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.

_____

„____” _____ 2026

ANALIZA ȘI DEZVOLTAREA COMPONENTELOR SERVER ALE SISTEMULUI DE AUTENTIFICARE CU DOI FACTORI

Proiect de master

Student: _____ **Curcubet Ecaterina, TI-241M**

Coordonator: _____ **Ludmila Peca, lect univ.**

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

Chişinău, 2026

REZUMAT

Lucrarea de față abordează analiza, proiectarea și dezvoltarea componentelor server ale unui sistem de autentificare cu doi factori (2FA), cu accent pe creșterea nivelului de securitate al proceselor de autentificare în aplicațiile moderne. Teza este structurată în mai multe capitole, fiecare tratând aspecte teoretice sau practice necesare fundamentării și implementării soluției propuse.

Primul capitol prezintă noțiunile generale privind autentificarea și securitatea informației, descriind principiile procesului de verificare a identității utilizatorilor, rolul factorilor de autentificare și limitele sistemelor tradiționale bazate pe un singur factor.

Capitolul al doilea analizează soluțiile existente de autentificare cu doi factori, incluzând OTP prin e-mail și SMS, TOTP generat prin aplicații mobile, precum și instrumente și biblioteci open-source utilizate în industrie. Sunt comparate avantajele și limitările fiecărei metode, iar la final este identificată soluția optimă pentru implementarea sistemului.

Capitolul al treilea introduce conceptul de autentificare adaptivă bazată pe risc, evidențiind principiile și mecanismele de evaluare a riscului, precum și avantajele și limitările acesteia față de soluțiile tradiționale. Această abordare permite solicitarea codului 2FA doar în situațiile în care nivelul de risc depășește pragul prestabilit, optimizând experiența utilizatorului fără a compromite securitatea.

Capitolul al patrulea este dedicat analizei și definirii arhitecturii server-side, incluzând cerințele funcționale și nefuncționale, modelul arhitectural, structura componentelor backend, precum și modelarea bazei de date. Capitolul al cincilea detaliază dezvoltarea componentelor server, incluzând implementarea modulelor pentru TOTP, structura endpoint-urilor API, integrarea cu aplicația client și testarea funcționalităților TOTP și 2FA adaptiv. Testarea a demonstrat corectitudinea, securitatea și performanța sistemului, evidențiind eficiența autentificării adaptive în reducerea interacțiunilor inutile și păstrarea unui nivel ridicat de protecție. Rezultatele obținute confirmă faptul că sistemul poate gestiona autentificări multiple simultan, aplică măsuri anti-abuz și respectă standardele de securitate. Lucrarea se încheie cu concluzii privind eficiența și aplicabilitatea soluției propuse, evidențiind contribuțiile realizate, limitele identificate și direcțiile de dezvoltare viitoare. Studiul demonstrează că un sistem de autentificare cu doi factori, integrat cu mecanism adaptiv bazat pe risc, nu doar că reduce semnificativ riscurile de securitate, dar oferă și o soluție scalabilă, ușor de integrat și adaptabilă la diverse aplicații moderne. Prin combinarea analizei teoretice cu dezvoltarea practică, lucrarea oferă o perspectivă completă asupra construirii unui mecanism modern și sigur de protecție a identității digitale, confirmând relevanța metodei 2FA în contextul actual al amenințărilor cibernetice sofisticate.

ABSTRACT

This thesis addresses the analysis, design, and development of the server components of a two-factor authentication (2FA) system, with a focus on enhancing the security level of authentication processes in modern applications. The thesis is structured into multiple chapters, each covering theoretical or practical aspects necessary for the foundation and implementation of the proposed solution.

The first chapter presents general concepts regarding authentication and information security, describing the principles of the user identity verification process, the role of authentication factors, and the limitations of traditional single-factor systems.

The second chapter analyzes existing two-factor authentication solutions, including OTP via email and SMS, TOTP generated through mobile applications, as well as open-source tools and libraries used in the industry. The advantages and limitations of each method are compared, and finally, the optimal solution for system implementation is identified.

