International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Understanding the Multifaceted Threats of Cyber security: A Comprehensive Analysis

Sapna , Ms.Shivani Anthal
Department of computer Applications
Chandigarh School of Business
Chandigarh Group of Colleges, Jhanjeri, Mohali,India
Sapna.ldh2002@gmail.com , Shivani.j2802@cgc.ac.in

Abstract- Cyber security exploration has significantly increased to give better protection for cyber operations and help significant security problems that may arise. The primary end of this exploration is to identify and understand common cyber security problems. In a recent study, experimenters examined 69 different studies to determine which types of security problems are constant and how severe they are. The experimenters anatomized colourful aspects similar to where the studies were published, which countries conducted the exploration, and the types of effects that were targeted by cyber-attacks. The findings of the study revealed that the current strategies used for cyber-security are veritably general, and the results they give bear further testing and real-world exploration to estimate their effectiveness.

1. Introduction

Cyber safety hazards constitute an increasing worry in the digital age of today, presenting difficulties for people, organizations, and countries alike. This study offers a thorough analysis of the different and constantly changing dangers that endanger the accessibility, security, and reliability of digital assets and information systems [1]. The security threats in cyberspace are evolving due to the increased availability of information sources and services. As technology advances, new types of cyber threats emerge, posing challenges to individuals and organizations. Staying vigilant and implementing robust security measures is crucial to mitigating these evolving risks in the digital landscape. Cyberattacks are increasing, and new cyber threats are becoming more widespread. In recent years, major incidents like the WannaCry ransomware and eBay data breaches have shown the security sector is facing significant challenges.

Organizations must stay vigilant and implement robust security measures to protect against these evolving threats. [2].

Students in Silicon Valley universities, an advanced technological community in the United States, for instance, reported minimal use of two-factor authentication or complex passwords for accounts, and they even felt at ease disclosing personally identifiable information to all members of the university community, even in the face of potential repercussions. [3]

According to the United Kingdom's cybersecurity survey, the most important target regarding detected possible hacks or breaches of information in 2020 will be organizations in the education sector. [4]

Over the past few decades, cyber security has advanced. When we find fraud, the first thing that springs to mind is cybersecurity. One of the main issues is the protection of personal data on the Internet. The number of [5] In recent years, connected devices have grown at a rapid pace, exceeding 50 billion by 2020. Dr. Yusuf Perwej, IJSRM Volume 09, Issue 12, December 2021 [www.ijsrm.in] EC-2021-670 The complexity of cyberinfrastructure has increased due to the increasing number of interconnected devices, leading to a rise in vulnerability levels [6].

Cybersecurity involves understanding different cyber pitfalls and creating defensive measures to guard the privacy, honesty, and validity of all computerized and data technologies. (2012) [7]

Privacy To help unauthorized people or systems from penetrating information, the term confidentiality is used.

integrity The term integrity is used to help unauthorized changes and elisions.

Vacuity The term' vacuity' is used to ensure that the mechanisms in charge of providing, storing, and recycling facts are available to those who need assistance.

Cyber security specialists widely believe that malicious software is the most important selection of weapons to commit cyber-attacks, which are intended to damage cyber security initiatives on the internet (2012). [8] Malicious software is a large category of attacks that are installed on a system, usually without the knowledge of the legitimate owner, and are designed to compromise the system to the

advantage of the adversary. Bots, Trojan horses, worms, viruses, and malware are some of the exemplary types of malware. [9]

