Communication in Physical Sciences, 2022, 8(4):707-720

A Detailed Review of Contemporary Cyber/Network Security Approaches and Emerging Challenges

.

Michael Oladipo Akinsanya, Oluwafemi Clement Adeusi, Kazeem Bamidele Ajanaku.
19 August 2022/Accepted : 12 November 2022/Published: 30 December 2022

Abstract: *This ability to use more digital technologies has exposed information systems to malicious actions and put their confidentiality, integrity, and availability at risk. The increasing difficulty in protecting critical assets against cybercriminals as cybercriminals are constantly changing tactics is an issue that organizations, individuals and governments are increasingly struggling with. What is bad about these threats is not necessarily their sophistication but the fact that conventional defense mechanisms do not have much sustainable capacity to combat these threats. To combat this ever-increasing threat, effective knowledge base must be established regarding the current state of security, and the changes that the attacks undergo. The goal of this research is to take an organized look at the existing environment of threats in the realm of cyberspace, the measures put in place in order to address these threats, and the gaps that require improvements through research. The review collates available literature findings with a view to identifying key challenges such as advanced persistent threats, zero-day exploits, and also risks posed by the increased use of emerging digital infrastructures. Next, it tries to analyze how innovative technologies. Artificial Intelligence (AI) and Machine Learning (ML) can be used in automating detection and response systems to improve resilience to dynamic attack. The findings not only describe the current situation in the sphere of cybersecurity but also outline its future trends pointing to the necessity of the perpetual innovation, collaboration of various stakeholders and versatile approaches to the threat environment that is changing very fast.*

Keywords: *AI, Cybersecurity, attacks, defense mechanism and trend.*

Michael Oladipo Akinsanya
Wichita State University,
Kansas State, USA.
Email: oladipoakinsanya@gmail.com

Oluwafemi Clement Adeusi
Department of Computer Science Network and Security, Staffordshire University, UK.
Email: ocadeusi@gmail.com

Kazeem Bamidele Ajanaku
Department of Mechanical Engineering, College of Engineering and Technology, Ladoke Akintola University of Science and Technology, Ogbomosho, Nigeria.

1. 0 Introduction

The high rate of internet advancements in recent decades has tremendously transformed the human society, economies and critical infrastructures. This change is commonly referred to as a digital revolution and it has increased the nature of communication, business, education, and governance thus rendering the internet to be an inevitable part of life (Kavak et al., 2021). Nowadays technology has been used in most of the activities that people and organization depend on in their daily lives especially in areas of banking, healthcare, gubernatorial processes, education, human resource management, smart cities, and energy systems (Ademilua, 2021; Ademilua & Areghan, 2022). . Although information and communication technology have created convenience, it has also created substantial security issues that warrant the concern of stakeholders at any level, whether on an

individual or national government level (Gunduz, 2022).

Due to the advancement in technology, security threats are increasing, and this poses a danger to an individual, organization and society. In order to address such risks, a set of measures are taken, namely legal regulations, social awareness raising, business ethics, and, most importantly, cybersecurity practices. Cybersecurity is protecting digital systems, assets, and the information in those systems against abnormal occurrences that hurt their operation. It is generally characterized by the maintenance of the confidentiality, integrity, and availability (CIA) of computer resources, be it of an individual or interconnected in the networks (Ullah et al., 2019). With above 60 percent industrial and social interactions today being done online, it is imperative to have good security standards in order to maintain a seamless, and secure exchange. To be successful in cybersecurity, strict attention should be paid to data protection, privacy, reliability, and service access, as these are the main aspects of cybersecurity (Kaur, 2022). Cybersecurity is considered one of the main options of preventing cybercrime and attacks to enable industries and societies to have secure interactions (Humayun et al., 2020). Therefore, the online safety of the users has become one of the most acute packing issues in the world (Kaur, 2022). With the increasing levels of digitalization, breaches can be rather costly not only personally or organizationally, but also as a national security issue and policy-making processes, as well as the robustness of the global infrastructure (Peters, 2015).

However, cybercrime cannot be dealt with solely by the use of technical solutions. A holistic approach that integrates an assortment of technology, the application of law and governance is needed. Effective policies and laws, as well as international cooperation, are needed so that the law enforcement agencies could investigate and prosecute freedom of crime (Tonge, 2013). Strict cybersecurity laws have been formulated by many countries, Ethiopia included, to ensure there is no breach and safeguarding sensitive information.