The third chapter introduces the concept of risk-based adaptive authentication, highlighting its principles and risk evaluation mechanisms, as well as its advantages and limitations compared to traditional solutions. This approach allows the 2FA code to be requested only in situations where the risk level exceeds a predefined threshold, optimizing the user experience without compromising security.

The fourth chapter is dedicated to the analysis and definition of the server-side architecture, including the functional and non-functional requirements, the proposed architectural model, the structure of backend components, and the database modeling. The fifth chapter details the development of server components, including the implementation of TOTP modules, the structure of API endpoints, integration with the client application, and testing of TOTP and adaptive 2FA functionalities. Testing demonstrated the correctness, security, and performance of the system, highlighting the efficiency of adaptive authentication in reducing unnecessary interactions while maintaining a high level of protection. The results confirm that the system can handle multiple simultaneous authentications, implements anti-abuse measures, and complies with security standards. The thesis concludes with findings regarding the efficiency and applicability of the proposed solution, highlighting the contributions made, identified limitations, and future development directions. The study demonstrates that a two-factor authentication system, integrated with a risk-based adaptive mechanism, not only significantly reduces security risks but also provides a scalable, easily integrable, and adaptable solution for various modern applications. By combining theoretical analysis with practical development, the thesis offers a comprehensive perspective on building a modern and secure identity protection mechanism, confirming the relevance of the 2FA method in the current context of increasingly sophisticated cyber threats.

CUPRINS

INTRODUCERE

În era digitală actuală, securitatea informațiilor reprezintă una dintre cele mai importante preocupări în dezvoltarea aplicațiilor software. Volumul tot mai mare de date sensibile stocate și procesate în mediul online, precum și creșterea numărului de atacuri cibernetice, impun necesitatea adoptării unor mecanisme avansate de protecție a identității utilizatorilor. În acest context, autentificarea utilizatorilor devine un proces esențial pentru asigurarea integrității, confidențialității și disponibilității datelor.
Autentificarea clasică, bazată pe un singur factor – de obicei, combinația nume de utilizator și parolă – nu mai oferă un nivel suficient de protecție.

Autentificarea cu doi factori adaugă un nivel suplimentar de securitate prin combinarea a două elemente diferite de identificare: ceva ce utilizatorul știe (parola), ceva ce deține (telefon, token, aplicație mobilă) sau ceva ce este (amprentă, recunoaștere facială). În acest mod, compromiterea unui singur factor nu este suficientă pentru a obține accesul la contul utilizatorului, reducând considerabil riscul accesului neautorizat. Tema prezentei teze de master – „Proiectarea și implementarea unui sistem de autentificare cu doi factori (2FA) pentru aplicații web” – abordează această problemă actuală și propune realizarea unei soluții software sigure, scalabile și ușor de integrat în aplicații existente. Sistemul va permite autentificarea clasică a utilizatorilor, urmată de o verificare suplimentară printr-un cod unic generat temporar (TOTP) sau transmis printr-un canal securizat. Scopul principal al lucrării constă în proiectarea și implementarea unui mecanism modern de autentificare care să ofere un nivel crescut de protecție a datelor utilizatorilor și să reducă riscurile asociate atacurilor de tip phishing, brute-force sau credential stuffing. Pentru atingerea acestui scop, au fost stabilite următoarele obiective:

- analiza metodelor și tehnologiilor actuale de autentificare;
- studierea principiilor de funcționare a mecanismelor 2FA;
- proiectarea unei arhitecturi software care integrează 2FA în fluxul de autentificare;
- implementarea unei aplicații web care să demonstreze funcționalitatea sistemului propus;
- testarea și validarea soluției din punct de vedere al securității și al experienței utilizatorului.

Metodologia de cercetare utilizată se bazează pe analiza comparativă a soluțiilor existente, proiectarea arhitecturii propuse, implementarea practică a unui prototip funcțional și evaluarea performanței acestuia în condiții reale de utilizare. Lucrarea îmbină aspecte teoretice privind securitatea informatică cu aplicarea practică a conceptelor moderne de autentificare.