2. Literature review

2.1 Background

Throughout the previous ten years, information and communication technology (ICT) has experienced substantial evolution, becoming widely used and deeply ingrained in our contemporary society.
The need for ICT systems and apps to be secure against cyberattacks is therefore being expressed by security policymakers today [14]. Cybersecurity is defending an ICT infrastructure from various cyber threats or attacks [15]. It encompasses various facets of cybersecurity, including safeguards for ICT, data and information in their raw form, and the processing and transfer of those elements. Associated fields of professional endeavour, the degree of protection offered by these measures, and the relationship between the physical and virtual components of the systems are additional factors [16].
Not all information security is, however, restricted to these three attributes; processes—privacy, identity, authentication, authorization, and accountability, for example—are also important aspects to take into account. In order to attain risk acceptance, risk management in this work refers to the entire risk management process, or, to be more precise, the ongoing identification, assessment, treatment, and monitoring of risks [18, 19]. Typically, information security risk is approached by breaking it down into three categories: assets, threats, and vulnerability [18, 19]. This is known as the risk analysis three-factor model. An information security risk assessment (ISRA) can be completed in a variety of ways. Nonetheless, most of them have in common that they identify an organization's significant assets first, followed by dangers that could jeopardize them [18].

With a logical classification and particular subtle components of different strike pushing devices, Hoque et al. [21] provide a comprehensive layout of DDoS attacks, their sources, and types. Additionally included are a detailed analysis of a few botnet models, mechanical assemblies created with the help of advantageous conditions and botnet outlines, and a bur-dens examination. Karim and associates [22]

Additionally, the study explores the changing threat landscape that is influenced by state-sponsored cyber warfare, geopolitical conflicts, and the unseen marketplace's monetization of cybercrime tools and services. For nations to efficiently identify and prevent future online risks, it highlights the crucial importance of a paradigm shift toward proactive intelligence regarding threats, threat hunting, and coordinated defensive mechanisms.

Cybersecurity has grown in importance as a worry for people, businesses, and governments in the current digital era. Given the growing utilization of technology, the possibility of cyberattacks also rises. This study paper's goal is to present a thorough examination of the many cybersecurity dangers. This essay will discuss the numerous kinds of cyber threats, including ransomware, phishing, and malware, and how they affect people, businesses, and governments. This study will also examine the standard practices for countering each kind of cyber threat.

Through rigorous examination and analysis, this research aims to provide a practical solution to reduce cyber security threats as well as a deeper understanding of this pressing issue.

2.2 Types of Cybersecurity Threats

What are the different categories of cyber threats (e.g., malware, phishing, ransomware)?

In today's digital environment, cyber risks are a constant source of concern. Although the article notes that there are numerous kinds of cyberattacks, it doesn't go into detail on the different kinds of cyberthreats [10]. Cyber dangers, which include malware, phishing, machine learning, artificial intelligence, and cryptocurrency attacks, are reportedly getting more complex [10][11]. One prevalent and widespread type of cyberthreat is malware [10][12]. This general word refers to a range of harmful software viruses, including trojans, worms, spyware, ransomware, and adware [10]. In addition to producing strange behavior when it installs undesirable software or programming on a target system, malware can also be used to spread to other systems, erase files, prevent access to programs, and steal data [12].

Phishing assaults, on the other hand, rank among the most common categories of cyberattacks [10]. These kinds of cybersecurity risks constantly jeopardize the assets and data of individuals, governments, and corporations [11]. As a result, it's critical to recognize these various types of cyberthreats and take the appropriate safety measures to keep them from doing damage.

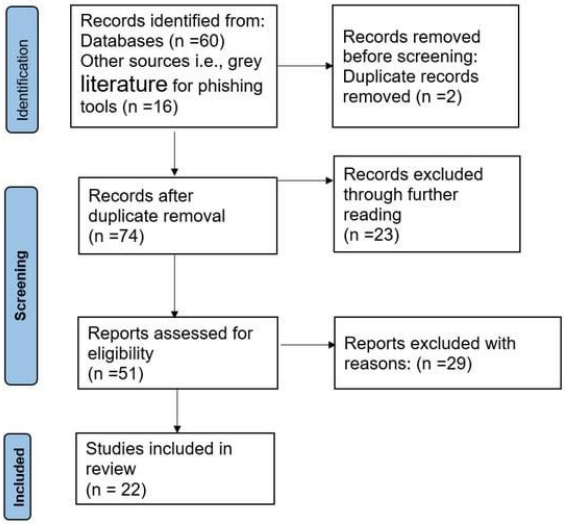


Figure 1. Report of literature: PRISMA diagram [19]

Fraudsters used 400.000 new malicious files each day (5% more than in 2021) to attack users in 2022. This information is based on the Kaspersky Security Bulletin (KSB) [23]. Researchers at Kaspersky Security found that, as of now, 9500 files are encrypted daily, an 181% increase in ransomware cases over 2021. Every day, 10% more malicious files targeting the Android platform are discovered by Kaspersky security experts.

