

Ministerul Educației și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice

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

„___” _____ **2025**

Elaborarea unui sistem de autentificare a utilizatorilor
cu aplicarea metodelor de securitate moderne

Teză de master

Student: _____ **Carcevschi Ion, SISRC-231M**
Conducător: _____ **DOROGAN Andrei, lec.univ., dr.**

Chișinău, 2025

Rezumat

Tema:Elaborarea unui sistem de autentificare a utilizatorilor cu aplicarea metodelor de securitate moderne

Componența lucrării:Capitolul 1 Practica de documentare,Capitolul 2 Elaborarea unui sistem de autentificare a utilizatorilor cu aplicarea metodelor de securitate moderne,Capitolul 3 Analiza economică

Cuvinte cheie:Autentificare,Securitate,Biometrie,RFID.

Obiectivele Studiului

Analiza metodelor tradiționale de autentificare și identificarea vulnerabilităților acestora. Evaluarea tehnologiilor moderne precum autentificarea fără parolă și soluțiile bazate pe biometrie. Implementarea unui prototip funcțional și testarea acestuia pentru validarea eficienței sistemului propus.

Metode Moderne de Autentificare

Biometria: autentificare prin recunoaștere facială, amprentă sau scanare oculară. Autentificare cu doi factori (2FA): combinarea parolei cu un cod generat sau primit pe un dispozitiv. Autentificare fără parolă: utilizarea dispozitivelor de încredere pentru acces.

Soluția Propusă

Prototip Tehnic: Integrarea unui sistem de autentificare bazat pe RFID și scanarea amprentelor. Platformă: Dezvoltarea unui sistem robust utilizând plăci Arduino Pro Micro, biblioteci software și module de securitate pentru gestionarea autentificării și autorizării utilizatorilor.

Analiza Riscurilor și Beneficiilor

Riscuri: depășirea bugetului, integrarea dificilă cu sisteme existente și rezistența la schimbare din partea utilizatorilor. Beneficii: reducerea costurilor operaționale, îmbunătățirea securității și creșterea încrederii utilizatorilor.

Testarea și Evaluarea

Realizarea de teste de securitate pentru verificarea rezistenței la atacuri cibernetice. Validarea performanței prin simulări și măsurarea timpilor de răspuns.

Concluzii

Implementarea unui sistem de autentificare modern contribuie semnificativ la protecția datelor și la reducerea riscurilor de securitate cibernetică. Soluțiile propuse susțin o infrastructură mai sigură și eficientă pentru utilizatori, promovând adoptarea unor tehnologii inovatoare în domeniul securității informatice.

Adnotation

Title: Development of a User Authentication System Using Modern Security Methods

Content Structure: Chapter 1: Documentation Practice Chapter 2: Development of a User Authentication System Using Modern Security Methods Chapter 3: Economic Analysis

Keywords: Authentication, Security, Biometrics, RFID.

Study Objectives: Analyze traditional authentication methods and identify their vulnerabilities. Evaluate modern technologies such as passwordless authentication and biometric-based solutions. Implement a functional prototype and conduct testing to validate the system's efficiency.

Modern Authentication Methods: Biometrics: Authentication through facial recognition, fingerprint scanning, or iris scanning. Two-Factor Authentication (2FA): Combining a password with a generated or received code on a device. Passwordless Authentication: Using trusted devices for access.

Proposed Solution: Technical Prototype: Integration of an authentication system based on RFID and fingerprint scanning. Platform: Development of a robust system using Arduino Pro Micro boards, software libraries, and security modules for managing user authentication and authorization.

Risk and Benefit Analysis: **Risks:** Budget overruns, difficult integration with existing systems, and resistance to change from users. **Benefits:** Reduced operational costs, improved security, and increased user trust.

Testing and Evaluation: Conducting security tests to assess resistance to cyberattacks. Validating performance through simulations and response time measurements.

Conclusions: Implementing a modern authentication system significantly contributes to data protection and reduces cybersecurity risks. The proposed solutions support a safer and more efficient infrastructure for users, promoting the adoption of innovative technologies in information security.