BIBLIOGRAFIE

1. „Confidentiality, Integrity, and Availability: The CIA Triad | Office of Information Security | Washington University in St. Louis”. Data accesării: 24 noiembrie 2025. [Online]. Disponibil la: https://informationsecurity.wustl.edu/guidance/confidentiality-integrity-and-availability-the-cia-triad/
2. A. Chiruță, „Atacurile Brute Force: Metode Eficiente de Protecție și Prevenire”, cyberFolks.ro. Data accesării: 24 noiembrie 2025. [Online]. Disponibil la: https://cyberfolks.ro/blog/atacurile-brute-force-metode-eficiente-de-protectie-si-prevenire/
3. „Care este diferența dintre Single Sign-On (SSO) și Active Directory?”, Webex Help Center. Data accesării: 24 noiembrie 2025. [Online]. Disponibil la: https://help.webex.com/article/WBX63960/What-is-the-Difference-Between-Single-Sign-On-(SSO)-and-Active-Directory
4. „What is ISO27001? Understanding Its Role in GDPR and PCI-DSS Compliance - Vorago Security Ltd”. Data accesării: 24 noiembrie 2025. [Online]. Disponibil la: https://www.voragosecurity.com/blog-posts/what-is-iso27001
5. J. Coutinho, „What is TOTP and why do you need it?” Data accesării: 24 noiembrie 2025. [Online]. Disponibil la: https://supertokens.com/blog/totp-why-you-need-it-and-how-it-works
6. „Multi-Factor Authentication”, RSD. Data accesării: 24 noiembrie 2025. [Online]. Disponibil la: https://www.rsd.md/mfa/
7. „Two-Factor vs Adaptive Authentication: Which Is Better? - The LastPass Blog”. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://blog.lastpass.com/posts/two-factor-vs-adaptive-authentication-which-is-better
8. K. Singh, „Two Factor Authentication Pros and Cons: 2FA Benefits & Risks”, LoginRadius. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://www.loginradius.com/blog/identity/2fa-benefits-risks
9. „Adaptive Multi-Factor Authentication (MFA)”, CyberArk. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://www.cyberark.com/what-is/adaptive-mfa/
10. „Ce este autentificarea cu doi factori (2FA)?”, Tree Web Solutions. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://treewebsolutions.com//ro/articole/ce-este-autentificarea-cu-doi-factori-2fa-17
11. „What Do OTP, TOTP, and HOTP Mean?”, NordPass. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://nordpass.com/blog/otp-totp-hotp/
12. „Base32 vs Base64 : A Comprehensive Comparison”. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://mojoauth.com/compare-binary-encoding/base32-vs-base64/
13. „Auth.js | Authentication for the Web”. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://authjs.dev/
14. „Backend modules — TYPO3 Explained main documentation”. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://docs.typo3.org/m/typo3/reference-coreapi/main/en-us/ExtensionArchitecture/HowTo/BackendModule/Index.html
15. „What Is an API (Application Programming Interface)? | IBM”. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://www.ibm.com/think/topics/api
16. „2-Factor Authentication OTP: TOTP & HOTP Algorithms”, DEV Community. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://dev.to/dmitrevnik/build-your-own-authenticator-totp-vs-hotp-explained-2315
17. H. G. Limited, „Autentificarea cu doi factori (2FA): De ce ar trebui să o folosești pentru fiecare cont - Hostragons®”. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://www.hostragons.com/ro/blog/de-ce-sa-folositi-autentificarea-cu-doi-factori-2fa/
18. „Postman: The World’s Leading API Platform | Sign Up for Free”. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://www.postman.com/