Compared to 2021, when the ratio was 72.5%, the survey found that 90% of firms experienced ransomware in 2022 [24]. This is a huge increase. More than 50% of new malware is essentially a version of already existing malware, according to Symantec [25]. Furthermore, the AV-TEST Institute monitors about 450,000 new dangerous programs (malware) and perhaps undesirable apps (PUAs) each day [26].

demonstrates the malware's spread from January to June of 2022. We saw 28% harmful incursions, 53% malicious PDFs and office files, 105% ransomware, 167% encrypted threats, 19% crypto-jacking, and 6% IoT malware [27].

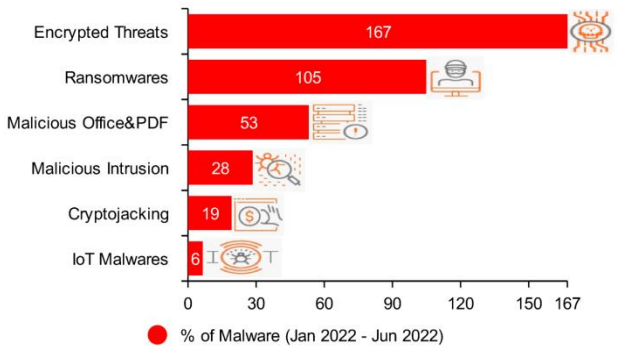


Figure 2. Global Malware trends by 2022

2.2.1 What are the common methods used to mitigate each type of cyber threat?

Users and organizations need to be proactive in preventing potential attacks in order to reduce cyber dangers. Anti-malware software can detect and stop dangerous software from running on a system, making it one of the most popular ways [12]. To prevent falling victim to phishing scams or other malware delivery methods, users should be mindful of dubious links, files, or webpages [12]. For the most part, malware can be avoided with a mix of common sense and antivirus software [12]. Via the use of a VPN, network communication can be encrypted as another popular defense against cyberattacks. This stops important information from being overheard and successfully conceals user behavior from possible attackers [12].

3. Cybersecurity Risk Management

A systematic set of actions make up the risk management process. To establish our risk management procedure, we adhere to the recommendations made by the ISO 310000 [30], NIST SP800-30 framework [31], and NERC CIP standards [32] risk management standards that are now in effect. There are six distinct sequential actions that make up the process. These activities are interconnected, and each activity includes procedures to support particular risk management duties**.**

3.1 Risk Assessment

It can be intimidating to think about the plethora of potential attacker exploits and techniques in cyber security [33]. Opportunistic attacks and targeted attacks are two different types of attacks. Instead of concentrating on how well a system can survive zero-day assaults, many cyber security risk assessment techniques focus on how susceptible a system is to known exploits. More importantly, in CSG, we look at whether defenses are put in place to make things as difficult as possible for the attacker and whether good security principles—such as least privilege, segmentation, diversity, etc.—have been followed.

The goal of this work is to "examine how cybersecurity investments are affected by uncertainties in cybersecurity risk assessment." Therefore, the goal of this paper is to further the field's earlier research [34, 35]. The foundational study assessed the values of the environment that were mimicked and considered them to be reliable. This implied that decisions taken with total confidence would be

informed by the choices of the tools that were put into use. Yet, it is impossible to fully trust the data due to the subjectivity and circumstances surrounding its collection.