The importance of cybersecurity is made stronger by the fact that the current life is highly reliant on the digital system in terms of social stability and economic resilience. Cyberattacks may be devastating, involving losses of money, the image, and, in the case of vital industries like healthcare or power-generating, even human lives (Sharma, 2012). Cybersecurity is thus used in various fields about the importance of protecting sensitive data, infrastructures, and warrant integrity of the small enterprise, governmental organizations, military institutions, educational institutions, health care facilities, and energy frameworks (Arabo, 2015). New technologies have also changed the security terrain Artificial Intelligence (AI) and Machine Learning (ML) are growing in popularity used to locate threats, identify vulnerabilities, automate mundane work, and alleviate the pressure on people working in the sphere of security (Jang-Jaccard, 2014). The tools would assist in intrusion detection, malware analysis, vulnerability assessment, and will be able to respond to cyber challenges and their effects with speed and precision (Naik et al., 2019). The deployment of AI and ML into a defense can help organizations be more resilient against sophisticated attacks, but recent adversarial ML methods indicate such technologies are not out of reach of attackers (Maeda, 2021).

The cyber domain is a complex realm and requires continual research, innovation, and cooperation. Some past literature has underscored that cybersecurity is multidimensional and encompasses a variety of topics including technical countermeasures like firewall and encryptions as well as soften, like user education, training and other behavior intervention measures. In addition, international collaboration is essential, since cybercrime is usually cross-border. Creating a safe cyberspace thus needs an involvement of not just the

technical professionals but also policy-makers as well as business executives and individuals.

The importance of cybersecurity in the global sphere has led to the implementation of many sets of regulations and policies aimed to enhance resiliency. International institutions like the United Nations and the European Union have launched programs to foster international collaboration and enjoy the benefits of cross-country collaboration, governments across the globe have decided to adopt acts to safeguard the digital property of their citizenry and privacy (Humayun et al., 2020). However, the scope of the cyber threats has been increasing in spite of these efforts. Other types of attack like malware, ransomware, phishing, and denial of service have not stopped and more recently there have been supply chain attacks, misinformation and disinformation campaigns which have complicated security approaches (Thakur et al., 2015). Those threats have varied effects across industries and some sectors are more equipped than others. At the same time, a significant number of companies still do not have appropriate preparation and are generally unable to implement good practices like software updates, password management and cybersecurity training of the workforce (Srivastava et al., 2022).

As a measure to enhance resilience, organizations are embracing the use of more intrusion detection and prevention systems, antivirus programs, encryption schemes and comprehensive oversight applications. Security strategies are also affected by the emerging technologies. An example is blockchain that has possibilities of storing secure data and sharing information and quantum computing that has positive and negative implications on encryption systems. The increased adoption of cloud platforms offers scalability and flexibility to the user, and at the same time opens them to new threats. Therefore, the essence of the cybersecurity environment is that it actively adapts to the changes, where the innovations spawn opportunities and threats.

To conclude, cybersecurity has become the focus of sustaining trust and resilience in the digital age. The almost universal usage of the digital systems across all industries implies that confidentiality, integrity, and availability are no longer an extra perk but a requirement to have a chance at survival and further development. There is a lot of work done in terms of the development of defensive practices but rapidly changing threats require constant vigilance, innovation, and cooperation across national borders. Further studies should also pay attention to combining such future technology as AI, ML, blockchain as well as quantum systems, but keep in mind the legal, ethical and social aspects. In this paper, therefore, the challenges, applications, and emerging directions of cybersecurity are explored in order to deliver the insights that could be used with regard to informing research, policy, and practice.

2.0 Related Works

Research on cybersecurity and artificial intelligence (AI) has grown tremendously, some exploring the benefits, and others the challenges. The study by Zhang et al. (2022) gives an in-depth description of the ways that AI may be used to promote cybersecurity through its applications in detecting anomalies, intrusions, and malware. Their analysis underlines the advantages and the potential of using artificial intelligence in identifying aberrant patterns, but it also argues that further advancements of AI use face certain challenges, which include reliance on large data, the vulnerability of adversaries to using AI, and the need to have a human component to supplement the automated methods. Along the same line, Yazdinejad et al. (2022) suggested deep learning shapes combining deep learning models to identify anomalies in an Industrial Internet of Things (IIoT) environment. Their method, evaluated on data sets of gas pipelines and water treatment plants, has yielded virtually perfect accuracy levels of 99.3 and 99.7 ped cent, respectively, representing the potential power of AI of defect detection in critical infrastructure.

