Ministerul Educaţiei și Cercetarii al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Informatică și Ingineria Sistemelor

Admis la susţinere
Şeful departamentului IIS: conf. univ., dr. V. Sudacevschi
_____
„__”_____ 2023_

STUDIUL SOLUȚIILOR DE SECURITATE IOT

Teză de master

Masterand:_____(Bîrsan Valeriu)
Conducător: _____(Moraru Victor conf.univ.,dr.)

Chişinău – 2023

Adnotare

Internetul Obiectelor (IoT) este esențial în conectarea dispozitivelor fizice și virtuale dotate cu tehnologii avansate pentru schimbul de date la nivel global. Acesta oferă numeroase beneficii, dar, în același timp, prezintă riscuri legate de securitatea datelor. Se așteaptă ca până în 2030 să existe peste 25 de miliarde de dispozitive IoT, sporind astfel vulnerabilitatea la atacuri și utilizări inadecvate, accentuate de lipsa criptării în majoritatea traficului IoT. Pentru a asigura o implementare sigură, este esențială dezvoltarea unor soluții cuprinzătoare de securitate, confidențialitate și autentificare. Studiul de față explorează taxonomia securității și amenințărilor în domeniul IoT, subliniind importanța unei arhitecturi bine definite și discutând diversele standarde, protocoale și metode de mitigare a riscurilor. Se propune folosirea tehnologiilor emergente precum Blockchain, Fog Computing, Edge Computing și Machine Learning pentru a îmbunătăți securitatea dispozitivelor IoT și a adresa provocările în acest domeniu.

În plus, este crucială adoptarea unui cadru legislativ robust și actualizat care să reglementeze utilizarea tehnologiilor IoT, stabilind astfel standarde clare pentru producători și utilizatori. Aceasta va contribui nu doar la protecția datelor și a intimității, ci și la promovarea unei utilizări responsabile și etice a IoT. În acest mod, se poate asigura că progresul tehnologic merge mână în mână cu securitatea și binele societății.

Cuvinte cheie: Internetul lucrurilor; securitate; amenințări; confidențialitate; vulnerabilități.

Adnotation

The Internet of Things (IoT) is essential in connecting physical and virtual devices equipped with advanced technologies for global data exchange. It offers many benefits, but at the same time, it poses data security risks. It is expected that by 2030 there will be more than 25 billion IoT devices, increasing vulnerability to attacks and misuse, exacerbated by the lack of encryption in most IoT traffic. To ensure secure deployment, it is essential to develop comprehensive security, privacy and authentication solutions. This study explores the taxonomy of IoT security and threats, highlighting the importance of a well-defined architecture and discussing various standards, protocols and risk mitigation methods. It proposes the use of emerging technologies such as Blockchain, Fog Computing, Edge Computing and Machine Learning to improve the security of IoT devices and address IoT challenges.

In addition, it is crucial to adopt a robust and up-to-date legislative framework regulating the use of IoT technologies, thus setting clear standards for manufacturers and users. This will not only help to protect data and privacy, but also to promote responsible and ethical use of IoT. This can ensure that technological progress goes hand in hand with security and the good of society.

Keywords: Internet of Things; security; threats; privacy; vulnerabilities.

CUPRINS

INTRODUCERE

Securitatea în cadrul Internet of Things (IoT) reprezintă un ansamblu de abordări și practici destinate să ofere protecție dispozitivelor fizice, rețelelor, proceselor și tehnologiilor implicate în mediul IoT împotriva unui spectru extins de amenințări de securitate. Securitatea IoT reprezintă familia de tehnici, strategii și instrumente folosite pentru a asigura integritatea și confidențialitatea acestor dispozitive, protejându-le de posibile compromisuri. Cu o notă ironică, caracteristica fundamentală a IoT [1], și anume conectivitatea sa extinsă, crește parțial vulnerabilitatea acestor dispozitive la atacuri cibernetice.

Datorită diversității și complexității ecosistemului IoT, conceptul de securitate se extinde și mai mult. Acest fapt a condus la dezvoltarea unei game variate de metodologii și practici pentru a asigura securitatea IoT. Acestea includ securitatea interfeței de programare a aplicațiilor (API), autentificarea infrastructurii cu chei publice (PKI) și măsuri de protecție a rețelelor, doar pentru a menționa câteva dintre tehnicile pe care specialiștii din domeniul IT le pot implementa pentru a contracara amenințările din ce în ce mai sofisticate ale criminalității cibernetice și ale atacurilor cibernetice asociate dispozitivelor IoT vulnerabile [2].