Cuprins

1. Concepte teoretice privind practica de documentare	
Introducere.....	8
1.1 Tendințe moderne de dezvoltare a sistemelor de autentificare, actualitatea temei.....	9
1.2 Metodelor de modelare/simulare a problemelor tehnice, de operare, management și mentenanță în securitate cibernetică.....	16
1.3 Soluții ingineresti moderne de dezvoltare a teoriei și tehnicii în domeniul securității cibernetică.....	17
1.4 Algoritmul de realizare a tezei de master.....	18
2. Elaborarea unui sistem de autentificare a utilizatorilor cu aplicarea metodelor de securitate moderne.	
2.1 Securitatea informației, zone de aplicare, vulnerabilități, soluții.....	19
2.2 Metode utilizate în analiza sistemului de autentificare.....	22
2.3 Metode utilizate în proiectarea sistemului.....	24
2.4 Structura software.....	25
2.5 Mecanismul de autentificare bazat pe amprentă și componenta RFID.....	28
2.6 Integrarea autentificării bazate pe RFID și biometrie într-un sistem de tip Zero Trust.....	29
2.7 Funcționarea mecanismului de autentificare biometrică.....	32
2.8 Aplicații și frecvențe utilizate.....	37
2.9 Securitatea Locală vs. Cloud.....	38
2.10 Utilizarea securității avansate pentru acces într-o clădire de birouri.....	42
2.11 Utilizarea tag-urilor RFID în industrie.....	46
2.12 Riscuri și vulnerabilități RFID.....	48
2.13 Protecția împotriva clonării sau interceptării datelor RFID.....	48
2.14 Tehnologii de prevenire a accesului neautorizat (IDS/IPS).....	49
3. Analiza economică	
3.1 Costuri pentru realizarea proiectului.....	52
3.2 Beneficii economice.....	55
3.3 Analiza riscurilor.....	57
Concluzii.....	59
Biografie.....	60

Introducere

Securitatea cibernetică este un domeniu al securității care se ocupă cu protejarea sistemelor informatice, rețelelor și datelor împotriva accesului neautorizat, a utilizării frauduloase, a distrugerii sau a modificărilor neautorizate. Acesta implică implementarea unor măsuri tehnice, procedurale și organizatorice pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor și a resurselor digitale. Practic, securitatea cibernetică acoperă o gamă largă de activități și tehnologii, inclusiv protecția împotriva atacurilor ciberneticе, precum malware-ul, phishing-ul, hacking-ul și alte amenințări digitale. Aceasta poate implica utilizarea de firewall-uri, programe antivirus, criptare, autentificare multifactorială, monitorizare a activității rețelei.

Scop și obiective

Scopul:

Dezvoltarea unui sistem de autentificare sigur, eficient și modern, care utilizează metode avansate de securitate pentru a proteja datele și identitatea utilizatorilor în fața amenințărilor ciberneticе contemporane.

Obiective:

a) Analiza metodelor tradiționale de autentificare:

Examinarea vulnerabilităților asociate cu autentificarea prin parole și identificarea limitărilor acestora în contextul amenințărilor moderne.

b) Studiul metodelor moderne de autentificare:

Investigarea tehnologiilor emergente de autentificare, cum ar fi autentificarea multifactorială (MFA), autentificarea biometrică, soluțiile fără parolă (passwordless) și tokenizarea.

c) Evaluarea standardelor și reglementărilor de securitate:

Analiza conformității cu reglementări de securitate, cum ar fi GDPR și alte standarde internaționale, pentru a asigura protecția datelor utilizatorilor.

d) Conceperea și implementarea prototipului:

Elaborarea unui prototip funcțional al sistemului de autentificare, integrând metodele moderne de securitate identificate în etapa de cercetare.

e) Testarea și evaluarea sistemului:

Realizarea testelor de securitate și performanță pentru a verifica eficiența sistemului în prevenirea atacurilor ciberneticе și în protejarea datelor utilizatorilor.

f) Propunerea de îmbunătățiri și ajustări:

Formularea unor recomandări pentru optimizarea securității și a experienței de utilizare în sistemul de autentificare dezvoltat.

Biografie

- [1] Rao, U.H., Nayak, U., The InfoSec Handbook. An introduction to information security, New York, Apress, pp.51-53, 2014, ISBN 978-1-4302-6383-8.
- [2] <https://www.microsoft.com/ro-ro/security/business/security-101/what-is-authentication>
- [3] <https://moldova.europalibera.org/a/sute-de-atacuri-cibernetice-asupra-institutiilor-statului-si-conturi-guvernamentale-de-e-mail-compromise/33018577.html>
- [4] Crihan, G., Crăciun, M., Dumitriu, L., An efficient hybrid authentication mechanism based on fingerprint recognition, RFID and homomorphic encryption, International Journal of Modeling and Optimization, vol.14, no. 2, pp.69-75, 2024, ISSN 2010-3697
- [5] <https://developer.orange.com/resources/openid-connect-1-0/>
- [6] <https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/>
- [7] https://www.smartsan.ro/blog/articole/tehnologia-rfid/?srsltid=AfmBOopQb3bFenjiI__JyYltKimBvz4PqbVA9qw_GgGZmTFYba2JH85g
- [8] <https://expertaccounts.com/blog/cloud-computing/romana/Securitatea-datelor-%E2%80%93-server-local-vs.-cloud-computing/>
- [9] 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/>
- [10] 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/>
- [11] 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/>
- [12] 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>
- [13] 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.