Universitatea Tehnică a Moldovei

Securitatea rețelelor IoT

Student: **Dodiță Corneliu**

Conducător: **Moraru Victor**
conf.univ.,dr.

Chişinău, 2022

Adnotare

Internetul lucrurilor (IoT) joacă un rol vital în interconectarea obiectelor fizice și virtuale care sunt încorporate cu senzori, software și alte tehnologii care intenționează să conecteze și să faciliteze schimbul de date cu dispozitive și sisteme de pe tot globul prin Internet. Cu o multitudinea de facilități pe care le oferă, IoT este avantajos pentru omenire, dar la fel ca cele două fețe ale unei monede, tehnologia, cu lipsa ei de securizare a informațiilor, poate duce la un mare coșmar.

Se estimează că până în anul 2030 vor exista aproape 25,44 miliarde de dispozitive IoT conectate în întreaga lume. Datorită creșterii fără precedent, IoT este pus în pericol de numeroase atacuri, deteriorări și utilizări greșite din cauza provocărilor precum limitările de resurse, eterogenitatea dispozitivelor, lipsa de standardizare, arhitectura etc. Se știe că aproape 98% din traficul IoT nu este criptat, expunând informații confidențiale și personale din rețea. Pentru a implementa o astfel de tehnologie în viitorul apropiat, este necesară o implementare cuprinzătoare de securitate, confidențialitate și autentificare.

Prin urmare, în această lucrare, este discutată taxonomia cuprinzătoare a securității și amenințărilor în cadrul paradigmei IoT. De asemenea, cu constatări perspicace, presupuneri și rezultate ale provocărilor pentru a ajuta dezvoltatorii IoT să abordeze riscurile și lacunele în securitate pentru o mai bună protecție.

Cu o arhitectură IoT cu cinci straturi și una cu șapte straturi sunt prezentate în plus față de arhitectura existentă cu trei straturi. Sunt discutate standardele de comunicare și protocoalele, împreună cu amenințările și atacurile corespunzătoare acestor trei arhitecturi. În plus, impactul diferitelor amenințări și atacuri împreună cu detectarea, atenuarea și prevenirea acestora sunt prezentate cuprinzător.

Soluțiile pentru îmbunătățirea caracteristicilor de securitate în dispozitivele IoT sunt propuse pe baza tehnologiilor Blockchain (BC), Fog Computing (FC), Edge Computing (EC) și Machine Learning (ML), împreună cu unele probleme deschise pentru cercetare.

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

Adnotation

The Internet of Things (IoT) plays a vital role in interconnecting physical and virtual objects that are embedded with sensors, software, and other technologies intending to connect and exchange data with devices and systems around the globe over the Internet. With a multitude of features to offer, IoT is advantageous to mankind, but just as two sides of a coin, the technology, with its lack of securing information, may result in a big nightmare.

It is estimated that by the year 2030, there will be nearly 25.44 billion IoT devices connected worldwide. Due to the unprecedented growth, IoT is endangered by numerous attacks, impairments, and misuses due to challenges such as resource limitations, heterogeneity, lack of standardization, architecture, etc. It is known that almost 98% of IoT traffic is not encrypted, exposing confidential and personal information on the network.

To implement such a technology in the near future, a comprehensive implementation of security, privacy and authentication is required. Therefore, in this paper, the comprehensive taxonomy of security and threats within the IoT paradigm is discussed. Also with insightful findings, presumptions, and outcomes of the challenges to assist IoT developers to address risks and security flaws for better protection.

A five-layer and a seven-layer IoT architecture are presented in addition to the existing three-layer architecture. The communication standards and the protocols, along with the threats and attacks corresponding to these three architectures, are discussed. In addition, the impact of different threats and attacks along with their detection, mitigation, and prevention are comprehensively presented.

The solutions to enhance security features in IoT devices are proposed based on Blockchain (BC) technology, Fog Computing (FC), Edge Computing (EC), and Machine Learning (ML), along with some open research problems.

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

Cuprins

Introducere

Noi trăim în timpuri cînd tehnologiile au devenit o necesitate aproape pentru toți oamenii, iar dovada acestui fapt servește dependența crescătoare de tehnologii în aproape toate aspectele vieții umane. În lumea de astăzi este observată o evoluție rapidă a aplicațiilor bazate pe Interent of Things(IoT)[1]. Evoluția domeniului IoT sa dovedit a fi un fenomen glorios în ultimii ani. Demonstrînd cum obiecte reale și virtuale dotate cu sensori, programe software și alte tehnologii sunt interconectate prin intermediul IoT[2]. Se contemplează o lume unde comunicarea și împărtășirea datelor cu alte dispozitive și sisteme la nivel global prin Internet reprezintă mai mult o necesitate decît comoditate. IoT este format dintr-un masiv de dispozitive capabile să comunice prin rețea însă exclude calculatoarele tradiționale ca laptopurile și serverele.

IoT s-a incubat peste tot, începînd cu sectorul medical și terminînd cu setoarele marilor industrii. Acum dispozitivele IoT pot fi implantate, purtate și portabile, rezultînd într-o lume revazivă și interactivă[3]. IoT modifică obiectele fizice din jurul nostru în obiecte deștepte(smart things), creînd un mediu informațional care schimbă crescător standartele de viață ale oamenilor. Ca instanță, dispozitivle IoT urmăresc și colectează măsurări esențiale (ca presiunea arterială, nevelul de zahăr în sînge, pulsul inimii, etc) în timp real, oferind alerte de urgență pentru a ridica șansele de supraviețuire a unui pacient[4]. Mai mult ca atît, automobilele autonome cu autopilot asistă șoferii în menținerea benzilor și în evitarea accidentelor rutiere deasemenea ele pot notifica automat serviciile de urgență în caz de accident rutier. IoT deasemenea acoperă multe aspecte din industriile moderne, incluzînd producerea, asamblarea, împachetarea, logistica, orașe deștepte și industria aviatică[5]. Cîteva din domeniile de bază în care sunt implementate aplicații bazate pe IoT ca sănatatea, comerțul, comunicațiile și divertismentul sunt demonstrate in Fig.1 .