În conformitate cu un raport de cercetare efectuat de Gartner, se estimează că până în 2025, vor fi în funcțiune aproximativ 50 de miliarde de dispozitive conectate și senzori în întreaga lume. Aceste dispozitive și senzori fac parte din rețeaua IoT și au potențialul de a aduce beneficii semnificative, dar și provocări semnificative în ceea ce privește securitatea.

Această proliferare a dispozitivelor și senzorilor IoT pune în evidență importanța securității în acest domeniu. Cu fiecare dispozitiv adăugat la rețeaua IoT, suprafața de atac potențială crește, ceea ce face ca securitatea să fie o prioritate critică. În absența măsurilor adecvate de securitate, dispozitivele IoT pot deveni vulnerabile la diverse amenințări, inclusiv accesul neautorizat, interceptarea datelor, manipularea sau chiar controlul dispozitivelor [2] de către părțile terțe.

Prin urmare, studiul soluțiilor de securitate pentru IoT este esențial pentru a proteja integritatea și confidențialitatea datelor, precum și pentru a asigura funcționarea corespunzătoare a acestor dispozitive într-un mediu interconectat. Această cercetare se concentrează pe identificarea, evaluarea și compararea diferitelor abordări și tehnologii de securitate disponibile pentru a ajuta organizațiile și comunitatea de cercetare să ia decizii informate în ceea ce privește implementarea soluțiilor de securitate adecvate pentru dispozitivele lor IoT.

BIBLIOGRAFIE

1. K. Chen *et al.*, „Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice”, *J Hardw Syst Secur*, vol. 2, nr. 2, pp. 97–110, iun. 2018, doi: 10.1007/s41635-017-0029-7.

2. M. Mămăligă, „ANALIZA RISCURILOR ȘI AMENINȚĂRILOR DE SECURITATE ALE DISPOZITIVELOR IoT”, 2022.

3. P. Williams, I. K. Dutta, H. Daoud, și M. Bayoumi, „A survey on security in internet of things with a focus on the impact of emerging technologies”, *Internet of Things*, vol. 19, p. 100564, aug. 2022, doi: 10.1016/j.iot.2022.100564.

4. P. K. Sadhu, V. P. Yanambaka, și A. Abdelgawad, „Internet of Things: Security and Solutions Survey”, *Sensors*, vol. 22, nr. 19, p. 7433, sep. 2022, doi: 10.3390/s22197433.

5. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, și B. Sikdar, „A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures”, *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

6. „CE ESTE MQTT?” [Online]. Disponibil la: https://www.automatizari-scada.ro/conectivitate-iot/ce-este-mqtt/#:~:text=MQTT%20(Message%20Queue%20Telemetry%20Transport,publicare%20si%20abonare%22%20(%22publish [citat 30.11.2023].

7. „What is CoAP? Understanding the Constrained Application Protocol”. [Online]. Disponibil la: https://www.radware.com/security/ddos-knowledge-center/ddospedia/coap/ [citat 12.12.2023].

8. S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. B. Sri- vastava, “On communication security in wireless ad-hoc sensor networks,” in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE Inter- national Workshops on*. IEEE, 2002, pp. 139–144.

9. G. Bere, B. Ahn, J. J. Ochoa, T. Kim, A. A. Hadi, and J. Choi, ‘‘Blockchainbased firmware security check and recovery for smart inverters,’’ in Proc. IEEE Appl. Power Electron. Conf. Expo. (APEC), Phoenix, AZ, USA, Jun. 2021, pp. 675–679.

10. James Howell, „An Introduction To IoT Architecture”. [Online]. Disponibil la: https://101blockchains.com/iot-architecture/ [citat 24.12.2023].

11. M. Cagalj, S. Capkun, and J.-P. Hubaux, “Wormhole-based an- tijamming techniques in sensor networks,” *IEEE transactions on Mobile Computing*, vol. 6, no. 1, 2007.

12. Z. Karakehayov, “Using reward to detect team black-hole attacks in wireless sensor networks,” *Wksp. Real-World Wireless Sensor Networks*, pp. 20–21, 2005.

13. B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in *Security and Privacy, 2005 IEEE Symposium on*. IEEE, 2005, pp. 49–63.

14. R. A. Rahman and B. Shah, “Security analysis of iot protocols: A focus in coap,” in *Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on*. IEEE, 2016, pp. 1–7.