Risk management is one domain in which this kind of approach is especially helpful. Experts evaluate risk frequently, and their judgment is determined by several variables, including their degree of risk tolerance. Furthermore, the results of deeds are seldom deterministic; instead, they rely on outside factors. Consequently, and in line with our methodology, performing a qualitative risk assessment is advised by the German Federal Office of Information Security. The architecture has been utilized to simulate security threats in vital utilities like water distribution systems, as reported in [36].

4. Emerging Trends in Cybersecurity

The transition to increasingly digitalized maritime infrastructures is now feasible thanks to recent developments in big data, artificial intelligence, and the Internet of Things (IoT) [37]. This indicates that a new evaluation of the cyber-security clause is now required.

4.1 Artificial Intelligence in Cybersecurity

Since the early days of artificial intelligence (AI), the idea of creating tools, software, or systems that are more intelligent than people has been "on the horizon" for research projects. AI was formerly known as machine intelligence. The issue is the expanding time horizon. as time goes on. We have observed how computers have determined a variety of displaying intelligence exhausting tasks, such as playing smart chess, as an example. [38]

from a human standpoint. Wherever there are exact algorithms that enable these methods, some of them have matured to a certain point. Certain approaches have gained so much recognition that they are now considered part of an application area rather than a subsection of artificial intelligence. Take data processing algorithms, which originated in the AI training domain. It may not be feasible to provide a comprehensive or nearly comprehensive assessment of all the useful AI techniques in a relatively short survey.[38]

Cybersecurity is one of the many fields that use artificial intelligence (AI). Artificial intelligence (AI) and machine learning can help hunt down cyber criminals, automate threat detection, and react faster than traditional software or human-driven systems, especially in light of the recent surge in cyberattacks and the proliferation of gadgets [39].

Gmail uses artificial intelligence (AI) to identify and block fraudulent emails and unsolicited spam. Users are contributing to the training of Gmail's artificial intelligence to identify spam in the future each time they click on an email message, regardless of whether it is spam [40]. Millions of users of Gmail have educated themselves about the service's artificial intelligence system.

4.2 Internet of Things (IoT) Security Difficulties

Device availability, processing system availability, and the proliferation of communication technology are all anticipated to fuel the explosive expansion of the explosive expansion of the Internet of Things (IoT). IoT security is therefore an important subject to discuss to safeguard the hardware and networks in the IoT system. [42]

The rapid growth of academic IoT security research is largely due to the availability of a tool for IoT or sensor network simulation and modeling. A comprehensive list of the simulators used in current research is provided by Chernyshev et al. [41]

A multitude of applications available on IoT devices are intended to simplify and ease daily living. Consider the possibility that engineers might remotely diagnose and fix any issue with a product. This occurs when an impending issue detected by the device has alerted the technical team to it before it becomes worse. [43]

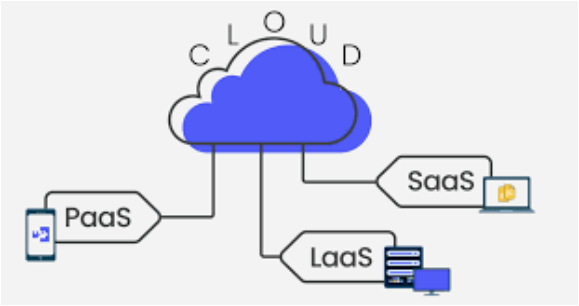
Smart cities, which combine intelligence with sustainability, are a prominent illustration of the uses of the Internet of Things. The application incorporates the entire infrastructure, several services, and technologies with ease. Here, wireless sensor networks and intelligent devices are successfully used by the Internet of Things network for monitoring and control [44].