Cybersecurity has also found a role in the protection of smart grids. Threats discussed by Gunduz et al. (2022) include denial of service (DoS), phishing, and insider attacks, which can affect the power systems. In their proposal, they have considered using layered security solution that comprises technical protection and employee literature education as the necessary defense tools. In the same vein, Zhang et al. (2022) concentrated on the Internet of Things (IoT), where they have created a deep learning-based model of malware-detection of the infected files. The overall performance pushed toward 97.46% classification accuracy, confirming the potential effectiveness of AI in the effort to secure IoT devices.

Previous efforts paved the way to these advances. Abbas et al. (2019) examined how AI can be employed to carry out cybersecurity initiatives like malware detection and detection, intrusion detection systems, risk assessment and security automation. Their studies revealed that AI is a way more effective measure to enhance the decision-making processes and prevent threats than securing it by conventional means. In the same manner, Nayana et al. (2019) evaluated the monetary gains of cyber threat intelligence (CTI). They noted that organizations get the biggest benefit out of CTI when it decreases uncertainty about possible threats and underlined that the government agencies have to focus on sharing intelligence with companies that have less prior judgment of risk instead of focusing on the most rated vulnerabilities.

On IoT security, HaddadPajouh et al. (2018) also presented a deep recurrent neural network (DRNN) model that can detect malware. They noted that conventional signature-based detection was increasingly becoming ineffective as a result of the rapid evolution of malware. Their DRNN methodology proved more accurate, but a caveat was the ability of evasion techniques to bypass detection. Liew et al. (2021) have helped fulfill that mission by suggesting the approach of analyzing the safety and security of a cyber-physical system by using the Systems-Theoretic Process Analysis (STPA) and introducing custom metrics. Their combined structure enhanced the detection of high-risk situations and allowed more effective evaluation of the adversaries' exploitation capabilities.

Some of the previous works addressed domain-specific cybersecurity issues. Cheng et al. (2016) discuss the importance of AI on smart healthcare cybersecurity, which implies the increasing volume of medical information, the increase of medical expenses, and lack of professional providers. They stated that AI may enhance the detection of threats and efficiency in health care but also posed threats, such as the possibility of the misuse of AI system.

Overall, these works show that, although AI and machine learning are potent in terms of promoting cybersecurity in a wide array of domains such as smart grids, IoT and healthcare, they also bring about new threats. Among the crucial concerns, there is the reliance on good-quality data, the chance of adversarial misuse, and the potential necessity of human talent to monitor automatic systems.

3.0 Methodology

This systematic review was performed according to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines suggested by Barry et al. (2022). The current review took into account publications of 2013-2021 and included only materials of serious peer-reviewed journals written in English. Relevancy was considered by including only articles that were directly concerned with cybersecurity, its applications, and problems therein. Four of the largest databases were chosen to assure reasonable coverage of the literature i.e., IEEE Xplore, Scopus, Springer Link, and Web of Science. Such databases were selected since they have broad coverage of scholarly output in computing, engineering, and information sciences as three crucial areas of cybersecurity research.

The search strategy was created by using both keywords and Boolean logic to identify the most suitable studies on the issue of cybersecurity.