15. F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 839–850, 2005.

16. A. A. Hadi, G. Bere, T. Kim, J. J. Ochoa, J. Zeng, and G.-S. Seo, ‘‘Secure and cost-effective micro phasor measurement unit (PMU)-like metering for Behind-the-Meter (BTM) solar systems using blockchain-assisted smart inverters,’’ in Proc. IEEE Appl. Power Electron. Conf. Expo. (APEC), Mar. 2020, pp. 2369–2375.

17. J. Choi, B. Ahn, G. Bere, S. Ahmad, H. A. Mantooth, and T. Kim, ‘‘Blockchain-based Man-in-the-Middle (MITM) attack detection for photovoltaic systems,’’ in Proc. IEEE Design Methodol. Conf. (DMC), Bath, United Kingdom, Jul. 2021.

18. T. Kim, J. Ochoa, T. Faika, H. A. Mantooth, J. Di, Q. Li, and Y. Lee, ‘‘An overview of cyber-physical security of battery management systems and adoption of blockchain technology,’’ IEEE J. Emerg. Sel. Topics Power Electron., vol. 10, no. 1, pp. 1270–1281, Feb. 2022.

19. N. Prusty, Building Blockchain Projects, 1st ed. Birmingham, U.K.: Packt, Apr. 2017.

20. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 1st ed. Morgan Kaufmann, Nov. 2008.

21. J. Ramos-Ruiz, J. Kim, W.-H. Ko, T. Huang, P. Enjeti, P. R. Kumar, and L. Xie, ‘‘An active detection scheme for cyber attacks on grid-tied PV systems,’’ in Proc. IEEE CyberPELS (CyberPELS), Miami, FL, USA, Oct. 2020, pp. 1–6.

22. J. Kim, W.-H. Ko, and P. R. Kumar, ‘‘Cyber-security with dynamic watermarking for process control systems,’’ in Proc. AIChE Annu. Meeting, 2019.

23. B. Satchidanandan and P. R. Kumar, ‘‘Dynamic watermarking: Active defense of networked cyber–physical systems,’’ Proc. IEEE, vol. 105, no. 2, pp. 219–240, Feb. 2017.

24. J. Ramos-Ruiz, H. Ibrahim, J. Kim, W. H. Ko, T. Huang, P. Enjeti, P. R. Kumar, and L. Xie, ‘‘Validation of a robust cyber shield for a grid connected PV inverter system via digital watermarking principle,’’ in Proc. IEEE 12th Int. Symp. Power Electron. Distrib. Gener. Syst. (PEDG), Chicago, IL, USA, Jun./Jul. 2021, pp. 1–6.

25. A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, D. Saleem, and H. Abu-Rub, ‘‘Intrusion detection for cybersecurity of power electronics dominated grids: Inverters PQ set-points manipulation,’’ in Proc. IEEE CyberPELS (CyberPELS), Miami, FL, USA, Oct. 2020, pp. 1–8.

26. W. J. Tzeng and F. Y. Wu, ‘‘Theory of impedance networks: The two-point impedance and LC resonances,’’ J. Phys. A, Math. Gen., vol. 39, no. 27, pp. 8579–8591, Jul. 2006.

27. K. Gupta, S. Sahoo, R. Mohanty, B. K. Panigrahi, and F. Blaabjerg, ‘‘Distinguishing between cyber attacks and faults in power electronic systems—A noninvasive approach,’’ IEEE J. Emerg. Sel. Topics Power Electron., vol. 11, no. 2, pp. 1578–1588, Apr. 2023.

28. O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, ‘‘Cyberphysical anomaly detection in microgrids using time-frequency logic formalism,’’ IEEE Access, vol. 9, pp. 20012–20021, 2021, doi: 10.1109/ACCESS.2021.3055229.

29. S. Sahoo, Y. Yang, and F. Blaabjerg, ‘‘Resilient synchronization strategy for AC microgrids under cyber attacks,’’ IEEE Trans. Power Electron., vol. 36, no. 1, pp. 73–77, Jan. 2021, doi: 10.1109/TPEL.2020.3005208.

30. C. Burgos-Mellado, C. Zuñiga-Bauerle, D. Muñoz-Carpintero, Y. Arias-Esquivel, R. Cárdenas-Dobson, T. DragiCevic, F. Donoso, and A. Watson, ‘‘Reinforcement learning-based method to exploit vulnerabilities of false data injection attack detectors in modular multilevel converters,’’ IEEE Trans. Power Electron., vol. 38, no. 7, pp. 8907–8921, Jul. 2023.