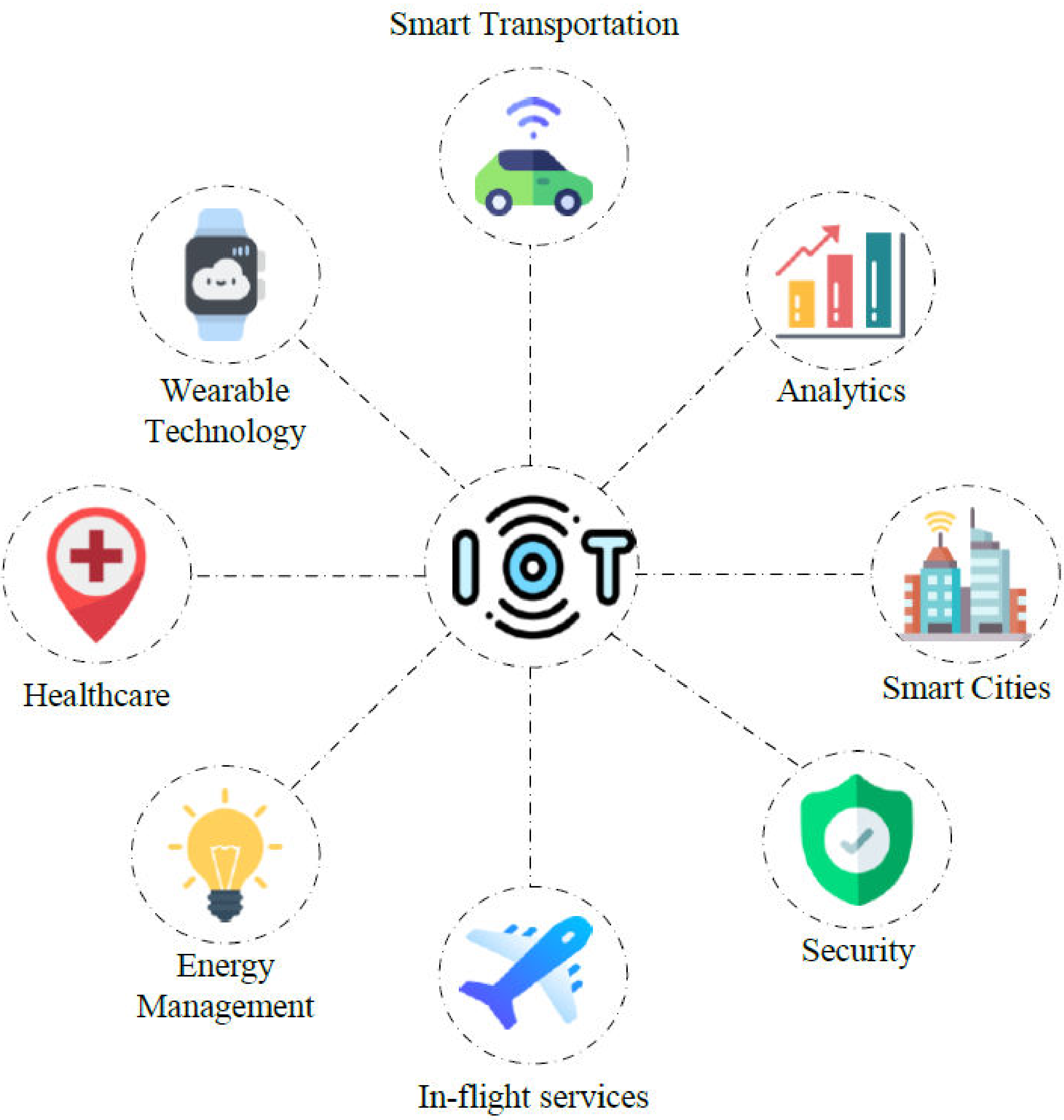

Fig. 1. Domeniile principale care folosesc aplicații IoT .

Pentru a implementa aplicații IoT, tehnologiile tradiționale au avut nevoia de a suporta modificații majore. Spre exemplu, pentru a converta un dispozitiv izolat în unul capabil ş-ă transmită date, este necesar dea mări memoria și capacitățile de procesare în timp ce sunt micșorate dimensiunile fizice ale aparatului[6]. Mai departe, crearea a diferite protocoale eficiente și sigure pentru comunicare între diferite dispozitive IoT este un punct la fel important. Îmbunătățirile suferite de rețelele convnețіonale pentru a ajuta operarea ecosistemului IoT au și ele stul lor de consecințe. Cu toate aceste, creșterea fără precedent a dispozitivelor interconectate a avut un efect paralizant asupra ecosistemului IoT. În consecință, există suficient spațiu pentru amenințări și atacuri în aplicații bazate pe IoT.

Vice Președintele global al New Net Technologies(NNT), Dirk Schrader, a menționat faptul că dispozitivele bazate pe IoT au devenit cireașa de pe tort pentru criminalii cibernetici. El deasemenea a spus că mai puțin de 42% din businesuri sunt capabile s-ă depisteze dispozitive IoT nesigure. Prin urmare ca cercetătorii s-ă dezvolte soluții bine fundamentate pentru urmărirea și prevenirea unor asemenea pericole, ei trebuie mai întîi să înțeleagă pericolele și atacurile pentru a face mediul IoT mai sigur, mai protejat și mai fiabil. Sunt trei aspecte importante care trebuie luate în considerație cînd IoT se examinează din perspectiva securității. Ca început, există un număr imens de dispozitive IoT, posibil miliarde. Acest fapt sugerează că IoT devine unul dintre cele mai complexe sisteme create de om vreodată luînd doar în cosiderație numărul de entități implicate[7]. Al doilea, toate dispozitivele sunt heterogene, în privința funcționalității, protocoalelor utilizate, mediilor de comunicare, sistemelor de opereare(unele dispozitive nu au sistem de oparare), resursele energetice, identitatea și așa mai departe[8]. Al treilea aspect, fiecare dispozitiv IoT este proprietatea unei companii sau a unui individ, și este administrat de aceiaș ori altă companie sau individ. Milioane de businesuri și persoane au control asupra unei subrețele de dispozitive IoT din domeniul lor de administrare. Și din punctul de vedere a protecției, securității și încrederii cum acest control este tehnic menținut reprezintă o problemă cirtică.

Spectrul de atacuri în domeniul IoT a crescut semnificativ, precum au crescut și pericolele pentru integritatea acestor entități din domeniul IoT [9]. Spre exemplu pericolele de securitate pentru automobilele cu autopilot pot duce la consecințe dezastruoase. Vehiculele autonome sunt vulnerabile al atacurile bazare pe sensori. Manipulînd sensorii(e.g., accelerometru, magnetometru, etc.), atacatorii pot colecta date, transfera soft malițios sau declanșa o activitate malițioasă[10]. În plus, smartphoanele și sistemele embeded contribuie la formarea unui ecosistem digital care rezultă în comunicare globală instantanee care simplifică viața datorită faptului că ecosistemul este sensitiv, flexibil și responsiv la necesitățile umane. Totuși, pe de altă parte, securitatea nu poate fi asigurată din cauza vulnerabilităților din IoT. Când semnalul unui utilizator este întrerupt sau interceptat, confidențialitatea lor poate fi pusă în pericol, iar informațiile lor pot fi scurse.

Organizarea acestei lucrări este constituită din 4 capitole. Motivația și contribuțiile prezentei lucrări sunt prezentate în capitolul 1. Descrierea conceptului IoT și fundamentele pericolelor de securitate și moduri de atac asupra securității sunt prezentate în capitolul 2. Capitolul 2 este deasemenea dedicat modelului de referință IoT și stacului de protocoale. O analiză profundă asupra vulnerabilităților, pericolelor și atacurilor asupra IoT sunt clasificate în capitolul 3. Scopurile de securitate și o cale de îmbunătățire a ei sunt prezentate în capitolul 4 unde se descriu soluții de securitate pentru IoT folosind tehnologii în plină dezvoltare ca, Blockchain(BC), Fog Computing(FG), Edge Computing(EC), și Machine Learning(ML). Careva probleme care rămîn deschise pentru cercetare sunt discutate la sfîrșitul capitolului 4. Ultimul capitol este dedicat concluziilor și unor puncte de cercetare pentru viitor.

Bibliografie

1. Jha, A.V.; Appasani, B.; Ghazali, A.N. Performance Evaluation of Network Layer Routing Protocols on Wireless Sensor Networks. In Proceedings of the 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 17–19 July 2019; pp. 1862–1865.

2. Tiwary, A.; Mahato, M.; Chidar, A.; Chandrol, M.K.; Shrivastava, M.; Tripathi, M. Internet of Things (IoT): Research, architectures and applications. Int. J. Future Revolut. Comput. Sci. Commun. Eng. 2018, 4, 23–27.