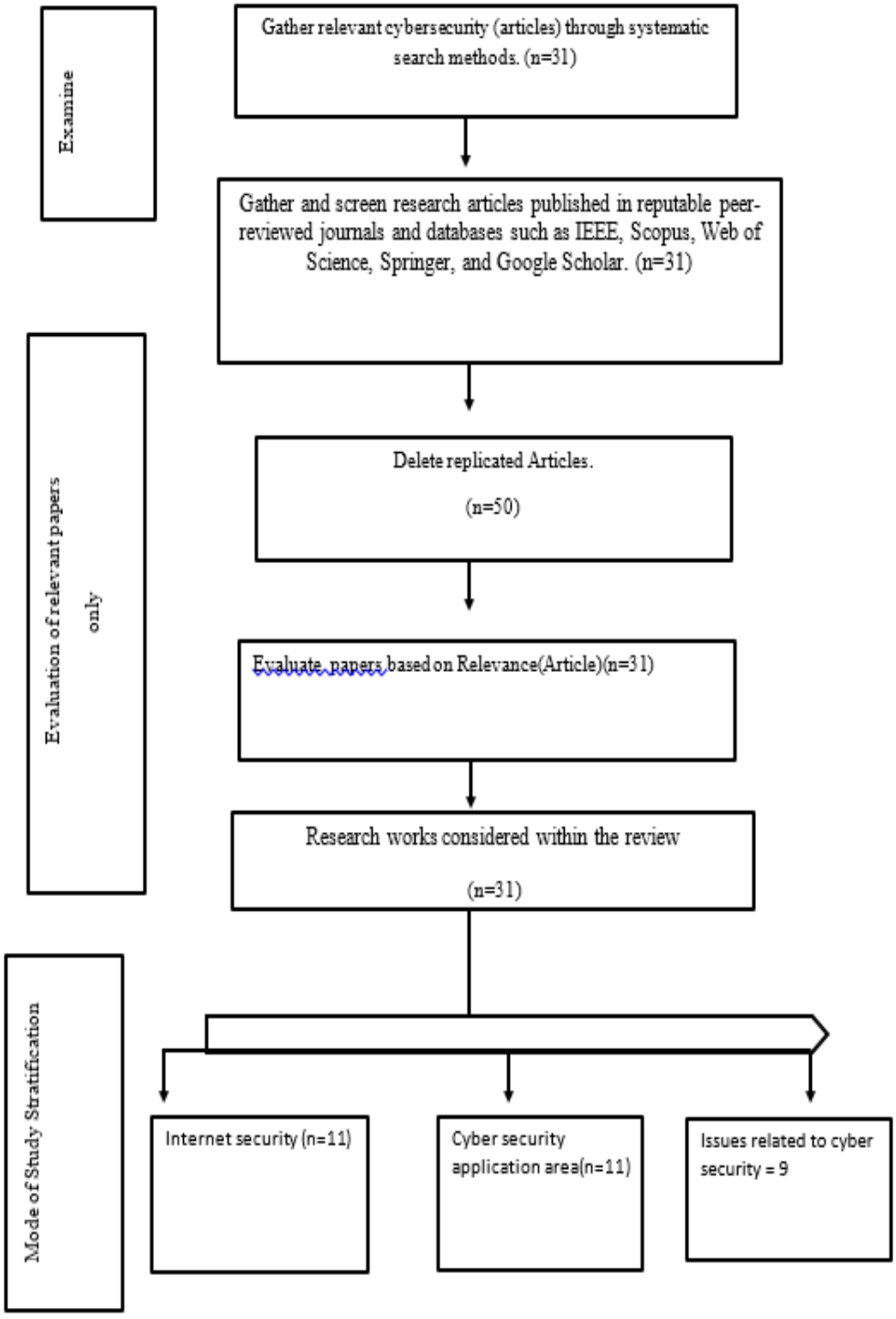

Fig1: Showing the search process and categorization of the studies.

The search has produced approximately 200 articles in the four databases. To tackle the results attained effectively, reference management tools were used to maintain a record and track the articles gathered. A critical filtering of the abstracts was done to identify relevance. The

articles were selected when the review of the abstracts showed that the articles are concerned with cybersecurity threats, countermeasure, or applications. This screening was done to further minimize the studies to 31, only after narrowing down to 40 studies, out of the 100 selected (Fig. 1). Further evaluation of the 40 articles on the websites was then carried out such that full article was read and its goals, methodologies and results evaluated. This was done to ensure that the end result of studies chosen to be analyzed were the most notable contributions that have been made in the given period of time and match with the research aims of the present review.

Academician, the researcher and the cyber security professionals must be geared towards the formulation of standard frameworks and platforms to exchange cyber threats and raise cooperative cyber defense solutions to agencies, industries, and governments. The issue of data protection and privacy is excruciating in the realms of the digital world and the concern towards the protection of data and privacy is rapidly rising. As such, the privacy regulations, data protection methods and privacy preservation techniques have to be enhanced and refined. Therefore, the researcher must be required to concentrate on ways of enhancing the privacy regulation, and privacy [reserving techniques employing multi-party homomorphic encryption technology and computation. Along with this, the advancements in blockchain technology are also among the essential issues to emphasize to the cyber security of the organization.