4.3 Cloud Security Risks and Solutions

A variety of market and technological variables are contributing to the growing popularity of cloud computing. Numerous firms are altering their computing architecture due to swiftly evolving business situations. With new ones being introduced and old ones being eliminated, the number of enterprise services and apps is always growing. Parts of the operations of almost 75% of corporations in North America and Europe are outsourced. This suggests that pertinent business-related data is dispersed not just throughout various computing systems within an organization, but also among various IT infrastructures connected to the business network of the corporation.[46]

4.3.1 THE ARCHITECTURAL ELEMENTS

The three categories of cloud service models that are often represented by a particular cloud architecture are SaaS, PaaS, and IaaS.



IAAS: Infrastructure as a Service (IAAS) is one way to get computer infrastructure as an on-demand service. It's one of three main cloud service models. The user buys servers, software, data center space, or network equipment and rents them in an outsourced, on-demand service model. Dynamic scaling and resource distribution are supported. Many people are usually present on a single piece of hardware. In the end, the client must decide which resources are best for them, depending on their personal needs. Additionally, it provides billing management.

PAAS: PAAS, also known as Platform as a Service, is a cloud-based method of delivering applications made up of services under the control of a third party. Because it lets your application grow or shrink in response to demand, developers can create web apps and services more quickly. The available deployment models are public, private, or a mix of both. In other words, as part of the PAAS service, third-party suppliers supply the hardware and software for cloud computing. Developers utilize these technologies to create and maintain useful apps and services. The more dependable PAAS (also called Application PAAS) management solution makes IAAS (Infrastructure as a Service) less expensive overall.

SAAS:Web browsers are used by users to access software and related data that are centrally hosted under the Software as a Service (SaaS) paradigm. Users no longer need to install apps locally in order to use them. SaaS services are frequently utilized in the creation and implementation of contemporary apps. Because the program is given online, users do not need to handle software upgrades or the underlying infrastructure.

5. Future Range of Dangers to Cybersecurity

Given how quickly technology is developing, cybersecurity has a complicated and dynamic future. An important area of worry is the proliferation of Internet of Things (IoT) devices. It is projected that 41.6 billion IoT devices will be in use by 2025 [43]. Due to a lack of robust security features, a large number of these devices are unfortunately susceptible to illegal activity such as denial-of-service (DDoS) assaults and unauthorized access to private data [44]. Furthermore, as artificial intelligence (AI) and machine learning (ML) continue to advance, the field of cyber security is facing new opportunities and risks. While AI-driven security solutions improve threat detection, they also give hackers new ways to create automated attacks and advanced evasion strategies [45]. Attackers can undermine security protections by manipulating AI systems through adversarial machine learning, which is a growing danger that calls for proactive research and remedies[46]. Moreover, the use of quantum computing presents noteworthy obstacles to conventional encryption techniques. Current encryption standards may become out-dated if widely used cryptographic algorithms are broken by quantum computers [47]. To protect sensitive data in the post-quantum computing age, this calls for research into quantum-resistant cryptography and the creation of quantum-safe algorithms [48].

The weaponization of misinformation and disinformation campaigns in cyberspace becomes a key concern when considered within the framework of socio-political dynamics. Social media platforms and online channels are utilized by hostile enterprises and state-sponsored actors to disseminate propaganda, sway public opinion, and erode confidence in democratic institutions [49]. To effectively detect and mitigate this threat, interdisciplinary research combining expertise in data science, social psychology, and cybersecurity is needed [50].

6. conclusion

In the current digital age, cyber dangers are a constant cause of concern. The thorough analysis provided in this research study emphasizes the multifaceted character of these risks. The analysis shows that phishing, machine learning, artificial intelligence, malware, and crypto currency attacks are among the more complex forms of cyber threats. Additionally, the report makes the case that VPN encryption and network security solutions are popular defences against cyber-attacks. Cyber risks can influence people in a variety of ways, including governments, businesses, and individuals. This research paper's discussion part emphasizes the significance of comprehending the different types of cyber threats and putting in place practical countermeasures to lessen their detrimental consequences. Overall, this study adds to the body of information about cyber security and highlights the need for more research to defend against the wide range of cyber threats that exist in the modern digital world.