19. L. Peca, S. Cojocaru, M. Dumitraşcu, and D. Ţurcanu, “EVALUATION OF CYBERSECURITY TRAINING PERCEPTIONS, ADOPTED PRACTICES AND STRATEGIC DIRECTIONS FOR CAPACITY BUILDING”, *J. Eng. Sci.*, vol. 32, no. 3, pp. 75–90, Nov. 2025.
20. ISTRATI, Daniela. *Metode de optimizare și interfețe în organizarea sistemelor de producție*. 2023. PhD Thesis. Universitatea Tehnică a Moldovei. https://repository.utm.md/handle/5014/25886.
21. O. Mangos, V. Rachier, S. Cojocaru, G. Bunescu and C. Rusu, "Web Platform for Wind Potential Assessment in the Republic of Moldova," *2025 International Conference on Electromechanical and Energy Systems (SIELMEN)*, Iasi, Romania, 2025, pp. 308-313, doi: 10.1109/SIELMEN67352.2025.11260662.
22. COJOCARU, Svetlana, PECA, Ludmila. Challenges and solutions on the use of Artificial Intelligence in Internet of Things network security. In: *Electronics, Communications and Computing: IC ECCO 2024*, Ed. 13, 17-18 octombrie 2024, Chișinău. Chișinău: „Tehnica-UTM”, 2024, Editia 13, pp. 120-121. ISBN (pdf) 978-9975-64-480-8 (PDF).
23. BOLUN, Ion, COJOCARU, Svetlana. A Differentiated Beneficiary Cybersecurity Approach. In: *Electronics, Communications and Computing*, Ed. 12, 20-21 octombrie 2022, Chișinău. Chișinău: „Tehnica-UTM”, 2023, Editia 12, pp. 115-118. ISBN (pdf) 978-9975-45-898-6 (PDF).
24. BRANIȘTE, Rodica, ISTRATI, Daniela, GOGOI, Elena. La qualite de l’eau : metodes et modeles numerique de recherche. In: *Conferința tehnico-științifică a studenților, masteranzilor și doctoranzilor*, 29-31 martie 2022, Chișinău. Chișinău, Republica Moldova: „Tehnica-UTM”, 2022, Vol.1, pp. 432-436. ISBN 978-9975-45-828-3.. ISBN (pdf) 978-9975-45-829-0 (Vol. I) (PDF)..
25. DUCA, Ludmila, COJUHARI, Irina, CIORBĂ, Dumitru, COJOCARU, Svetlana. Limbaje formale și automate finite: Ghid pentru lecțiile practice. Universitatea Tehnică a Moldovei, Facultatea Calculatoare, Informatică și Microelectronică, Departamentul Ingineria Software și Automatică. Chișinău: Tehnica-UTM, 2024. 128 p. ISBN 978-9975-64-381-8.
26. PECA, Ludmila, TSURCANU, Dinu. Reducing cyber risk through a human–centred approach. In: *Journal of Engineering Science*, 2025, vol. 32, nr. 1, pp. 18-31. ISSN 2587-3474. DOI: https://doi.org/10.52326/jes.utm.2025.32(1).02
27. Țurcanu, D., Peca, L., Prisacaru, A., & Țurcanu, T. (2025). CYBER SECURITY PROFESSIONAL DEVELOPMENT WITHIN CYBERCOR. *JOURNAL OF ENGINEERING SCIENCE*, *32*(2), 87–98. https://doi.org/10.52326/jes.utm.2025.32(2).08
28. PECA, Ludmila, ȚURCANU, Dinu. Network security: Practical examples solved to be introduced in network security. [Practical Guide]. Fac. of Computers, Informatics and Microelectronics, Dep. Software Engineering and Automatics: Tehnica UTM, 2023, 243 p. ISBN 978-9975-45-941-9.
29. POȘTARU, ANDREI. Экспериментальный метод и программные средства для исследования динамического пове дения трибосистем скольжения. In: Электронная обработка материалов, 2024, vol. 60, nr. 2, pp. 74-86. ISSN 0013-5739. DOI: https://doi.org/10.52577/eom.2024.60.2.74 https://ibn.idsi.md/ro/vizualizare_articol/206975
30. M. Chiper, D. Stanescu, T. Becheru and L. Peca, "Adversarial Attacks for Scripts," *2025 24th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Chisinau, Moldova, Republic of, 2025, pp. 1-7, doi: 10.1109/RoEduNet68395.2025.11208410.
31. ISTRATI, Daniela. Influența factorilor fundamentali în sistemele de producție. In: *Conferința tehnico-științifică a studenților, masteranzilor și doctoranzilor*, 29-31 martie 2022, Chișinău. Chișinău, Republica Moldova: „Tehnica-UTM”, 2022, Vol.1, pp. 442-445. ISBN 978-9975-45-828-3.. ISBN (pdf) 978-9975-45-829-0 (Vol. I) (PDF).
32. Leahu, A., Andrievschi-Bagrin, V., Ciorbă, D., Fiodorov, I. (2025). On Dynamic Probabilistic Models in Network Reliability. In: Hoskova-Mayerova, S., Flaut, C., Flaut, D., Rackova, P. (eds) Changes and Innovations in Social Systems. Studies in Systems, Decision and Control, vol 505. Springer, Cham. https://doi.org/10.1007/978-3-031-43506-5_5