Table 1: Showing related works including findings and limitations

Authors	Paper	Approaches	Findings	Limitation
Kavak et. (2021)	Blockchain-assisted cyber security in medical things using artificial intelligence	Combination of blockchain and artificial intelligence (AI).	Blockchain was found to be effective in improving the security of medical records and detecting attacks on medical Internet of Things (IoT) devices.	Data on the security of medical devices is lacking. This makes assessing the efficacy of blockchain-based solutions for enhancing cyber security in medical devices challenging
(Ulah et al., 2019)	A Novel System-Theoretic Matrix-Based Approach to Analyzing Safety and Security of Cyber-Physical Systems	System-theoretic matrix (STM	The STM was useful for spotting possible risks and weaknesses as well as for developing mitigation plans.	The approach has only been used in one case study. For the process to be validated, further case studies are required. The methodology does not address the issue of uncertainty since the cyber-physical system is more complicated, making analysis unpredictable and exposing it to risk.

Yazdinejad etal. (2020)	An ensemble deep learning model for cyber threat hunting in the industrial Internet of things	LSTM and AE neural networks.	The model was able to detect cyber threats with high accuracy.	The model has only been evaluated on a dataset of Internet of Things (IoT) data from a single industrial control system. The model does not address the issue of false positives.
Humayun, et al.(2020)	Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems	Healthcare 4.0 and blockchain integration with secure cloud-based electronic health record systems	Develop mode secure and safe Model to Reduce the need for manual data entry and offer a safe and efficient means for authorized individuals to access electronic health records (EHRs) using Blockchain technology.	The issues are the high costs of running with blockchain technology and the shortage of skilled workers to use and operate the blockchain systems and deficiency in massively agreed standards to exchange data and privacy-preserving processes to share data.
Ullah et al. (2019)	Used Cyber threat Detection for Deep learning approaches for the Internet of Things (IoT)	The researcher uses combined deep learning approaches to detect the cyber security threat of malware attacks.	A cyber threat taxonomy model is developed to locate malware-based intrusion by tracing pirated software used as an avenue of attack on the Internet of Things (IoT) networks.	It requires significant computational resources and extensive datasets while overlooking adversarial attacks that are intentionally crafted to deceive deep learning models.
Langer (2017).	Developed an extensive review examining how machine learning (ML) is applied within the field of cybersecurity.	Systematic review on the role of machine learning in cyber security	The paper indicates the challenges facing application of machine learning to cybersecurity such as the requirement of large labeled data, difficulty of interpreting its model, and likelihood that it is vulnerable to	The researcher does not address antimachine learning attacks and their challenges

	adversarial manipulations.

Distributed ladder system and blockchain technology give an excellent suggestion to safety and decentralized systems and various researchers have studied the application of blockchain technology in a variety of cybersecurity fields like transaction (Peters and Panayi, 2015) supply chain (Dutta, 2020) and in medical. Although blockchain technology can be credited with a significant part to play in offering security measures to the cyber security sector, there exist security complications and obstacles which include irreversible or unalterable transactions the malleability of smart contact, weakness of blockchain technology protocols like consensus protocol such as PoS and PoW to be attacked, reliance on outside system like oracle is other security problem with blockchain technology. To curb or reduce such type of security issues and concerns in Blockchain technology, proper security measures need to be taken and carried out like; using secure smart contract development techniques, deployment of robust consensual protocols, integration of desired privacy enhancing techniques and implementation of such measures would do so. To develop a secure and resilient system, it is important that the benefits of blockchain and DLT and associated cybersecurity problems are balanced (Fig. 1 and Table 1).

4.1 Challenges of Cybersecurity

In the modern digitalized environment, people, organizations, and governments face the urgent problem of cybersecurity. As the rate of technology expands and there is general increase in digital devices, it has been more crucial to have information networks, systems and data secure and guarded against intrusion, theft or other destruction. Although some achievements have been obtained in the sphere of technologies, the security of such important assets and information is still a challenging process. It is in this section that the significant challenges on cybersecurity are outlined as well as the potential areas of enhancement.

4.2 Delicate character of cyber attack

The complexity of the attacks to fix the computer systems and networks is one of the greatest threats that are increasing due to cyber-attacks (Tankard, 2011). Cybercriminals are constantly inventing new and sophisticated tools and techniques to attack weaknesses. Such malware include multi-vector attacks, polymorphic as well as file less malware, zero-day exploits and advanced persistent threats (Sharma, 2012).

The Advanced Persistent threats (APTs) are directed and well-organized attacks that target vulnerable areas within the high value sectors like defense, government, technology and manufacturing. Usually, these attacks are state-sponsored, or supported by criminal groups with political, economic, or strategic interests (Prenosil, 2014; Hejase, 2020). The remarkable one is the case of Operation Aurora (2009), as it targeted large corporations such as Google and Adobe by stealing intellectual property using highly sophisticated tactics (Tankard, 2011; Prenosil, 2014; Hejase, 2020).