References

1. Cybersecurity Threats and Vulnerabilities : Systematic Mapping Study.
2. 3. Liu, Y., Peng, W., & Su, J. (2014). A study of IP prefix hijacking in cloud computing networks. *Security and Communication Networks*, *7*(11), 2201-2210.
3. 6. Moallem, A. (2019). Cyber security awareness among college students. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9* (pp. 79-87). Springer International Publishing.
4. 7. Garba, A. A., Jeribi, F., Al-Shourbaji, I., Alhameed, M., Reegu, F., & Alim, S. (2021). An Approach to Weigh Cybersecurity Awareness Questions in Academic Institutions Based on Principle Component Analysis: A Case Study of Saudi Arabia. *Int. J. Sci. Technol. Res*, *10*, 319-326.
5. 6. Dawson, J. and Thomson, R., "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance", Frontiers in Psychology, 9(JUN), pp. 1–12, 2018, doi: 10.3389/fpsyg.2018.0074
6. 7.C. L. Philip, Q. Chen and C. Y. Zhang, "Data-intensive applications challenges techniques and technologies: A survey on big data", Information Sciences, vol. 275, pp. 314-347, 2014
7. 18.S.E. Goodman, H.S. Lin (Eds.), Toward a Safer and More Secure Cyberspace, The Nat'l Academics Press (2007)
8. DHS S&T
   Roadmap for cybersecurity research
   Jan. 2009
   http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf
   last accessed: June 2013
9. Types of Cyber Attacks You Should Be Aware of in 2024. (n.d.) retrieved March 18, 2024, from www.simplilearn.com
10. Top Cybersecurity Threats [2023]. (n.d.) retrieved March 18, 2024, from onlinedegrees.sandiego.edu/top-cyber-security-threats/
11. Top 15 Types of Cybersecurity Risks & How To Prevent Them. (n.d.) retrieved March 18, 2024, from www.executech.com
12. Cybersecurity Threats: Everything you Need to Know. (n.d.) retrieved March 18, 2024, from www.exabeam.com/information-security/cyber-security-threat/
13. . Rainie, L., Anderson, J., & Connolly, J. (2014). Cyber attacks likely to increase
14. .Fischer, E. A. (2014). Cybersecurity issues and challenges: In brief.
15. Fischer, E. A. (2009). *Creating a National Framework for Cybersecurity: An analysis of issues and options*. Nova Science Publishers
16. Zhuang, R., Bardas, A. G., DeLoach, S. A., & Ou, X. (2015, October). A theory of cyber attacks: A step towards analyzing MTD systems. In *Proceedings of the second ACM workshop on moving target defense* (pp. 11-20).
17. Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. *International Journal of Information Security*, *17*, 681-699.
18. *ISO/IEC 27002:2013 Information Technology–Security Techniques–Information Security Risk Management*; Standard; International Organization for Standardization: Geneva, Switzerland, 2018.
19. PRISMA. PRISMA:Preferred Reporting Items for Systematic Reviews and Meta-Analyses. Available online: http://www.prismastatement.org (accessed on 4 August 2022)
20. Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS attacks: trends and challenges. *IEEE Communications Surveys & Tutorials*, *17*(4), 2242-2270.
21. Karim, A., Salleh, R. B., Shiraz, M., Shah, S. A. A., Awan, I., & Anuar, N. B. (2014). Botnet detection techniques: review, future trends, and issues. *Journal of Zhejiang University SCIENCE C*, *15*, 943-983.
22. Kaspersky Security Bulletin 2022. Statistics. Available online: https://securelist.com/ksb-2022-statistics/108129/ (accessed on 29 November 2022)
23. The SpyCloud Ransomware Defense Report. 2022. Available online: https://spycloud.com/resource/ransomware-defense-report-2022/ (accessed on 30 November 2022).
24. The Ransomware Threat Landscape. Available online: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-threat-landscape-what-expect-2022 (accessed on 19 October 2022).
25. Malware. Available online: https://www.av-test.org/en/statistics/malware/ (accessed on 16 October 2022)
26. /SonicWall Cyber Threat Report. Available online: https://theblockchaintest.com/uploads/resources/SonicWall%20-%20Cyber%20Threat%20Report%20-%202022%20Feb.pdf (accessed on 3 December 2022).
27. Airmic, A. (2011). IRM (2010). A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. *The Public Risk Management Association*.
28. Cybersecurity, C.I. Framework for Improving Critical Infrastructure Cybersecurity. Available online: http://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed on 29 May 2018).

