

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

**Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice**

**Admis la susținere
Șefă departament TSE:
Tîrșu Valentina, conf. univ., dr.**

20 ianarie 2025

**CERCETAREA METODELOR ȘI
MIJLOACELOR AVANSATE DE PROTECȚIE A
DATELOR ȘI ACCES ÎN SISTEMELE IOT**

Teză de master

Student:

**Tîrnovan Cristian
gr. SISRC-231M**

Conducător:

**Șestacova Tatiana
conf. univ., dr.**

Chișinău, 2025

REZUMAT

Autorul: Tîrnovan Cristian gr. SISRC-231M

Tema: Cercetarea metodelor și mijloacelor avansate de protecție a datelor și acces în sistemele IoT

Structura lucrării: Lucrarea este compusă din pagini de titlu, aviz, rezumat, introducere, 3 capitole, concluzii și bibliografie.

Cuvinte cheie: securitatea IoT, criptografie avansată, autentificare multifactorială, standarde de securitate, acces controlat.

Problematica studiului: Tema explorează problemele legate de securitatea datelor și controlul accesului în sistemele IoT, evidențiind provocările generate de interconectivitatea și diversitatea dispozitivelor. Lucrarea analizează punctele slabe ale sistemelor existente și propune soluții inovatoare pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor.

Scopul lucrării: Studiarea și analiza metodelor și mijloacelor moderne de protecție a datelor și acces în sistemele IoT, cu accent pe integrarea criptografiei avansate, autentificării multifactoriale și arhitecturilor de securitate scalabile, capabile să contracareze amenințările cibernetice emergente.

Obiectivele tezei:

1. Analiza problemelor de securitate a datelor și acces în sistemele IoT pentru a identifica punctele slabe și soluțiile implementate.
2. Cercetarea tendințelor actuale în domeniul securității IoT, inclusiv atacurile cibernetice emergente și metodele de prevenire.
3. Elaborarea și evaluarea propunerii de soluții de securitate care să răspundă nevoilor specifice ale aplicațiilor IoT.
4. Crearea și realizarea unei aplicații pentru criptarea și decriptarea în securitatea IoT.
5. Elaborarea unei aplicații client server pentru securitatea accesului în sistemelor IoT.

Metode aplicate: În cadrul lucrării au fost utilizate metode analitice pentru identificarea problemelor de securitate, metode experimentale pentru dezvoltarea și testarea prototipurilor de soluții, precum și metode comparative pentru evaluarea performanței și eficienței acestora.

Rezultatele obținute: Lucrarea analizează metode avansate de protecție, precum criptografia end-to-end (E2EE) și algoritmul Tiny Encryption Algorithm (TEA), aplicate în sistemele IoT. Printr-un prototip, s-a demonstrat implementarea unei soluții de securitate care integrează criptografia avansată și autentificarea cu tokenuri. Studiul a evaluat impactul criptografiei asupra performanței rețelelor IoT și a oferit strategii pentru optimizarea securității fără a compromite scalabilitatea.

SUMMARY

Author: Tîrnovan Cristian, group SISRC-231M

Topic: Research on advanced methods and means for data and access protection in IoT systems

Structure of the paper: The paper consists of a title page, endorsement, abstract, introduction, three chapters, conclusions, and bibliography.

Keywords: IoT security, advanced cryptography, multi-factor authentication, security standards, access control.

Research problem: The topic addresses issues related to data security and access control in IoT systems, highlighting the challenges posed by the interconnectivity and diversity of devices. The paper analyzes vulnerabilities in existing systems and proposes innovative solutions to ensure data confidentiality, integrity, and availability.

Purpose of the paper: To study and analyze modern methods and means for data protection and access control in IoT systems, focusing on the integration of advanced cryptography, multi-factor authentication, and scalable security architectures capable of countering emerging cyber threats.

Thesis Objectives:

1. Analyze data security and access issues in IoT systems to identify vulnerabilities and implemented solutions.
2. Research current trends in IoT security, including emerging cyber-attacks and prevention methods.
3. Develop and evaluate proposed security solutions tailored to the specific needs of IoT applications.
4. Design and implement an application for encryption and decryption in IoT security.
5. Develop a client-server application for security and access in IoT systems.

Methods applied: The study employed analytical methods to identify security issues, experimental methods to develop and test solution prototypes, and comparative methods to assess the performance and efficiency of these solutions.

Results obtained: The study analyzes advanced protection methods such as end-to-end encryption (E2EE) and the Tiny Encryption Algorithm (TEA), applied in IoT systems. Through a prototype, the implementation of a security solution integrating advanced encryption and token-based authentication was demonstrated. The study evaluated the impact of encryption on IoT network performance and proposed strategies to optimize security without compromising scalability.

CUPRINS

INTRODUCERE	7
1 ANALIZA PROBLEMELOR DE SECURITATE DATELOR SI ACCES IN SISTEME IOT	8
1.1 Modele de structură pentru sisteme IOT	8
1.1.1 Dispozitive IoT, Controlere și Periferice	10
1.2 Provocarile securității IoT	14
1.3 Analiza metodelor si mijloacelor pentru asigurarea securitatii elementelor IoT.....	15
2 CERCETAREA MIJLOACELOR AVANSATE ÎN PROTECTIA SISTEMELOR IoT.....	18
2.1 Mijloacele avansate pentru protejarea sistemelor IoT	18
2.2 Metode de securizare.....	20
2.2.1 Criptografia pentru protecția datelor.....	21
2.2.2 Autentificarea și controlul accesului.....	22
2.3 Securizarea comunicațiilor	22
2.3.1 Utilizarea Blockchain în Securitatea IoT	23
2.3.2 Aplicații ale Blockchain în Securitatea IoT.....	24
2.3.3 Modele de implementare a securității avansate în dispozitive IoT	27
3 PROPUNERI DE SOLUȚII ȘI IMPLEMENTĂRI PENTRU SECURITATEA DATELOR ȘI CONTROLUL ACCESULUI ÎN IOT	30
3.1 Dezvoltarea unei soluții pentru protecția datelor și acces în IoT	30
3.2 Testarea și evaluarea performanțelor soluției propuse.....	38
3.2.1 Studii de caz pentru implementări reale în sistemele IoT.....	39
3.3 Crearea unei aplicatii Python pentru criptarea datelor end-to-end în IoT	40
3.4 Realizarea unei aplicații pentru criptare și decriptare utilizată în securitatea IoT	45
3.5 Elaborarea unei aplicații client server pentru securitatea și accesul în IoT	54
CONCLUZII	59
BIBLIOGRAFIE	61

INTRODUCERE

În contextul evoluției rapide a tehnologiilor digitale, Internetul Lucrurilor (IoT) a devenit un pilon fundamental în transformarea modului în care interacționăm cu mediul înconjurător. Cu toate acestea, pe măsură ce numărul dispozitivelor conectate crește exponențial, securitatea acestora devine o preocupare majoră. Actualitatea temei acestei lucrări de master se regăsește în necesitatea stringentă de a aborda provocările legate de securizarea IoT, având în vedere vulnerabilitățile care pot fi exploatare de atacatori și impactul potențial asupra utilizatorilor și infrastructurii critice. Internet of Things (IoT) este o rețea de obiecte fizice care conțin electronice încorporate în arhitectura lor pentru a comunica și a simți interacțiunile între ele sau cu mediul extern. În următorii ani, tehnologia bazată pe IoT va oferi niveluri avansate de servicii și va schimba practic modul în care oamenii își duc viața de zi cu zi. Progresele în medicină, inginerie, business, agricultură, orașe inteligente și case inteligente sunt doar câteva dintre exemplele categorice în care IoT este puternic stabilit. Cu alte cuvinte IoT este conectarea oricărui dispozitiv (de la telefoane mobile, vehicule, electrocasnice și alte elemente încorporate cu senzori și actuatori) cu Internetul, astfel încât aceste obiecte să poată schimba date între ele într-o rețea. Este interesant de menționat faptul că diferența între IoT și Internet, este absența rolului uman. Dispozitivele IoT pot crea informații despre comportamentele individuale, pot analiza și acționa .

Scopul tezei de master constă în cercetarea metodelor și mijloacelor avansate de protecție a datelor și acces în sistemele IoT cerceta și de a prelucra datele necesare pentru a dezvolta soluții eficiente de securizare a ecosistemului IoT. Aceasta implică nu doar o înțelegere aprofundată a tehnologiilor existente, ci și explorarea unor metode inovatoare de protecție care să asigure integritatea, confidențialitatea și disponibilitatea informațiilor în acest spațiu interconectat.

Obiectivele tezei:

1. Analiza problemelor de securitate a datelor și acces în sistemele IoT pentru a identifica punctele slabe și soluțiile implementate.
2. Cercetarea tendințelor actuale în domeniul securității IoT, inclusiv atacurile cibernetice emergente și metodele de prevenire.
3. Elaborarea și evoluarea propuneri de soluții de securitate care să răspundă nevoilor specifice ale aplicațiilor Io
4. Crearea și realizarea unei aplicații pentru criptarea și decriptare în securitatea IoT
5. Elaborarea unei aplicații client server pentru securitatea și accesul în IoT sistemelor IoT.

Prin abordarea acestor obiective, lucrarea își propune să contribuie semnificativ la dezvoltarea unor soluții sustenabile care să asigure un mediu IoT mai sigur, protejând astfel utilizatorii și infrastructurile critice de amenințările în atacuri cibernetice.