Another severe problem is zero-day exploits, which are attacks against the weaknesses unsuspected by the software programmer and the security specialists. Attackers use these flaws to compromise the systems before patches are delivered (Kaur, 2014). An example of this would be Stuxnet, which was a very sophisticated worm that pillaged supervisory control and data acquisition (SCADA) systems of the Iranian nuclear facility utilising various zero-day vulnerabilities to deactivate the centrifuge activity (Arabo, 2015). Zero-day exploits are known to have a long life cycle (outcome) timeframe in terms of discover and exploit, disclose and patch which makes it hard to identify and protect.

4.3 Internet of things (IOT) Security

Various devices connected on the Internet of Things (IoT) number in billions across the globe and are designed to be convenient, yet they are posing new challenges to cybersecurity. The low processing capability of IoT devices, lack of update, old or mediocre firmware, default settings with low security strength are concepts that predispose them to exploitation (Clark & Van Oorscot, 2013).

The next critical issue is data privacy as the IoT devices pick up huge volumes of very sensitive personal and corporate information. Secure storage and weak encryption predispose the risk and chances of being hacked illegally. Moreover, the use of wireless communication channels like Wi-Fi, Bluetooth and mobile networks introduces a possibility of an attacker to intercept or tamper with the communications or downright interfere (Clark & Van Oorscot, 2013; Gunduz, 2022).

4.4 AI - Driven attacks

Artificial intelligence (AI) and machine learning are versatile technologies that can not only strengthen cybersecurity but also be used to fuel cybercrime by malicious actors AI-powered attacks can be classified into two major types, AI-assisted attacks, where the AI becomes an aid to human attackers supporting them in their planning and execution of cybercrimes, and autonomous AI attacks, where an AI system is the engine that launches cybercrimes and drives them forward through adaptation. These threats have various forms such as in the deep fake attacks, which involves falsifying images, videos, or audio files using an AI system with the purpose of deceiving the systems during social engineering malicious activity attempts, or impersonating other individuals, sometimes without violating biometric authentication or spreading fake news (Vouvoutsis et al., 2022). Likewise, botnets use networks of hacked devices to perpetrate high-volume operations like distributed denial-of-service (DDoS) attacks, spamming, and data theft, and AI technologies can help increase their capacity to target individuals, grow fast, and avoid detection. Also, reinforcement learning allows dynamic adaption of the strategies by AI-enabled attacks to optimize their effectiveness according to feedbacks made by the targeted systems. The combination of these AI-based threats has strong adaptive qualities with rapid movement and is becoming hard to detect making it one of the most significant threats in current cybersecurity issues.

4.5 Cloud Computing

Cloud computing is also coming in with more vulnerabilities due to the rising usage of such computing. Cloud services have charms like flexibility and scalability to organizations and also, it is exposed to risks like data breaches and unauthorized access, unsecure APIs, and shared infrastructure risks. The result of these weaknesses may include service failure, loss of data, and loss of confidentiality which is a great risk to the organizations depending largely on the use of cloud environments.

4.6 Future research and Emerging challenges

The field of cybersecurity is open to challenges and opportunities and could be a fast-changing environment, but as well there are a number of recently emerging research areas that could provide possible solutions. Automation of controls, real-time threat recognition, analysis of large quantities of data, and streamlined responses are being captured on Artificial intelligence and machine learning that will be generalized to learning as well as dynamic responses. Combination of traditional biometrics authentication, facial recognition or fingerprint scan, with measures, e.g. password protection can offer higher levels of security against unauthorized users. Quantum computing has also brought the importance of quantum-resistant cryptography where the encryption system is also secure in the post-quantum era. Additionally, a more human centered approach to security that focuses on awareness and training along with a role of user behaviour in protecting systems, become more important. These strategies are the creation of user-friendly interfaces, security education fostering, and investigation of socio-

technical approaches that enhance human factor side of cybersecurity. Another major direction is automation of incident response and intelligent orchestration platforms and frameworks are being developed to increase efficiency and minimize the time needed to respond. Of equal significance is the improved intelligence of any threat and provision of supporting information so that cooperation of the industries, governments and institutions is enhanced to allow anticipation, prediction, and minimization of any threat of an impending attack. Together, these developments will be critical in enhancing cybersecurity across the world and developing resiliency to new threats with elevated sophistication.