31. S. M. S. Hussain, T. S. Ustun, and A. Kalam, ‘‘A review of IEC 62351 security mechanisms for IEC 61850 message exchanges,’’ IEEE Trans. Ind. Informat., vol. 16, no. 9, pp. 5643–5654, Sep. 2020.

32. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. London, U.K.: Pearson, 2017.

33. J. Hong, C.-C. Liu, and M. Govindarasu, ‘‘Detection of cyber intrusions using network-based multicast messages for substation automation,’’ in Proc. Innov. Smart Grid Technol. (ISGT), Washington, DC, USA, Feb. 2014, pp. 1–5.

34. N. Kush, E. Ahmed, M. Branagan, and E. Foo, ‘‘Poisoned GOOSE: Exploiting the GOOSE protocol,’’ in Proc. 12th Australas. Inf. Secur. Conf. (AISC), Auckland, New Zealand, Feb. 2014, pp. 17–22.

35. L. E. da Silva and D. V. Coury, ‘‘A new methodology for real-time detection of attacks in IEC 61850-based systems,’’ Electr. Power Syst. Res., vol. 143, pp. 825–833, Feb. 2017.

36. M. C. Magro, P. Pinceti, L. Rocca, and G. Rossi, ‘‘Safety related functions with IEC 61850 GOOSE messaging,’’ Int. J. Electr. Power Energy Syst., vol. 104, pp. 515–523, Jan. 2019.

37. B. Kang, P. Maynard, K. McLaughlin, S. Sezer, F. Andrén, C. Seitl, F. Kupzog, and T. Strasser, ‘‘Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations,’’ in Proc. IEEE 20th Conf. Emerg. Technol. Factory Autom. (ETFA), Luxembourg City, Luxembourg, Sep. 2015, pp. 1–8.

38. J. Johnson, B. Fox, K. Kaur, and J. Anandan, ‘‘Evaluation of interoperable distributed energy resources to IEEE 1547.1 using SunSpec modbus, IEEE 1815, and IEEE 2030.5,’’ IEEE Access, vol. 9, pp. 142129–142146, Oct. 2021.

39. J. Lázaro, A. Astarloa, M. Rodríguez, U. Bidarte, and J. Jiménez, ‘‘A survey on vulnerabilities and countermeasures in the communications of the smart grid,’’ Electronics, vol. 10, no. 16, p. 1881, Aug. 2021, doi: 10.3390/electronics10161881.

40. J. Ni, K. Zhang, X. Lin, and X. S. Shen, ‘‘Securing fog computing for Internet of Things applications: Challenges and solutions,’’ IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.

41. V. K. Sehgal, A. Patrick, A. Soni, and L. Rajput, ‘‘Smart human security framework using Internet of Things, cloud and fog computing,’’ in Intelligent Distributed Computing. Springer, 2015, pp. 251–263.

42. A. I. Awad, ‘‘Machine learning techniques for fingerprint identification: A short review,’’ in Proc. Int. Conf. Adv. Mach. Learn. Technol. Appl. Springer, 2012, pp. 524–531.

43. R. Oulhiq, S. Ibntahir, M. Sebgui, and Z. Guennoun, ‘‘A fingerprint recognition framework using artificial neural network,’’ in Proc. 10th Int. Conf. Intell. Syst., Theories Appl. (SITA), Oct. 2015, pp. 1–6.

44. R. Vishwakarma și A. K. Jain, „A survey of DDoS attacking techniques and defence mechanisms in the IoT network”, *Telecommun Syst*, vol. 73, nr. 1, pp. 3–25, ian. 2020, doi: 10.1007/s11235-019-00599-z.

45. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, și B. Sikdar, „A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures”, *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

46. OPAL-RT, „OPAL-RT HYPERSIM”. [Online]. Disponibil la: https://villas.fein-aachen.org/doc/node-client-hypersim.html [citat 22.12.2023].

47. R. Fu, M. E. Lichtenwalner, și T. J. Johnson, „A Review of Cybersecurity in Grid-Connected Power Electronics Converters: Vulnerabilities, Countermeasures, and Testbeds”, *IEEE Access*, vol. 11, pp. 113543–113559, 2023, doi: 10.1109/ACCESS.2023.3324177.