3. González-Zamar, M.D.; Abad-Segura, E.; Vázquez-Cano, E.; López-Meneses, E. IoT Technology Applications-Based Smart Cities: Research Analysis. Electronics 2020, 9, 1246.

4. Internet of Things in Healthcare: Applications, Benefits, and Challenges. Available online: https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html [accesat pe 3.10.21]

5. Cvar, N.; Trilar, J.; Kos, A.; Volk, M.; Stojmenova Duh, E. The Use of IoT Technology in Smart Cities and Smart Villages: Similarities, Differences, and Future Prospects. Sensors 2020, 20, 3897.

6. Ryan, P.J.; Watson, R.B. Research Challenges for the Internet of Things: What Role Can OR Play? Systems 2017, 5, 24.

7. Jha, A.V.; Appasani, B.; Ghazali, A.N.; Pattanayak, P.; Gurjar, D.S.; Kabalci, E.; Mohanta, D.K. Smart grid cyber-physical systems: Communication technologies, standards and challenges. Wirel. Netw. 2021, 27, 2595–2613.

8. Jha, A.V.; Mishra, S.K.; Appasani, B.; Ghazali, A.N. Communication Networks for Metropolitan E-Health Applications. IEEE Potentials 2021, 40, 34–42.

9. Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. Information 2016, 7, 44.

10. Rajendran, G.; Nivash, R.S.R.; Parthy, P.P.; Balamurugan, S. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In Proceedings of the International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–6.

11. Chen, L.; Thombre, S.; Järvinen, K.; Lohan, E.S.; Alén-Savikko, A.; Leppäkoski, H.; Bhuiyan, M.Z.H.; Bu-Pasha, S.; Ferrara, G.N.; Honkala, S.; et al. Robustness, security and privacy in location-based services for future IoT: A survey. IEEE Access 2017, 5, 8956–8977.

12. Shin, H.; Lee, H.K.; Cha, H.Y.; Heo, S.W.; Kim, H. IoT security issues and light weight block cipher. In Proceedings of the International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Okinawa, Japan, 11–13 February 2019; pp. 381–384.

13. Gamundani, A.M. An impact review on internet of things attacks. In Proceedings of the International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 17–20 May 2015; pp. 114–118.

14. Kumar, N.; Madhuri, J.; Channe Gowda, M. Review on security and privacy concerns in Internet of Things. In Proceedings of the International Conference on IoT and Application (ICIOT), Nagapattinam, India, 19–20 May 2017; pp. 1–5.

15. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.

16. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. J. Netw. Comput. Appl. 2017, 88, 10–28.

17. Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. J. Cyber Secur. Mobil. 2015, 4, 65–88.

18. Kozlov, D.; Veijalainen, J.; Ali, Y. Security and privacy threats in IoT architectures. BODYNETS 2012, 256–262.

19. Lee, E.; Seo, Y.D.; Oh, S.R.; Kim, Y.G. A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Commun. Surv. Tutor. 2021, 23, 1020–1047.

20. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. Sensors 2021, 21, 3654.

21. Mann, P.; Tyagi, N.; Gautam, S.; Rana, A. Classification of Various Types of Attacks in IoT Environment. In Proceedings of the 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 3 November 2020; pp. 346–350.

22. Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A survey on privacy and security of Internet of Things. Comput. Sci. Rev. 2020, 38, 10031.

23. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. J. Netw. Comput. Appl. 2017, 84, 25–37.

24. Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion Detection Systems in the Internet of Things: A Comprehensive Investigation. Comput. Netw. 2019, 160, 165–191.

25. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. Comput. Netw. 2018, 141, 199–221.

26. Sun, L.; Du, Q. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. Entropy 2018, 20, 730.

27. Elazhary, H. Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions. J. Netw. Comput. Appl. 2019, 128, 105–140.

28. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security. Digit. Commun. Netw. 2020, 6, 147–156.

29. Memon, R.A.; Li, J.P.; Ahmed, J.; Nazeer, M.I.; Ismail, M.; Ali, K. Cloud-based vs. blockchain-based IoT: A comparative survey and way forward. Front. Inform. Technol. Electron. Eng. 2020, 21, 563–586.

30. Tran, N.K.; Babar, M.A.; Boan, J. Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs. J. Netw. Comput. Appl. 2020, 173, 102844.

31. Fersi, G. Fog computing and Internet of Things in one building block: A survey and an overview of interacting technologies. Cluster Comput. 2021, 1–31.

32. Atlam, H.F.; Walters, R.J.; Wills, G.B. Fog Computing and the Internet of Things: A Review. Big Data Cogn. Comput. 2018, 2, 10.

33. Hamdan, S.; Ayyash, M.; Almajali, S. Edge-Computing Architectures for Internet of Things Applications: A Survey. Sensors 2020, 20, 6441.

34. Capra, M.; Peloso, R.; Masera, G.; Ruo Roch, M.; Martina, M. Edge Computing: A Survey on the Hardware Requirements in the Internet of Things World. Future Internet 2019, 11, 100.

35. Ashouri, M.; Lorig, F.; Davidsson, P.; Spalazzese, R. Edge Computing Simulators for IoT System Design: An Analysis of Qualities and Metrics. Future Internet 2019, 11, 235.

36. Amiri-Zarandi, M.; Dara, R.A.; Fraser, E. A survey of machine learning-based solutions to protect privacy in the Internet of Things. Comput. Secur. 2020, 96, 101921.

37. Adnan, A.; Muhammed, A.; Abd Ghani, A.A.; Abdullah, A.; Hakim, F. An Intrusion Detection System for the Internet of Things Based on Machine Learning: Review and Challenges. Symmetry 2021, 13, 1011.

38. Alwarafy, A.; Al-Thelaya, K.A.; Abdallah, M.; Schneider, J.; Hamdi, M. A Survey on Security and Privacy Issues in EdgeComputing-Assisted Internet of Things. IEEE Internet Things J. 2020, 8, 4004–4022.

39. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A survey on access control in the age of internet of things. IEEE Internet Things J. 2020, 7, 4682–4696.

40. Parmar, M.S.; Shah, P.P. Uplifting Blockchain Technology for Data Provenance in Supply Chain. Int. J. Adv. Sci. Technol. 2020, 29, 5922–5938.

41. Granjal, J.; Monteiro, E.; Silva, J.S. Security for the internet of things: A survey of existing protocols and open research issues. IEEE Commun. Surv. Tutor. 2015, 17, 1294–1312.

42. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet Things J. 2018, 6, 2188–2204.

43. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in Internet-of-Things. IEEE Internet Things J. 2017, 4, 1250–1258.

44. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. 2017, 4, 1125–1142.

45. Malik, M.; Dutta, M.; Granjal, J. A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things. IEEE Access 2019, 7, 27443–27464.

46. Alshehri, F.; Muhammad, G. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. IEEE Access 2021, 9, 3660–3678.

47. Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; Markakis, E.K. A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. IEEE Commun. Surv. Tutor. 2020, 22, 1191–1221.

48. Viriyasitavat, W.; Da Xu, L.; Bi, Z.; Hoonsopon, D. Blockchain technology for applications in internet of things—mapping from system design perspective. IEEE Internet Things J. 2019, 6, 8155–8168.

49. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Commun. Surv. Tutor. 2019, 22, 616–644.

50. Cha, S.C.; Hsu, T.Y.; Xiang, Y.; Yeh, K.H. Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. IEEE Internet Things J. 2018, 6, 2159–2187.

51. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Commun. Surv. Tutor. 2020, 22, 1646–1685.

52. Mosenia, A.; Jha, N.K. A comprehensive study of security of internet-of-things. IEEE Trans. Emerg. Top. Comput. 2016, 5, 586–602.

53. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733.

54. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Integration of blockchain and cloud of things: Architecture, applications and challenges. IEEE Commun. Surv. Tutor. 2020, 22, 2521–2549.

55. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and opportunities in securing the industrial internet of things. IEEE Trans. Ind. Inform. 2020, 17, 2985–2996.

56. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT middleware: A survey on issues and enabling technologies. IEEE Internet Things J. 2016, 4, 1–20.

57. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the internet of things. IEEE Commun. Surv. Tutor. 2018, 21, 1636–1675.

58. Qiu, T.; Chi, J.; Zhou, X.; Ning, Z.; Atiquzzaman, M.; Wu, D.O. Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Commun. Surv. Tutor. 2020, 22, 2462–2488.

59. Hamad, S.A.; Sheng, Q.Z.; Zhang, W.E.; Nepal, S. Realizing an internet of secure things: A survey on issues and enabling technologies. IEEE Commun. Surv. Tutor. 2020, 22, 1372–1391.

60. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Commun. Surv. Tutor. 2018, 21, 1676–1717.

61. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. 2019, 6, 8182–8201.

62. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network intrusion detection for IoT security based on learning techniques. IEEE Commun. Surv. Tutor. 2019, 21, 2671–2701.

63. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A survey on the edge computing for the Internet of Things. IEEE Access 2017, 6, 6900–6919.

64. Ni, J.; Zhang, K.; Lin, X.; Shen, X. Securing fog computing for internet of things applications: Challenges and solutions. IEEE Commun. Surv. Tutor. 2017, 20, 601–628.

65. Restuccia, F.; D'Oro, S.; Melodia, T. Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet Things J. 2018, 5, 4829–4842.

66. Omoniwa, B.; Hussain, R.; Javed, M.A.; Bouk, S.H.; Malik, S.A. Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. IEEE Internet Things J. 2018, 6, 4118–4149.

67. Khanam, S.; Ahmedy, I.B.; Idris, M.Y.I.; Jaward, M.H.; Sabri, A.Q.B.M. A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE Access 2020, 8, 219709–219743.

68. Alotaibi, B. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. IEEE Sens. J. 2019, 19, 10953–10971.

69. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access 2019, 7, 82721–82743.

70. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. IEEE Commun. Surv. Tutor. 2020, 22, 1686–1721.

71. Benkhelifa, E.; Welsh, T.; Hamouda, W. A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. IEEE Commun. Surv. Tutor. 2018, 20, 3496–3509.

72. Sengupta, J.; Ruj, S.; Bit, S.D. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. J. Netw. Comput. Appl. 2020, 149, 102481.

73. Yugha, R.; Chithra, S. A survey on technologies and security protocols: Reference for future generation IoT. J. Netw. Comput. Appl. 2020, 169, 102763.

74. Bhoyar, P.; Sahare, P.; Dhok, S.B.; Deshmukh, R.B. Communication technologies and security challenges for internet of things: A comprehensive review. AEU-Int. J. Electron. Commun. 2019, 99, 81–99.

75. Bellavista, P.; Berrocal, J.; Corradi, A.; Das, S.K.; Foschini, L.; Zanni, A. A survey on fog computing for the Internet of Things. Pervasive Mob. Comput. 2019, 52, 71–99.

76. Peña-López, I. ITU Internet Report 2005: The Internet of Things. Available online: https://www.comminit.com/global/content/ itu-internet-reports-2005-internet-things

77. Sikder, A.K.; Petracca, G.; Aksu, H.; Jaeger, T.; Uluagac, A.S. A survey on sensor-based threats to internet-of-things (IoT) devices and applications. arXiv 2018, arXiv:1802.02041v1.

78. Hongsong, C.; Zhongchuan, F.; Dongyan, Z. Security and trust research in m2m system. In Proceedings of the 2011 IEEE International Conference on Vehicular Electronics and Safety, Beijing, China, 10–12 July 2011; pp. 286–290.

79. Kumar, S.A.; Vealey, T.; Srivastava, H. Security in internet of things: Challenges, solutions and future directions. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 5772–5781.

80. Lee, S.K.; Bae, M.; Kim, H. Future of IoT networks: A survey. Appl. Sci. 2017, 7, 1072.

81. Chen, H.; Jia, X.; Li, H. A Brief Introduction to IoT Gateway. In Proceedings of the IET International Conference on Communication Technology and Application (ICCTA), Beijing, China, 14–16 October 2011; pp. 1–4.

82. Tan, H.; Tsudik, G.; Jha, S. MTRA: Multi-Tier randomized remote attestation in IoT networks. Comput. Secur. 2019, 81, 78–93.

83. Internet of Things Challenges in Storage and Data. Available online: https://www.computerweekly.com/news/252450705/ Internet-of-things-challenges-in-storage-and-data[accesat pe 4.10.21]

84. 12 Benefits of Cloud Computing. Available online: https://www.salesforce.com/in/products/platform/best-practices/benefitsof-cloud-computing/

85. Li, X.; Wang, Q.; Lan, X.; Chen, X.; Zhang, N.; Chen, D. Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach. IEEE Access 2019, 7, 9368–9383.

86. Kepçeo ˘glu, B.; Murzaeva, A.; Demirci, S. Performing energy consuming attacks on IoT devices. In Proceedings of the 27th Telecommunications Forum (TELFOR), Belgrade, Serbia, 26–27 November 2019; pp. 1–4.

87. Bilal, M. A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers. arXiv 2017, arXiv:1708.04560. Available online: https://arxiv.org/abs/1708.04560

88. Dodig, I.; Cafuta, D.; Kramberger, T.; Cesar, I. A Novel Software Architecture Solution with a Focus on Long-Term IoT Device Security Support. Appl. Sci. 2021, 11, 4955.

89. Capella, J.V.; Campelo, J.C.; Bonastre, A.; Ors, R. A Reference Model for Monitoring IoT WSN-Based Applications. Sensors 2016, 16, 1816.

90. Sadiku, M.N.; Tembely, M.; Musa, S.M. Home area networks: A primer. Int. J. 2017, 7, 208.

91. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. Comput. Netw. 2010, 54, 2787–2805.

92. Swamy, S.N.; Kota, S.R. An Empirical Study on System Level Aspects of Internet of Things (IoT). IEEE Access 2020, 8, 188082–188134.

93. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of Things: A General Overview between Architectures, Protocols and Applications. Information 2021, 12, 87.

94. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.

95. Shelby, Z.; Hartke, K.; Bormann, C.; Frank, B. Constrained Application Protocol (CoAP), Draft-Ietf-Corecoap-18, Work in Progress. sl: IETF. 2013. Available online: http://tools.ietf.org/html/draft-ietf-corecoap-18[accesat pe 6.10.21]

96. IoT Standards and Protocols Guide—Protocols of the Internet of Things. Available online: https://www.avsystem.com/blog/iotprotocols-and-standards/

97. Bormann, C.; Castellani, A.P.; Shelby, Z. Coap: An application protocol for billions of tiny internet nodes. IEEE Internet Comput. 2012, 16, 62–67.

