CUPRINS

INTRODUCERE

În era digitală contemporană, Internet of Things (IoT) a evoluat rapid de la un concept futurist la o realitate omniprezentă, transformând fundamental modul în care interacționăm cu tehnologia în viața de zi cu zi. Odată cu proliferarea dispozitivelor IoT în diverse domenii, de la automatizări domestice la sisteme industriale complexe, securitatea acestor dispozitive a devenit o preocupare crucială. În acest context, emergența și evoluția accelerată a inteligenței artificiale (AI) a deschis noi perspective în consolidarea securității și protecției dispozitivelor IoT.

Această lucrare își propune să exploreze intersecția dinamică dintre IoT, inteligența artificială și securitatea cibernetică, concentrându-se pe dezvoltarea și implementarea sistemelor de protecție bazate pe AI. Cercetarea noastră este motivată de necesitatea crescândă de a fortifica ecosistemul IoT într-un peisaj al amenințărilor cibernetice în continuă evoluție. Prin utilizarea sistemelor neuronale AI și a agenților autonomi, ne propunem să dezvoltăm sisteme sofisticate care pot detecta, analiza și preveni diverse tipuri de amenințări cibernetice.

Relevanța acestui studiu este subliniată de statisticile recente care indică vulnerabilitatea crescândă a dispozitivelor IoT la atacuri cibernetice, cu consecințe potențial devastatoare atât pentru utilizatorii individuali, cât și pentru organizații. În acest context, implementarea sistemelor de securitate bazate pe AI reprezintă o necesitate strategică în dezvoltarea unor măsuri de protecție proactive și eficiente.
Obiectivele principale ale acestei cercetări includ:

- dezvoltarea unor sisteme AI pentru detectarea și prevenirea amenințărilor cibernetice;
- analiza și evaluarea eficacității diferitelor strategii de securitate;
- identificarea și remedierea vulnerabilităților comune în ecosistemul IoT;
- propunerea unor soluții inovatoare pentru îmbunătățirea securității dispozitivelor IoT.

Metodologia noastră combină analiza teoretică aprofundată cu experimente practice într-un mediu controlat, utilizând o varietate de dispozitive IoT și sisteme AI. Prin implementarea unor scenarii de testare a securității, vom evalua eficacitatea sistemelor AI în îmbunătățirea mecanismelor de apărare.

Structura lucrării reflectă abordarea noastră sistematică, începând cu o analiză comprehensivă a domeniului securității IoT, continuând cu prezentarea detaliată a metodologiilor de protecție și a experimentelor realizate, și culminând cu o discuție asupra implicațiilor etice și a direcțiilor viitoare în securitatea IoT. Contribuția originală a acestei lucrări constă în dezvoltarea unor sisteme AI inovatoare pentru protecția dispozitivelor IoT, precum și în propunerea unor strategii de securitate adaptative. Prin combinarea expertizei în domeniul IoT cu cele mai recente avansări în inteligența artificială, această lucrare își propune să aducă o contribuție semnificativă la îmbunătățirea securității în ecosistemul IoT.

BIBLIOGRAFIE

[1]K. Dhondge, *Lifecycle IoT Security for Engineers*. [Online]. Available: https://thomasu.on.worldcat.org/search/detail/1286429132?queryString=iot%20security&clusterResults=true&groupVariantRecords=false. Accessed: Sep. 2, 2024.

[2] M. Liyanage, P. Kumar, and M. Ylianttila, *IoT Security: Advances in Authentication*. [Online]. Available: https://thomasu.on.worldcat.org/search/detail/1195817311?queryString=iot%20security&clusterResults=true&groupVariantRecords=false. Accessed: Sep. 5, 2024.

[3] J. Matherly, *Shodan Exploits Methods*. [Online]. Available: https://developer.shodan.io/api/exploits/rest. Accessed: Sep. 2, 2024.

[4] Censys, *Search Language*. [Online]. Available: https://search.censys.io/search/language?resource=hosts. Accessed: Oct. 13, 2024.

[5] ZoomEye, *API Reference*. [Online]. Available: https://www.zoomeye.org/doc?channel=api. Accessed: Nov. 8, 2024.

[6] OpenVAS, *Greenbone Cloud Service – Manual*. [Online]. Available: https://docs.greenbone.net/GCS-Manual/gcs/en/. Accessed: Sep. 20, 2024.

[7] Metasploit, *Running Modules, Module Documentation*. [Online]. Available: https://docs.metasploit.com/docs/using-metasploit/basics/. Accessed: Aug. 9, 2024.

[8] Burp Suite, *Burp Suite Documentation*. [Online]. Available: https://portswigger.net/burp/documentation. Accessed: Oct. 11, 2024.

[9] OWASP, *Zed Attack Proxy (ZAP): Getting Started, Security Testing Basics*. [Online]. Available: https://www.zaproxy.org/getting-started/#security-testing-basics. Accessed: Nov. 19, 2024.

[10] Kali Linux, *Introduction, Kali Tools*. [Online]. Available: https://www.kali.org/docs/tools/kali-tools/. Accessed: Nov. 11, 2024.

[11] Nmap, *Nmap Network Scanning*. [Online]. Available: https://nmap.org/docs.html. Accessed: Oct. 16, 2024.

[12] Wireshark, *TCP/IP Deep Dive Analysis with Wireshark*. [Online]. Available: https://nmap.org/docs.html. Accessed: Nov. 17, 2024.

[13] S. Pal, V. G. Diaz, and D.-N. Le, *IoT Security and Privacy Paradigm*. [Online]. Available: https://thomasu.on.worldcat.org/search/detail/1289822338?queryString=iot%20security&clusterResults=true&groupVariantRecords=false. Accessed: Oct. 3, 2024.

[14] N. Jaswal, *Mastering Metasploit: Take Your Penetration Testing and IT Security Skills to a Whole New Level with the Secrets of Metasploit*. [Online]. Available: