MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Electronică şi Telecomunicaţii

Departamentul Telecomunicații și Sisteme Electronice

Admis la susţinere

Şefă departament TSE:

V. Tîrșu dr., conf. univ.

„___” _____ 2025

Elaborarea soluțiilor de securitate inteligente bazate pe internetul obiectelor (IoT)

Student: **Cupcinenco Eugeniu, SISRC-231M**

Conducător: **Dorogan Andrei. dr., lect., univ**

Chișinău 2025

REZUMAT

La teza de master

Tema : „Elaborarea soluțiilor de securitate inteligente bazate pe internetul obiectelor (IoT)”

Actualitatea și importanța temei - este important de a avea o metodă sigură de securizare, având în vedere creșterea continuă a numărului de dispositive IOT conectate la internet care sunt inevitabile în diferite sfere ale vieții, volumul de date interceptat poate prezenta pericol și amenințărare cibernetică tot mai complexă. Într-un context global digitalizat, tema „ Soluții de securitate inteligente bazate pe internetul obiectelor ” rămâne esențială pentru a asigura securitatea informațiilor pe dispozitivele IOT și continuitatea operării cu aceste dispozitive. Implementarea unor soluții moderne și proactive nu este doar o necesitate tehnologică, ci și o obligație socială și economică care va spori folosirea dispozitivelor IOT.

Cuvinte cheie: Dispozitive IOT, Raspberry Pi, Raspbian, VPN, Securitate cibernetică

Scopul tezei – este identificarea, analiza și propunerea unor soluții eficiente pentru securitatea internetului obiectelor și a unor dispositive a acestora, având ca obiectiv principal asigurarea unui nivel ridicat de securitate, confidențialitate și protecție împotriva accesului neautorizat prin aplicarea diferitor metode de securizare.

Obiective specifice sunt**:**

Analiza generală a securizării dispozitivelor IOT:

Studiul amănunțit a nivelului de securizare

Evaluarea actualității a produselor pe piață

Proiectarea și testarea unor noi soluții de securizare eficientă

Implementarea unui plan de securizare a dispozitivului

Testarea planului de securizare propus

Scopul și obiectivele tezei sunt orientate către dezvoltarea unui cadru teoretic și practic care să contribuie la îmbunătățirea securității rețelelor pentru dispozitivele IOT, având în vedere tendințele actuale în domeniul cibernetic.

Semnificația și valoarea aplicativă constă în :

Analizarea metodelor de securizare a minicomputerului Raspberry Pi pentru evidențierea punctelor forte și slabe datorită cărora este posibil îmbunătățirea securității rețelei și securității de control acces la datele stocate.

SUMMARY

Master thesis

Theme : "Developing smart security solutions based on the Internet of Things (IoT)"

Topicality and importance of the theme - it is important to have a secure method of securization, given the continuous increase in the number of IOT devices connected to the internet that are inevitable in different spheres of life, the volume of intercepted data can present danger and increasingly complex cyber threat. In a digitized global context, the topic of "Smart security solutions based on the Internet of Things" remains essential to ensure information security on IOT devices and continuity of operation with these devices. Implementing modern and proactive solutions is not only a technological necessity, but also a social and economic obligation that will increase the use of IOT devices.

Keywords: IOT devices, Raspberry Pi, Raspbian, VPN, Cybersecurity

The aim of the thesis - is to identify, analyze and propose effective solutions for the security of the Internet of Things and their devices, with the main objective to ensure a high level of security, privacy and protection against unauthorized access by applying different security methods.

Specific objectives are:

General analysis of securization of IOT devices:

Thorough study of the level of securization

Assessment of the state of the art of products on the market

Design and test new effective securization solutions

Implement a plan to secure the device

Testing the proposed security plan

The aims and objectives of the thesis are oriented towards developing a theoretical and practical framework to help improve network security for IOT devices, taking into account current trends in the cyber domain.

The significance and applicative value consists in :

Analyzing the methods for securing the Raspberry Pi minicomputer in order to highlight the strengths and weaknesses due to which it is possible to improve the network security and access control security to the stored data.

Cuprins

Introducere

1. Analiza tendințelor moderne a dispozitivelor IOT

Securitatea în cadrul Internetului Lucrurilor (IoT)

Internetul Lucrurilor (IoT) desemnează o rețea vastă de dispozitive inteligente conectate, capabile să comunice și să partajeze date pentru a simplifica și îmbunătăți aspecte ale vieții moderne. De la locuințe inteligente și dispozitive purtabile până la aplicații industriale avansate, tehnologia IoT redefinește modul în care interacționăm cu lumea digitală.

Totuși, această dezvoltare rapidă aduce în prim-plan provocări majore legate de securitate. Dispozitivele IoT, deși inovatoare, pot fi expuse atacurilor cibernetice care amenință confidențialitatea datelor, integritatea sistemelor și funcționarea optimă a acestora. Printre riscurile frecvent întâlnite se numără lipsa unor standarde unitare de securitate, actualizările insuficiente ale software-ului și protecția deficitară a datelor.

Pentru a preveni astfel de vulnerabilități, securitatea în domeniul IoT necesită implementarea unor măsuri de protecție solide, precum criptarea datelor, autentificarea multi-factor și segmentarea rețelelor. Un ecosistem IoT securizat presupune protejarea tuturor componentelor implicate – dispozitive, rețele de comunicare și platforme de stocare a datelor. Deoarece fiecare dispozitiv conectat poate reprezenta un potențial punct de acces pentru atacatori, abordarea securității trebuie să fie una complexă și continuă, acoperind toate etapele: de la proiectarea inițială, până la mentenanța pe termen lung, prin actualizări de securitate constante.Un obstacol semnificativ îl constituie diversitatea dispozitivelor IoT și absența unei standardizări globale în materie de securitate, ceea ce complică implementarea unor politici unitare de protecție. În special, dispozitivele mai vechi sau de calitate inferioară pot prezenta riscuri ridicate din cauza parolelor implicite slabe sau lipsei criptării datelor. Pe lângă riscurile tehnice, factorul uman joacă, de asemenea, un rol esențial. Utilizarea unor parole nesigure, ignorarea actualizărilor de securitate sau lipsa cunoștințelor despre protecția datelor pot amplifica expunerea la amenințări cibernetice. Prin urmare, educarea utilizatorilor și dezvoltarea unor interfețe prietenoase, care să simplifice adoptarea bunelor practici de securitate, sunt esențiale.

Această lucrare analizează importanța securității dispozitivelor IoT, principalele amenințări cibernetice și soluțiile moderne necesare pentru protejarea dispozitivelor și datelor într-un ecosistem tehnologic în continuă expansiune.

Scopul și Obiectivele

Scopul principal al dispozitivelor IoT (Internet of Things) este de a crea un ecosistem interconectat de dispozitive care să comunice între ele și să proceseze informații în timp real pentru a îmbunătăți viața cotidiană și a eficientiza procesele din diferite domenii. Aceste dispozitive urmăresc să automatizeze sarcinile zilnice, să optimizeze consumul de resurse, să îmbunătățească confortul, securitatea și performanța în industrie și alte sectoare. Prin conectarea diferitelor obiecte la internet, IoT permite controlul, monitorizarea și analiza acestora de la distanță, facilitând astfel gestionarea eficientă a mediului înconjurător.

Obiective specifice ale dispozitivelor IoT

1. Automatizarea proceselor
2. Monitorizare și control de la distanță
3. Actualizarea sistemului
4. Implementarea metodelor noi de securizare a dispozitivului
5. Testarea metodelor noi de securizare a dispozitivului

Bibliografie:

1. *Securitatea in aplicatii de Internet-of-Things (IoT)* © 2011[citat 08.10.2024]. Disponibil: https://www.electrokits.ro/securitatea-in-aplicatii-de-internet-of-things-iot/

2. Edgar Weippl, Shishir K. Shandilya, Soon Ae Chun. *Internet of Things Security Fundamentals, Techniques and Applications.* [citat 08.10.2024]. ISBN: 9788793609532

3. *SAP* [citat 08.10.2024] Disponibil: https://www.sap.com/romania/products/artificial-intelligence/what-is-iot.html

4. J. Paulo Davim, Vicente García Díaz, Vijender Kumar Solanki. *Handbook of IoT and Big Data.* [citat 08.10.2024]. ISBN: 9780429624490

5. *Securitatea cibernetică IoT pentru consumator* [citat 08.10.2024] Disponibil: https://www.sgs.com/ro-md/services/securitatea-cibernetica-iot-pentru-consumatori

6. Raspberry Pi Documentation [citat 11.11.2024] Disponibil: https://www.raspberrypi.com/documentation/computers/getting-started.html

7. Statement of Compliance (SoC) [citat 16.11.2024] Disponibil: https://pip.raspberrypi.com/categories/1004-cyber-security

8. How to Run a Raspberry Pi in VirtualBox [citat 16.11.2024] Disponibil: https://www.howtogeek.com/run-a-raspberry-pi-in-virtualbox/?fbclid=IwY2xjawGufpVleHRuA2FlbQIxMAABHVJoDSa6Iq_oqwx4qjXqZ-guv4ZCfO4PjbM_RRVK4aRlL7wDszOm6jPSog_aem_6NRvWz-xB7B0TYnT7arxWw

9. What is a Raspberry Pi? [citat 12.11.2024] Disponibil: https://opensource.com/resources/raspberry-pi

10. How to Configure the Firewall in Raspberry Pi [citat 02.01.2025] https://www.sunfounder.com/blogs/news/how-to-configure-the-firewall-in-raspberry-pi

11. IoT- Etapa urmatoare a evolutiei [citat 06.01.2025] https://www.roweb.ro/ro/blog/iot-eteapa-urmatoare-a-evolutiei/

12. Industrial Internet of Things (IIoT) [citat 12.23.2024] https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot

13. Revolutionizing Remote Monitoring: The Internet of Things (IoT) in Action [citat 08.01.2025] https://iotbusinessnews.com/2023/11/08/66040-revolutionizing-remote-monitoring-the-internet-of-things-iot-in-action/

14. IoT – Avantaje și dezavantaje [citat 08.01.2025] https://revicon.ro/iot-avantaje-si-dezavantaje/

15. Ce înseamnă backup [citat 08.01.2025] https://techcafe.ro/how-to/ce-inseamna-backup-de-ce-este-bine-sa-l-faci/

16. Tîrșu V., Sava L. Integrating elasticsearch and kibana in ict management *processes for economic efficiency in multimedia content administration.* In: The scientific heritage. Economic Sciences., Vol.1 № 142 (142), 2024, p.15-20 . 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/

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. Sava L., Tîrșu V., Plămădeală C. *Performance evaluation of microtik routers according to electromagnetic compatibility testing standards.* În: Electrotehnica, Electronica, Automatica, vol.72/4, p.57-61. Romania, Sibiu: ISSN: 2392-828X, categoria B+. Disponibil: https://eea-journal.ro/articles-and-issues/current-issues/

19. 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

20. 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

21. 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

22. Sava, L., Vortolomei, D. Organizarea şi analiza activităţii economice în domeniul telecomunicaţiilor. Note de curs, Chişinău, Editura UTM, 2022, ISBN: 978-9975-45-805-4.