98. Cheshire, S.; Krochmal, M. Multicast DNS. RFC 2013, 6762. Available online: https://www.rfc-editor.org/info/rfc6762. [accesat pe 8.10.21]

99. Vasseur, J.; Agarwal, N.; Hui, J.; Shelby, Z.; Bertrand, P.; Chauvenet, C. RPL: The IP routing protocol designed for low power and lossy networks. IPSO Alliance 2011, 1–20. Available online: http://www.cse.chalmers.se/edu/year/2019/course/DAT300 /PAPERS/rpl.pdf [accesat pe 8.10.21]

100. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.W.; Kelsey, R.; Levis, P.; Alexander, R.K. RPL: IPv6 routing protocol for low-power and lossy networks. RFC 2012, 6550, 1–157. Available online: https://datatracker.ietf.org/doc/html/rfc6550 [accesat pe 8.10.21]

101. Yang, Z.; Yue, Y.; Yang, Y.; Peng, Y.; Wang, Z.; Liu, W. Study and Application on the Architecture and Key Technologies for IOT. In Proceedings of the International Conference on Multimedia Technology, Hangzhou, China, 26–28 July 2011; pp. 747–751.

102. Palattella, M.R.; Accettura, N.; Vilajosana, X.; Watteyne, T.; Grieco, L.A.; Boggia, G.; Dohler, M. Standardized protocol stack for the internet of (important) things. IEEE Commun. Surv. Tutor. 2012, 15, 1389–1406.

103. IEEE 802 Working Group. IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs); IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006); IEEE: Manhattan, NY, USA, 2011; pp. 1–314.

104. Hasan, M.; Hossain, E.; Niyato, D. Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches. IEEE Commun. Mag. 2013, 51, 86–93.

105. IEEE 802 Working Group. IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies; IEEE Std 1905.1-2013; IEEE: Manhattan, NY, USA, 2013; pp. 1–93.

106. User Datagram Protocol(UDP). Available online: https://www.geeksforgeeks.org/user-datagram-protocol-udp [accesat pe 13.10.21]

107. Pipkin, D.L. Halting the Hacker: A Practical Guide to Computer Security, 2nd ed.; Prentice Hall Professional: Hoboken, NJ, USA, 2003.

108. Bertino, E.; Martino, L.D.; Paci, F.; Squicciarini, A.C. Web services threats, vulnerabilities, and countermeasures. In Security for Web Services and Service-Oriented Architectures; Springer: Heidelberg, Germany, 2019; pp. 25–44.

109. Kizza, J.M. Guide to Computer Network Security, 1st ed.; Springer: Heidelberg, Germany, 2009; pp. 387–411.

110. Dahbur, K.; Mohammad, B.; Tarakji, A.B. A survey of risks, threats and vulnerabilities in cloud computing. In Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, New York, NY, USA, 18–20 April 2011; pp. 1–6.

111. Rainer, R.K.; Cegielski, C.G. Ethics, privacy, and information security. In Introduction to Information Systems: Supporting and Transforming Business; John Wiley & Sons: Hoboken, NJ, USA, 2010; Volume 3, pp. 70–121.

112. Tankard, C. Advanced persistent threats and how to monitor and deter them. Netw. Secur. 2011, 2011, 16–19.

113. Coffed, J. The Threat of Gps Jamming: The Risk to An Information Utility; EXELIS: Herndon, VA, USA, 2014; pp. 6–10.

114. Tippenhauer, N.O.; Pöpper, C.; Rasmussen, K.B.; Capkun, S. On the requirements for successful GPS spoofing attacks. In Proceedings of the 18th ACM Conference on COMPUTER and Communications Security, Chicago, IL, USA, 17–21 October 2011; pp. 75–86.

115. Uluagac, A.S.; Subramanian, V.; Beyah, R. Sensory channel threats to cyber physical systems: A wake-up call. In Proceedings of the IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 301–309.

116. Ge, M.; Hong, J.B.; Guttmann, W.; Kim, D.S. A framework for automating security analysis of the internet of things. J. Netw. Comput. Appl. 2017, 83, 12–27.

117. Anthi, E.; Ahmad, S.; Rana, O.; Theodorakopoulos, G.; Burnap, P. Eclipse. IoT: A secure and adaptive hub for the Internet of Things. Comput. Secur. 2018, 78, 477–490.

118. Sanchez Alcon, J.A.; López, L.; Martínez, J.F.; Rubio Cifuentes, G. Trust and privacy solutions based on holistic service requirements. Sensors 2016, 16, 16. Available online: https://www.mdpi.com/1424-8220/16/1/16 [accesat pe 14.10.21]

119. Mauro, C.; Pallavi, K.; Rabbani, M.M.; Ranise, S. Attestation-enabled secure and scalable routing protocol for IoT networks. Ad Hoc Netw. 2020, 98, 102054. 120. Prabadevi, B.; Jeyanthi, N. Distributed Denial of service attacks and its effects on Cloud environment-a survey. In Proceedings of the International Symposium on Networks, Computers and Communications, Hammamet, Tunisia, 17–19 June 2014; pp. 1–4.

121. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6.

122. Qian, L.; Zhu, Z.; Hu, J.; Liu, S. Research of SQL injection attack and prevention technology. In Proceedings of the International Conference on Estimation, Detection and Information Fusion (ICEDIF), Harbin, China, 10–11 January 2015; pp. 303–306.

123. Everything You Need to Know About Facebook's Data Breach Affecting 50M Users. Available online: http://https/ /techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/ [accesat pe 18.10.21]

124. Zou, Y.; Wang, G. Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack. IEEE Trans. Ind. Inform. 2016, 12, 780–787.

125. Chan, H.; Perrig, A.; Song, D.X. Random key predistribution schemes for sensor networks. In Proceedings of the IEEE Symposium Security Privacy, Berkeley, CA, USA, 11–14 May 2003; pp. 197–213.

126. Abomhara, M.; Køien, G.M. Security and privacy in the Internet of Things: Current status and open issues. In Proceedings of the IEEE International Conference Privacy Security Mobile System (PRISMS), Aalborg, Denmark, 11–14 May 2014; pp. 1–8.

127. Ashraf, Q.M.; Habaebi, M.H. Autonomic schemes for threat mitigation in Internet of Things. J. Netw. Comput. Appl. 2015, 49, 112–127.

128. Znaidi, W.; Minier, M.; Babau, J.P. An Ontology for Attacks in Wireless Sensor Networks; RR-6704; INRIA: Rocquencourt, France, 2008.

129. Ye, F.; Luo, H.; Lu, S.; Zhang, L. Statistical en-route filtering of injected false data in sensor networks. IEEE J. Sel. Areas Commun. 2005, 23, 839–850.

130. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The sybil attack in sensor networks: Analysis & defenses. In Proceedings of the ACM Third International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 27 April 2004; pp. 259–268.

131. Sarigiannidis, P.G.; Karapistoli, E.D.; Economides, A.A. Detecting sybil attacks in wireless sensor networks using UWB rangingbased information. Expert Syst. Appl. 2015, 42, 7560–7572.

132. Savola, R.M.; Abie, H.; Sihvonen, M. Towards metrics-driven adaptive security management in e-health IoT applications. In Proceedings of the 7th International Conference Body Area Network, Brussels, Belgium, 24–26 February 2012; pp. 276–281.

133. Choi, H.; Zhu, S.; Porta, T.F.L. SET: Detecting node clones in sensor networks. In Proceedings of the IEEE 3rd Int. Confernce Security Privacy Commun. Netw. Workshops (SecureComm), Nice, France, 17–21 September 2007; pp. 341–350.

134. Xing, K.; Liu, F.; Cheng, X.; Du, D.H.C. Real-time detection of clone attacks in wireless sensor networks. In Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS), Beijing, China, 17–20 June 2008; pp. 3–10.

135. Standaert, F.X. Introduction to side-channel attacks. Secure Integrated Circuits and Systems; Springer: Boston, MA, USA, 2010; pp. 27–42. ISBN 978-0-387-71829-3.