33. POȘTARU, GHEORGHE; STOICEV, PETRU; POȘTARU, ANDREI; BODNARIUC, ION; BUGA, ALEXANDRU; PLATON, ANDREI. Determination of the tribotechnical characteristics of the materials used for precessional transmissions design. In: Acta Technica Napocensis - Series: Applied Mathematics, Mechanics, and Engineering, 2024, vol. 67, supl. nr. 2, pp. 577-584. ISSN 1221-5872.
34. S. -F. Ion, C. Carabas, N. Ţăpuş and D. Ciorbă, "Enhancing Blockchain Performance via Unikraft: A Case Study of Implementation and Scalability Analysis on MultiversX," *2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, Romania, 2024, pp. 1-8, doi: 10.1109/RoEduNet64292.2024.10722595.
35. ISTRATI, Daniela, CALMÎCOV, Igor, MORARU, Vasile, ZAPOROJAN, Sergiu. Interfaces dans l'organisation des systemes de production. In: *Intellectus*, 2023, nr. 2, pp. 145-154. ISSN 1810-7079. DOI: https://doi.org/10.56329/1810-7087.23.2.16
36. L. Alexei, R. Maria, D. Ciorbă and F. Ion, "Geometric distributions MinMax and MaxMin modified as lifetime distributions and statistical estimators for them," *2025 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, Chisinau, Moldova, Republic of, 2025, pp. 1-5, doi: 10.1109/BlackSeaCom65655.2025.11193904.
37. PLĂMĂDEALĂ, Maxim, BALAMATIUC, Eduard, NEGAI, Marin, FIȘTIC, Cristofor, CIORBĂ, Dumitru. Enhancing machine learning model performance through data augmentation techniques across varied dataset sizes. In: *Conferinţa tehnico-ştiinţifică a studenţilor, masteranzilor şi doctoranzilor*, 27-29 martie 2024, Chișinău. Chișinău, Republica Moldova: „Tehnica-UTM", 2024, Vol.2, pp. 855-860. ISBN 978 9975-64-460-0. ISBN (pdf) 978-9975-64-458-7 (Vol.2).
38. DUCA, Ludmila, ZAPOROJAN, Sergiu, ISTRATI, Daniela, MUNTEAN, Nicolae. Effectiveness of Artificial Intelligence Integration in ERP Systems for Fitness Centers. In: *Electronics, Communications and Computing: IC ECCO 2024*, Ed. 13, 17-18 octombrie 2024, Chișinău. Chișinău: „Tehnica-UTM", 2024, Editia 13, pp. 188-189. ISBN (pdf) 978-9975-64-480-8 (PDF).
39. ALEXEI, Arina. SYSTEMIC SECURITY FRAMEWORK FOR HEI'S. In: Scientific and Practical Cyber Security Journal (SPCSJ), Vol 8(2), 2024, pp. 59–67. ISSN 2587-4667.
40. Arina, Alexei, Ion Bolun, and Anatolie Alexei. "Cybersecurity challenges in healthcare: mitigating risks in a rapidly evolving digital landscape." Bulletin of Electrical Engineering and Informatics 14.6 (2025): 4867-4875.
41. BOLUN, I, ALEXEI, A. Aspecte de securizare a rețelelor și sistemelor informatice biomedicale. In: ECONOMICA, vol.4, numărul 160, 2024, pag.60-75. DOI: 10.53486/econ.2024.130.060.
42. Alexei, A., Moraru, V., & Alexei, A. (2025). SECURING MOLDOVAN SMALL AND MEDIUM-SIZED BUSINESSES: STRATEGIES BASED ON IT INFRASTRUCTURE DOMAINS. In: JOURNAL OF ENGINEERING SCIENCE, 32(2), 75–86. https://doi.org/10.52326/jes.utm.2025.32(2).07.
43. ISTRATI, Daniela. Temperature capture and image processing system: a case study .... In: *Journal of Engineering Science*, 2022, vol. 29, nr. 2, pp. 108-115. ISSN 2587-3474. DOI: https://doi.org/10.52326/jes.utm.2022.29(2).10
44. ALEXEI, A., PLATON, N., BOLUN, I., ALEXEI, An. Smart and digital healthcare. Advanced technologies and security issues. In: CEEeGov: Central and Eastern European eDem and eGov Days, Budapest, Hungary, September 2024. ACM, New York, NY, USA, 7 Pages. DOI: https://doi.org/10.1145/3670243.3673857.
45. Alexei, A., Alexei, A. (2025). Towards More Protected Medical Data: Assessing the Security of Web and Email Infrastructures in SMEs in the Republic of Moldova. In: Sontea, V., Tiginyanu, I., Railean, S. (eds) 7th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2025. IFMBE Proceedings, vol 135. Springer, Cham. https://doi.org/10.1007/978-3-032-06497-4_31.
46. POȘTARU, ANDREI. Experimental Method and Software Instruments for Sliding Tribosystem Dynamic Behavior Research. In: Surface Engineering and Applied