5.0 Conclusion

Cybersecurity is the practice focused on shielding internet systems, networks, or confidential information against malicious operations that compromise the sufficiency of confidentiality, integrity, and availability. With more and more industries relying on technology (healthcare, finance, education, defense, energy, and governance systems, etc.), the need to protect the underlying digital infrastructure has become critical. The threat environment is versatile such as malicious hackers and cybercriminals, state-sponsored hackers, terrorist attackers, and internal threat. Emerging threats are advanced persistent threats, AI-based malware, reinforcement learning-based intrusions, vulnerability of Internet of Things (IoT) devices, weak cryptographic methods, and cloud platform vulnerability.

In the future, such phenomena as quantum-safe cryptography, biometric authentication, and knowledge-based systems with the help of artificial intelligence and machine learning can improve digital defense. Technological innovation is not sufficient in order to attain resilience. It asks long-term investments, inter-sectoral cooperation, and some initiative among people, institutions, and states. Cybercrime as an issue is still growing in both scope and scale with an evolving number of tools and disruptive technologies that require equally dynamic solutions.

There is still no chance to make any system impenetrable in terms of cyberattacks, however, constant innovation, robust governance, and more human-centered activities can help to minimize the risks. Creating a safe and reliable cyber is thus not a sole or a single initiative, but one that has to be carried out continuously to achieve assurance, continuity, and certainty in a fast-developing interconnected world.

6.0 References

Ademilua, D.A. (2021). Cloud Security in the Era of Big Data and IoT: A Review of Emerging Risks and Protective Technologies. *Communication in Physical Sciences*, 7, 4, pp. 590-604

Ademilua, D. A., & Areghan, E. (2022). AI-Driven Cloud Security Frameworks: Techniques, Challenges, and Lessons from Case Studies. *Communication in Physical Sciences,* 8, 4, pp. 674–688

Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, 121, 2, pp. 1189–1211. https://doi.org/10.1007/s11192-019-03222-9

Arabo, A. (2015). Cyber security challenges within the connected home ecosystem futures. *Procedia Computer Science*, 61pp. 227–232. https://doi.org/10.1016/j.procs.2015.09.201

AsSadhan, B., & Moura, J. M. F. (2014). An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic. *Journal of Advanced Research,* 5, 4, pp. 435–448. https://doi.org/10.1016/j.jare.2013.11.005

Barry, E. S., Merkebu, J., & Varpio, L. (2022). State-of-the-art literature review methodology: A six-step approach for knowledge synthesis. *Perspectives on Medical Education*, 11, 5, pp. 281–288. https://doi.org/10.1007/s40037-022-00725-9

Cheng, Y.-L., Lee, C.-Y., Huang, Y.-L., Buckner, C. A., Lafrenie, R. M., Dénommée, J. A., Caswell, J. M., Want, D. A., Gan, G. G., Leong, Y. C., Bee, P. C., Chin, E., Teh, A. K. H.,

Picco, S., Villegas, L., Tonelli, F., Merlo, M., Rigau, J., Diaz, D., ... Mathijssen, R. H. J. (2016). Smart health and cybersecurity in the era of artificial intelligence. In *Advanced biometric technologies* (p. 13). Intech. https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics

Clark, J., & Van Oorschot, P. C. (2013). SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. In *Proceedings - IEEE Symposium on Security and Privacy* (pp. 511–525). IEEE. https://doi.org/10.1109/SP.2013.41

Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E: Logistics and Transportation Review, 142*, 102067. https://doi.org/10.1016/j.tre.2020.102067

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094

HaddadPajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R. (2018). A deep recurrent neural network based approach for Internet of Things malware threat hunting. *Future Generation Computer Systems*, *85*, 88–96. https://doi.org/10.1016/j.future.2018.03.007

Hejase, H. J., Kazan, H., & Moukadem, I. (2020). Advanced persistent threats (APT): An awareness review. *Journal of Economics and Economic Education Research*, 21, 6, pp. 1–8. https://doi.org/10.13140/RG.2.2.31300.65927

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering*, 45, 4, pp. 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80, 5, pp. 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences*, 34, 8, pp. 5766–5781. https://doi.org/10.1016/j.jksuci.2021.01.018

Kaur, R., & Singh, M. (2014). A survey on zero-day polymorphic worm detection techniques. *IEEE Communications Surveys & Tutorials*, 16, 3, pp. 1520–1549. https://doi.org/10.1109/SURV.2014.022714.00160