136. Wood, A.D.; Stankovic, J.A.; Son, S.H. JAM: A jammed-area mapping service for sensor networks. In Proceedings of the 24th IEEE Real-Time Systems Symposium, Cancun, Mexico, 5 December 2003; pp. 286–297.

137. Hussein, A.A.; Leow, C.Y.; Rahman, T.A. Robust multiple frequency multiple power localization schemes in the presence of multiple jamming attacks. PLoS ONE 2017, 12, e0177326.

138. Shabana, K.; Fida, N.; Khan, F.; Jan, S.R.; Rehman, M.U. Security issues and attacks in wireless sensor networks. Int. J. Adv. Res. Comput. Sci. Electron. Eng. 2016, 5, 81.

139. Ho, J.-W.; Wright, M.; Das, S.K. Fast detection of replica node attacks in mobile sensor networks using sequential analysis. In Proceedings of the IEEE INFOCOM, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1773–1781.

140. Wurm, J.; Hoang, K.; Arias, O.; Sadeghi, A.-R.; Jin, Y. Security analysis on consumer and industrial IoT devices. In Proceedings of the 21st IEEE Asia South Pacific Design Automation Conference (ASP-DAC), Macao, China, 25–28 January 2016; pp. 519–524.

141. Puthal, D.; Nepal, S.; Ranjan, R.; Chen, J. Threats to networking cloud and edge datacenters in the Internet of Things. IEEE Cloud Comput. 2016, 3, 64–71.

142. Koh, J.Y.; Nevat, I.; Leong, D.; Wong, W.C. Geo-spatial location spoofing detection for Internet of Thing. IEEE Internet Things J. 2016, 3, 971–978.

143. Lough, D.L. A Taxonomy of Computer Attacks with Applications to Wireless Networks; Virginia Polytechnic Institute and State University: Blacksburg, VA, USA, 2001.

144. Bu, K.; Xu, M.; Liu, X.; Luo, J.; Zhang, S.; Weng, M. Deterministic detection of cloning attacks for anonymous RFID systems. IEEE Trans. Ind. Informat. 2015, 11, 1255–1266.

145. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. Computer 2002, 35, 54–62.

146. Mirai "Internet of Things" Malware From Krebs DDoS Attack Goes Open Source. Available online: https://nakedsecurity.sophos. com/2016/10/05/mirai-internet-of-things-malware [accesat pe 21.10.21]

147. Liu, Y.; Li, Y.; Man, H. MAC layer anomaly detection in ad hoc networks. In Proceeding of the 6th Annual IEEE SMC Information Assurance Workshop (IAW), West Point, NY, USA, 15–17 June 2005; pp. 402–409.

148. Riaz, R.; Kim, K.-H.; Ahmed, H.F. Security analysis survey and framework design for IP connected LoWPANs. In Proceedings of the IEEE International Symposium Autonomous Decentralized Systems (ISADS), Athens, Greece, 23–25 March 2009; pp. 1–6.

149. Hamid, M.A.; Rashid, M.; Hong, C.S. Routing security in sensor network: Hello flood attack and defense. In Proceedings of the IEEE ICNEWS, Phoenix Park, Korea, 20–22 February 2006; pp. 2–4.

150. Murphy, J. Enhanced Security Controls for IBM Watson IoT Platform, Armonk. Available online: https://developer.ibm.com/ iotplatform/2016/09/23/enhanced-securitycontrols-for-ibm-watson-iot-platform/ [accesat pe 25.10.21]

151. Teng, L.; Zhang, Y. SERA: A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks. In Proceedings of the IEEE 2nd International Conference on Computer Modeling Simulation (ICCMS), Sanya, China, 22–24 January 2010; pp. 79–82.

152. Sathish, R.; Scholar, P.G. Dynamic detection of clone attack in wireless sensor networks. In Proceedings of the International Conference on Communication Systems Network Technologies, Gwalior, India, 6–8 April 2013; pp. 501–505.

153. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Netw. 2003, 1, 293–315.

154. Karakehayov, Z. Using reward to detect team black-hole attacks in wireless sensor networks. In Proceedings of the Workshop on Real World Wireless Sensor Network, Stockholm, Sweden, 20–21 June 2005; pp. 20–21.

155. Wang, W.; Bhargava, B.K. Visualization of wormholes in sensor networks. In Proceedings of the 3rd ACM Workshop Wireless Security, Philadelphia, PA, USA, 1 October 2001; pp. 51–60.

156. Kaissi, R.Z.E.; Kayssi, A.; Chehab, A.; Dawy, Z. DAWWSEN: A Defense Mechanism Against Wormhole Attacks in Wireless Sensor Networks. Ph.D. Thesis, American University of Beirut, Beirut, Lebanon, 2005.

157. Perrey, H.; Landsmann, M.; Ugus, O.; Wählisch, M.; Schmidt, T.C. TRAIL: Topology Authentication in RPL. In Proceedings of the ACM International Conference on Embedded Wireless System and Network (EWSN), Graz, Austria, 15–17 February 2016; pp. 59–64.

158. Dvir, A.; Holczer, T.; Buttyán, L. Vera-version number and rank authentication in RPL. In Proceedings of the IEEE 8th International Conference on Mobile Ad Hoc Sensor Systems (MASS), Valencia, Spain, 17–22 October 2011; pp. 709–714.

159. Accettura, N.; Piro, G. Optimal and secure protocols in the IETF 6TiSCH communication stack. In Proceedings of the IEEE 23rd International Symposium on Industrial Electronics (ISIE), Istambul, Turkey, 1–4 June 2014; pp. 1469–1474.

160. Singh, M.; Rajan, M.; Shivraj, V.; Balamuralidhar, P. Secure MQTT for Internet of Things (IoT). In Proceedings of the IEEE 5th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 4–6 April 2015; pp. 746–751.

161. Song, S.; Choi, H.-K.; Kim, J.-Y. A secure and lightweight approach for routing optimization in mobile IPv6. EURASIP J. Wirel. Commun. Netw. 2009, 2009, 1–10.

162. Neisse, R.; Steri, G.; Baldini, G. Enforcement of security policy rules for the Internet of Things. In Proceedings of the IEEE 10th International Confernce on Wireless and Mobile

Computing Networking and Communications (WiMob), Larnaca, Cyprus, 8–10 October 2014; pp. 165–172.

163. Xbox 360 Timing Attack. Available online: http://beta.ivc.no/wiki/index.php/Xbox_360_Timing_Attack [accesat pe 27.10.21]

164. Zhang, Q.; Wang, X. SQL injections through back-end of RFID system. In Proceedings of the International Symposium on Computer Network and Multimedia Technology, Wuhan, China, 18–20 January 2009; pp. 1–4.

165. Farris, I.; Taleb, T.; Khettab, Y.; Song, J. A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Commun. Surv. Tutor. 2019, 21, 812–837.

166. Singh, J.; Pasquier, T.; Bacon, J.; Ko, H.; Eyers, D. Twenty security considerations for cloud-supported Internet of Things. IEEE Internet Things J. 2016, 3, 269–284.

167. Bose, T.; Bandyopadhyay, S.; Ukil, A.; Bhattacharyya, A.; Pal, A. Why not keep your personal data secure yet private in IoT: Our lightweight approach. In Proceedings of the IEEE 10th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, 7–9 April 2015; pp. 1–6.