BIBLIOGRAFIE

1. Bădițoiu, Ioana. Raport de cercetare Semestrul II. Disponibil online:[file:///C:/Users/criss/Downloads/Ioana_Baditoiu_Raport_cercetare_Sem_II%20\(1\).pdf](file:///C:/Users/criss/Downloads/Ioana_Baditoiu_Raport_cercetare_Sem_II%20(1).pdf)
Actualizat: 12 ianuarie 2022.
2. Basic Concepts of IoT. Disponibil online:
[file:///C:/Users/criss/Downloads/Ioana_Baditoiu_Raport_cercetare_Sem_II%20\(1\).pdf](file:///C:/Users/criss/Downloads/Ioana_Baditoiu_Raport_cercetare_Sem_II%20(1).pdf).
Actualizat: 5 februarie 2021.
3. Internet of Things: Arhitectura, Tehnologii, Securitate, Confidențialitate și Aplicații. ResearchGate. Disponibil online:
https://www.researchgate.net/publication/337195882_Internet_of_Things_Arhitectura_Tehnologii_Securitate_Confidentialitate_si_Aplicatii . Actualizat: 15 noiembrie 2021.
4. Chapter 1: Introduction to Internet of Things. Medium. Disponibil online: <https://medium.com/iot-with-raspberry-pi/chapter-1-introduction-to-internet-of-things-c8c459f4f961> . Actualizat: 18 aprilie 2022.
5. How Big is the IoT Market? The Wired Shopper. Disponibil online:
<https://thewiredshopper.com/how-big-is-the-iot-market/> . Actualizat: 10 mai 2023.
6. Ernst & Young. The Future of IoT. Disponibil online:
[https://www.ey.com/Publication/vwLUAssets/EY_-_Future_of_IoT/\\$FILE/EY-future-of-iot.pdf](https://www.ey.com/Publication/vwLUAssets/EY_-_Future_of_IoT/$FILE/EY-future-of-iot.pdf) .
Actualizat: 27 iunie 2023.
7. International Telecommunication Union (ITU). ITU-T Y.2060: Overview of the Internet of Things. Geneva, 2012. Disponibil online: <https://www.itu.int/rec/T-REC-Y.2060-201206-I/en> . Actualizat: 12 august 2023.
8. NIST. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. National Institute of Standards and Technology. Disponibil online:
<https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8228.pdf> . Actualizat: 5 septembrie 2023.
9. Cisco. IoT Networking: Transforming Industries and Business. Disponibil online:
<https://www.cisco.com/site/us/en/solutions/networking/industrial-iot/index.html> . Actualizat: 8 noiembrie 2023.
10. ISO/IEC. 27001: Information Security Management Standards. Disponibil online:
<https://www.iso.org/standard/27001> . Actualizat: 22 decembrie 2022.
11. European Telecommunications Standards Institute (ETSI). ETSI EN 303 645: Cyber Security for Consumer Internet of Things. Disponibil online: [Link](#) chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf. Actualizat: 10 ianuarie 2023.

12. Accenture. The IoT Revolution and its Security Implications. Disponibil online: [Link](#). Actualizat: 25 februarie 2023.
13. Microsoft Azure. IoT Security Solutions. Disponibil online: <https://www.accenture.com/us-en/insights/internet-of-things> . Actualizat: 30 martie 2023.
14. TÎRȘU, V., CRISTEA E. Baze de date : Ghid metodic pentru lucrările de laborator. Chișinău: Ed. “Tehnica-UTM”, 2024, 112 pag. ISBN 978-9975-64-392-4. Disponibil: <https://library.utm.md/items/?biblionumber=2628876>
15. TÎRȘU, V. Programare : Ghid metodic pentru lucrări de laborator. Chișinău: Ed. “Tehnica-UTM”, 2022, pag.130, ISBN 978-9975-45-861-0. Disponibil: <https://library.utm.md/items/?biblionumber=2619626>
16. SAVA, L., VORTOLOMEI, D. Organizarea și analiza activității economice în domeniul telecomunicațiilor. Note de curs, Chișinău, Editura UTM, 2022, ISBN: 978-9975-45-805-4.
17. TÎRȘU V., CERBU O. Interactive visualization of geographical data using proxmox and modern technologies. In: The scientific heritage. Economic Sciences., Vol.1 № 142 (142), 2024, p.21-26. Budapest, Hungary. ISSN 9215 — 0365, Cosmos Impact Factor - 3.336 SJIF Impact Factor - 5.78 DOI: , Categoria B+. Disponibil: <http://www.scientific-heritage.com/ru/arhiv/>
18. GUL, F., TUDOSE, D., ȚURCANU, T. A Versatile IoT Development Board for Environmental Sensing and Biometric Applications. In: 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet). 19-20 September, 2024, Bucharest, Romania. <https://ieeexplore.ieee.org/document/10722601>