29. . NERC, C. (2006). Standards as approved by the NERC board of trustees may 2006. *North American Electric Reliability Corporation: Atlanta, GA, USA*.
30. Dhanjani, N., Rios, B., & Hardin, B. (2009). *Hacking: The Next Generation: The Next Generation*. " O'Reilly Media, Inc.".
31. . Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., & Smeraldi, F. (2014). Cybersecurity games and investments: A decision support approach. In *Decision and Game Theory for Security: 5th International Conference, GameSec 2014, Los Angeles, CA, USA, November 6-7, 2014. Proceedings 5* (pp. 266-286). Springer International Publishing.
32. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision support systems*, *86*, 13-23.
33. Busby, J. S., Gouglidis, A., Rass, S., & König, S. (2016, October). Modelling security risk in critical utilities: The system at risk as a three player game and agent society. In *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 001758-001763). IEEE.
34. Bures, M.; Ahmed, B.S.; Rechtberger, V.; Klima, M.; Trnka, M.; Jaros, M.; Bellekens, X.; Almog, D.; Herout, P. PatrIoT: IoT Automated Interoperability and Integration Testing Framework. *Proceedings of the 2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST)*; Porto de Galinhas, Brazil, 12–16 April 2021; pp. 454-459.
35. Patil, P. (2016). Artificial intelligence in cybersecurity. *International journal of research in computer applications and robotics*, *4*(5), 1-5.
36. 6. C. Tschider, "Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age", SSRN Electronic Journal, 2018.
37. . C. Bitter, D. Elizondo and T. Watson, "Application of artificial neural networks and related techniques to intrusion detection", The 2010 International Joint Conference on Neural Networks (IJCNN), 2010
38. W. Feng *et al.*AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS Comput. Networks (2018)
39. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294
40. Nasser S. A., Andrew J., Olga A.," Internet of Things Security: A Review of Risks and Threats to Healthcare Sector ", IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, June 2017
41. **8** R. Petrolo, V. Loscrí and N. Mitton, "Towards a smart city based on cloud of things", *Proc. ACM Int. Workshop Wireless Mobile Technol. Smart Cities*, pp. 61-66, 2014
42. Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*, *59*, 126-140
43. Statista. (2023). Number of Internet of Things (IoT) connected devices worldwide in 2025. Retrieved from https://www.statista.com/statistics/1183457/iot-number-of-connected-devices-worldwide/
44. Zeadally, S., et al. (2020). Security and privacy issues in wireless sensor networks for healthcare applications. IEEE Access, 8, 37673-37700.
45. Swapan, M. S. I., & Ahmed, M. M. (2021). Applications of artificial intelligence in cybersecurity: A comprehensive review. IEEE Access, 9, 125678-125704.
46. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317-331.
47. Mosca, M. (2018). Why quantum computing poses an existential threat to blockchain systems. Retrieved from https://hackernoon.com/why-quantum-computing-poses-an-existential-threat-to-blockchain-systems-7a0a703c5be5
48. Chen, L., & Jordan, S. (2020). Post-quantum cryptography: Algorithms and implementations. CRC Press
49. Watts, C. (2021). Weaponizing disinformation: The threat to democracies. Journal of Strategic Security, 14(3), 57-73.
50. Shu, K., et al. (2019). Understanding misinformation propagation in social media: A review of current research and a way forward. ACM Computing Surveys (CSUR), 52(5), 1-36.