168. Kumar, J.; Rajendran, B.; Bindhumadhava, B.S.; Babu, N.S.C. XML wrapping attack mitigation using positional token. In Proceedings of the International Confernce Public Key Infrastructure and its Applications (PKIA), Bangalore, India, 14–15 November 2017; pp. 36–42.

169. Deng, J.; Han, R.; Mishra, S. Defending against path-based dos attacks in wireless sensor networks. In Proceedings of the 3rd ACM Workshop Security Ad Hoc Sensor Network, Alexandria, VA, USA, 14–15 November 2005; pp. 89–96.

170. Gupta, H.; Oorschot, P.C.V. Onboarding and Software Update Architecture for IoT Devices. In Proceedings of the 17th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 26–28 August 2019; pp. 1–11.

171. Skorobogatov, S. Fault attacks on secure chips: From glitch to flash. In Design and Security of Cryptographic Algorithms and Devices (ECRYPT II); University of Cambridge: Cambridge, UK, 2011; pp. 1–64.

172. Stanciu, A.; Balan, T.-C.; Gerigan, C.; Zamfir, S. Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm. In Proceedings of the International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP), Brasov, Romania, 25–27 May 2017; pp. 1001–1006.

173. MohammadI, S.; Jadidoleslamy, H. A comparison of link layer attacks on wireless sensor networks. Int. J. Appl. Graph Theory Wirel. Ad Hoc Netw. Sens. Netw. 2011, 3, 35–56.

174. Swamy, S.N.; Jadhav, D.; Kulkarni, N. Security threats in the application layer in IoT applications. In Proceedings of the International Confernce IoT Social, Mobile, Analytics Cloud (I-SMAC), Palladam, India, 10–11 February 2017; pp. 477–480.

175. Sharmeen, S.; Huda, S.; Abawajy, J.H.; Ismail, W.N.; Hassan, M.M. Malware Threats and Detection for Industrial Mobile-IoT Networks. IEEE Access 2018, 6, 15941–15957.

176. Ham, H.-S.; Kim, H.-H.; Kim, M.-S.; Choi, M.-J. Linear SVM-based Android malware detection for reliable IoT services. J. Appl. Math. 2014, 2014, 594501.

177. Kaur, P.; Sharma, S. Spyware detection in Android using hybridization of description analysis permission mapping and interface analysis. Procedia Comput. Sci. 2015, 46, 794–803.

178. Wolinsky, D.I.; Syta, E.; Ford, B. Hang with your buddies to resist intersection attacks. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), Berlin, Germany, 4–8 November 2013; pp. 1153–1166.

179. Grover, J.; Laxmi, V.; Gaur, M.S. Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks. CSI Trans. ICT 2013, 1, 261–279.

180. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. Comput. Netw. 2015, 76, 146–164.

181. Cherian, M.; Chatterjee, M. Survey of security threats in iot and emerging countermeasures. In Proceedings of the International Symposium on Security in Computing and Communication, Bangalore, India, 19–22 September 2018; pp. 591–604.

182. Sepulveda, J.; Willgerodt, F.; Pehl, M. SEPUFSoC: Using PUFs for memory integrity and authentication in multi-processors system-on-chip. In Proceedings of the GLSVLSI '18: Proceedings of the 2018 on Great Lakes Symposium on VLSI, Chicago, IL, USA, 23–25 May 2018; pp. 39–44.

183. Bîrleanu, F.G.; Bizon, N. Reconfigurable computing in hardware security–a brief review and application. J. Electr. Eng. Electron. Control Comput. Sci. 2016, 2, 1–12.

184. Katsikogiannis, G.; Kallergis, D.; Garofalaki, Z.; Mitropoulos, S.; Douligeris, C. A policy-aware Service Oriented Architecture for secure machine-to-machine communications. Ad Hoc Netw. 2018, 80, 70–80.

185. Laplante, P.A. Blockchain and the Internet of Things in the industrial sector. IEEE Comput. Soc. 2018, 20, 15–18.

186. Orman, H. Blockchain: The emperors new PKI? IEEE Internet Comput. 2018, 22, 23–28.

187. Henry, R.; Herzberg, A.; Kate, A. Blockchain access privacy: Challenges and directions. IEEE Secur. Priv. 2018, 16, 38–45.

188. Fog Computing: Focusing on Mobile Users at the Edge. Available online: https://arxiv.org/abs/1502.01815 [accesat pe 29.10.21]

189. Dastjerdi, A.V.; Buyya, R. Fog Computing: Helping the Internet of Things Realize Its Potential. Computer 2016, 49, 112–116.

190. Sehgal, V.K.; Patrick, A.; Soni, A.; Rajput, L. Smart human security framework using Internet of Things, cloud and fog computing. Intelligent Distributed Computing. Springer 2015, 321, 251–263.

191. Feasibility of Fog Computing. Available online: https://arxiv.org/abs/1701.05451

192. IoT Agenda. IoT and Big Data Analytics. Available online: https://internetofthingsagenda.techtarget.com/

193. Alwaris, A.; Alhothaily, A.; Hu, C.; Cheng, X. Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Comput. 2017, 21, 34–42.

194. Mollah, M.B.; Azad, M.A.K.; Vasilakos, A. Secure data sharing and searching at the edge of cloud-assisted Internet of Things. IEEE Cloud Comput. 2017, 4, 34–42.

195. Alrowaily, M.; Lu, Z. Secure edge computing in IoT systems: Review and case studies. In Proceedings of the IEEE/ACM Symposium on Edge Computing (SEC), Seattle, WA, USA, 25–27 October 2018; pp. 440–444.

196. Li, Y.; Wang, S. An energy-aware edge server placement algorithm in mobile edge computing. In Proceedings of the IEEE International Confernce Edge Comput. (EDGE), San Francisco, CA, USA, 2–7 July 2018; pp. 66–73.

197. 6 Significant Issues That Edge Computing in IoT Solves. Available online: https://internetofthingsagenda.techtarget.com/ feature/6-significant-issues-that-edge-computing-in-IoT-solves [accesat pe 30.10.21]

198. Premsankar, G.; Di Francesco, M.; Taleb, T. Edge computing for the Internet of Things: A case study. IEEE Internet Things J. 2018, 5, 1275–1284.

199. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile edge computing: A survey. IEEE Internet Things J. 2018, 5, 450–465.
200. Pavani, K.; Damodaram, A. Intrusion detection using MLP for MANETs. In Proceedings of the Third International Conference on Computational Intelligence and Information Technology (CIIT 2013), Mumbai, India, 18–19 October 2013; pp. 440–444.
201. Kulkarni, R.V.; Venayagamoorthy, G.K. Neural network based secure media access control protocol for wireless sensor networks. In Proceedings of the 2009 International Joint Conference on Neural Networks, Atlanta, GA, USA, 14–19 June 2009; pp. 1680–1687.
202. Xiao, L.; Xie, C.; Chen, T.; Dai, H.; Poor, H.V. A mobile offloading game against smart attacks. IEEE Access 2016, 4, 2281–2291.
203. Xiao, L.; Yan, Q.; Lou, W.; Chen, G.; Hou, Y.T. Proximity-based security techniques for mobile users in wireless networks. IEEE Trans. Inf. Forensics Secur. 2013, 8, 2089–2100.
204. Xiao, L.; Li, Y.; Han, G.; Liu, G.; Zhuang, W. PHY-layer spoofing detection with reinforcement learning in wireless networks. IEEE Trans. Veh. Technol. 2016, 65, 10037–10047.
205. Spirina, K. Biometric Authentication: The Future of IoT Security Solutions. Available online:https://www.IoTevolutionworld.com/IoT/articles/438690biometricauthenticationfuture-IoT-security-solutions.html [accesat pe 9.11 2021].
206. Blanco-Novoa, Ó.; Fernández-Caramés, T.; Fraga-Lamas, P.; Castedo, L. An electricity price-aware open-source smart socket for the Internet of energy. Sensors 2017, 17, 643.
207. Zhang, Y.; Wen, J. An IoT electric business model based on the protocol of bitcoin. In Proceedings of the 18th International Conference on Intelligence in Next Generation Networks, Paris, France, 17–19 February 2015; pp. 184–191.
208. Lundqvist, T.; Blanche, A.; Andersson, H.R.H. Thing-to-thing electricity micro payments using blockchain technology. In Proceedings of the Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6.
209. Salahuddin, M.A.; Al-Fuqaha, A.; Guizani, M.; Shuaib, K.; Sallabi, F. Softwarization of Internet of Things infrastructure for secure and smart healthcare. arXiv 2018, arXiv:1805.11011. Available online: https://arxiv.org/abs/1805.11011[accesat pe 6.11 2021].
210. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In Proceedings of the IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777.