Electrochemistry. 2024, vol. 60, Issue 5, pp 706-716, ISSN: 1068-3755
DOI: https://doi.org/10.3103/S1068375524700297
47. BOSTAN, ION; STOICEV, PETRU; POŞTARU, GHEORGHE; BUGA, ALEXANDRU; BODNARIUC, ION; POŞTARU, ANDREI; PLATON, ANDREI. Particularities of tribological behavior of the contact elements of the precessional gear, made of metallic and plastic materials. In: International Journal of Modern Manufacturing Technologies, 2023, vol. 15, pp. 16-27. ISSN 2067-3604. DOI: https://doi.org/10.54684/ijmmt.2023.15.3.16 https://ibn.idsi.md/ro/vizualizare_articol/194562
48. ISTRATI, Daniela, CALMÎCOV, Igor, MORARU, Vasile, ZAPOROJAN, Sergiu. Development of an Employee Scheduling Application Under Consecutive Days-off Constraints. In: *Electronics, Communications and Computing: IC ECCO 2024*, Ed. 13, 17-18 octombrie 2024, Chişinău. Chișinău: „Tehnica-UTM", 2024, Editia 13, pp. 178-179. ISBN (pdf) 978-9975-64-480-8 (PDF).
49. DUCA, Ludmila, ZAPOROJAN, Sergiu, ISTRATI, Daniela. ERP system implementation in companies. In: *Electronics, Communications and Computing: IC ECCO 2024*, Ed. 13, 17-18 octombrie 2024, Chișinău. Chișinău: „Tehnica-UTM", 2024, Editia 13, pp. 169-170. ISBN (pdf) 978-9975-64-480-8 (PDF).
50. ISTRATI, Daniela. A Brief Overview of Intelligent Interfaces in Production Systems. In: *Electronics, Communications and Computing*, Ed. 12, 20-21 octombrie 2022, Chișinău. Chișinău: „Tehnica-UTM", 2023, Editia 12, pp. 158-161. ISBN (pdf) 978-9975-45-898-6 (PDF).