211. Shae, Z.; Tsai, J.J.P. On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine. In Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 1972–1980. 212. Lei, A.; Cruickshank, H.; Cao, Y.; Asuquo, P.; Ogah, C.P.A.; Sun, Z. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. IEEE Internet Things J. 2017, 4, 1832–1843.

213. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Koreea, 19–22 February 2017; pp. 464–467.

214. Samaniego, M.; Deters, R. Internet of Smart Things-IoST: Using Blockchain and CLIPS to Make Things Autonomous. In Proceedings of the IEEE International Conference on Cognitive Computing (ICCC), Honulul, HI, USA, 25–30 June 2017; pp. 9–16.

215. Faruque, M.A.A.; Vatanparvar, K. Energy Management-as-a-Service Over Fog Computing Platform. IEEE Internet Things J. 2016, 3, 161–169.

216. SGao, S.; Peng, Z.; Xiao, B.; Xiao, Q.; Song, Y. SCoP: Smartphone energy saving by merging push services in Fog computing. In Proceedings of the IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), Vilanova i la Geltrú, Spain, 14–16 June 2017; pp. 1–10.

217. Dubey, H.; Monteiro, A.; Constant, N.; Abtahi, M.; Borthakur, D.; Mahler, L. Fog computing in medical Internet-of-Things: Architecture implementation and applications. In Handbook of Large-Scale Distributed Computing in Smart Healthcare, 1st ed.; Khan, S.U., Zomaya, A.Y., Abbas, A., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2017; pp. 281–321, ISBN 978-3-319-58280-1.

218. Rahmani, A.M.; Gia, T.N.; Negash, B.; Anzanpour, A.; Azimi, I.; Jiang, M. Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Gener. Comput. Syst. 2018, 78, 641–658.

219. Gia, T.N.; Jiang, M.; Rahmani, A.M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H. Fog computing in healthcare Internet of Things: A case study on ecg feature extraction. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology, Liverpool, UK, 26–28 October 2015; pp. 356–363.

220. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge Computing: Vision and Challenges. IEEE Internet Things J. 2016, 3, 637–646.

221. Ni, J.; Zhang, A.; Lin, X.; Shen, X.S. Security, Privacy, and Fairness in Fog-Based Vehicular Crowdsensing. IEEE Commun. Mag. 2017, 55, 146–152.

222. Markakis, E.K.; Karras, K.; Zotos, N.; Sideris, A.; Moysiadis, T.; Corsaro, A.; Pallis, E. EXEGESIS: Extreme Edge Resource Harvesting for a Virtualized Fog Environment. IEEE Commun. Mag. 2017, 55, 173–179.

223. Huang, Y.; Lu, Y.; Wang, F.; Fan, X.; Liu, J.; Leung, V.C. An Edge Computing Framework for Real-Time Monitoring in Smart Grid. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, USA, 21–23 October 2018; pp. 99–108.

224. Oyekanlu, E.; Nelatury, C.; Fatade, A.O.; Alaba, O.; Abass, O. Edge computing for industrial IoT and the smart grid: Channel capacity for M2M communication over the power line. In Proceedings of the IEEE 3rd International Conference on ElectroTechnology for National Development (NIGERCON), Owerri, Nigeria, 7–10 November 2017; pp. 1–11.

225. Muhammed, T.; Mehmood, R.; Albeshri, A.; Katib, I. UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities. IEEE Access 2018, 6, 32258–32285.

226. Barik, R.K.; Dubey, H.; Mankodiya, K. SOA-FOG: Secure service-oriented edge computing architecture for smart health big data analytics. In Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP), Montreal, UK, 14–16 November 2017; pp. 477–481.

227. Singh, D.; Tripathi, G.; Alberti, A.M.; Jara, A. Semantic edge computing and IoT architecture for military health services in battlefield. In Proceedings of the 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 185–190.

228. Aman, M.N.; Sikdar, B.; Chua, K.C.; Ali, A. Low Power Data Integrity in IoT Systems. IEEE Internet Things J. 2018, 5, 3102–3113.

229. Gope, P.; Sikdar, B. Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. IEEE Internet Things J. 2019, 6, 580–589.

230. Ahmed, S.; Lee, Y.; Hyun, S.; Koo, I. Feature Selection–Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning. IEEE Access 2018, 6, 27518–27529.

231. Ozay, M.; Esnaola, I.; Vural, F.T.Y.; Kulkarni, S.R.; Poor, H.V. Machine Learning Methods for Attack Detection in the Smart Grid. IEEE Trans. Neural Netw. Learn. Syst. 2016, 27, 1773–1786.

232. Zhang, D.; Han, X.; Deng, C. Review on the research and practice of deep learning and reinforcement learning in smart grids. CSEE J. Power Energy Syst. 2018, 4, 362–370.

233. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny, M.S.H. Application of Big Data and Machine Learning in Smart Grid and Associated Security Concerns: A Review. IEEE Access 2019, 7, 13960–13988.

234. Mercer, C. How Machine Learning Will Change Society. Available online: https://www.techworld.com/picture-gallery/techinnovation/5-ways-machine-learning-will-change-society-3666674[accesat pe 11.11 2021].

235. Chen, M.; Hao, Y.; Hwang, K.; Wang, L.; Wang, L. Disease prediction by machine learning over big data from healthcare communities. IEEE Access 2017, 5, 8869–8879.

236. Vito, S.D.; Francia, G.D.; Esposito, E.; Ferlito, S.; Formisano, F.; Massera, E. Adaptive machine learning strategies for network calibration of IoT smart air quality monitoring devices. Pattern Recognit. Lett. 2020, 136, 264–271.

237. Punithavathi, P.; Geetha, S.; Karuppiah, M.; Islam, S.K.F.; Hassan, M.M.; Choo, K.K.R. A lightweight machine learning-based authentication framework for smart IoT devices. Inf. Sci. 2019, 484, 255–268.

238. Bigini, G.; Freschi, V.; Lattanzi, E. A Review on Blockchain for the Internet of Medical Things: Definitions, Challenges, Applications, and Vision. Future Internet 2020, 12, 208.

239. Sepasgozar, S.; Karimi, R.; Farahzadi, L.; Moezzi, F.; Shirowzhan, S.M.; Ebrahimzadeh, S.; Hui, F.; Aye, L. A Systematic Content Review of Artificial Intelligence and the Internet of Things Applications in Smart Home. Appl. Sci. 2020, 10, 3074.