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: State of the art and future directions. *Journal of Cybersecurity*, 7, 1, pp. 1–13. https://doi.org/10.1093/cybsec/tyab005

Langer, S. G. (2017). Cyber-security issues in healthcare information technology. *Journal of Digital Imaging*, 30, 1, pp. 117–125. https://doi.org/10.1007/s10278-016-9913-x

Liew, L. S., Sabaliauskaite, G., Kandasamy, N. K., & Wong, C. Y. W. (2021). A novel system-theoretic matrix-based approach to analysing safety and security of cyber-physical systems. *Telecom*, *2*(4), 536–553. https://doi.org/10.3390/telecom2040030

Maeda, R., & Mimura, M. (2021). Automating post-exploitation with deep reinforcement learning. *Computers & Security*, 100, 102108. https://doi.org/10.1016/j.cose.2020.102108

Naik, L. B., AsSadhan, B., Moura, J. M. F., Saadawi, T., El-Desouki, A., Elmaghraby, A. S., Losavio, M. M., Rao, U. S., Swathi, R., Sanjana, V., Arpitha, L., Chandrasekhar, K., Chinmayi, P. K., Naik, P. K., Alshehri, M., Ben-asher, N., Gonzalez, C., Alshehri, M., Hemminghaus, C., ... Ddos, S. (2019). Special issue on cyber security and AI. *Journal of Advanced Research*, 41, 5, pp. 557–559. https://doi.org/10.4218/etr2.12236

Peters, G. W., & Panayi, E. (2015). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.2692487

Prenosil. (2014). Advanced persistent threat attack detection: An overview. *International Journal of Advancement in Computer Networking and Security (IJCNS)*, 4, 4, pp. 50–54. https://www.researchgate.net/publication/305956804

Sabaliauskaite, G., Cui, J., & Liew, L. S. (2018). Integrating autonomous vehicle safety and security analysis using STPA method and the six-step model. Retrieved from https://www.researchgate.net/publication/326504334

Sharma, R. (2012). Study of latest emerging trends on cyber security and its challenges to society. *International Journal of Science and Engineering Research*, 3, 6, pp. 1–4.

Srivastava, G., Jhaveri, R. H., Bhattacharya, S., Pandya, S., Rajeswari, P. K. R., Maddikunta, G., Yenduri, G., Hall, J. G., Alazab, M., & Gadekallu, T. R. (2022). XAI for cybersecurity: State of the art, challenges, open issues and future directions. *arXiv*. http://arxiv.org/abs/2206.03585

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security*, 2011, 8, pp. 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2016). An investigation on cyber security threats and security models. In *Proceedings - 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015* (pp. 307–311). IEEE. https://doi.org/10.1109/CSCloud.2015.71

Tonge, A. M. (2013). Cyber security: Challenges for society - Literature review. *IOSR Journal of Computer Engineering*, 12, 2, pp. 67–75. https://doi.org/10.9790/0661-1226775

Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in Internet of Things using deep learning approach. *IEEE Access*, 7, pp. 124379–124389. https://doi.org/10.1109/ACCESS.2019.2937347

Vouvoutsis, V., Casino, F., & Patsakis, C. (2022). On the effectiveness of binary emulation in malware classification. *Journal of Information Security and Applications*, 68, 103258. https://doi.org/10.1016/j.jisa.2022.103258

Yazdinejad, A., Kazemi, M., Parizi, R. M., Dehghantanha, A., & Karimipour, H. (2022). An ensemble deep learning model for cyber threat hunting in industrial internet of things. *Digital Communications and Networks*, 9, 1, pp. 101–110. https://doi.org/10.1016/j.dcan.2022.09.008

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. K. R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review*, 55, *2, pp.* 1029–1053. https://doi.org/10.1007/s10462-021-09976-0.

Consent for publication

Not Applicable

Availability of data and materials

The publisher has the right to make the data public

Competing interest

Authors declared no conflict of interest.

This work was sole collaboration among all the authors

Funding

There is no source of external funding

Authors Contributions

Michael Oladipo Akinsanya conceptualized the study, developed the research framework, and provided critical revisions that shaped the overall direction of the work. Oluwafemi Clement Adeusi reviewed and synthesized relevant literature, analyzed the role of AI and ML in cybersecurity, and contributed to drafting significant portions of the manuscript. Kazeem Bamidele Ajanaku organized the structure of the review, addressed emerging challenges such as zero-day exploits and advanced persistent threats, and ensured clarity and coherence in presenting findings before final submission.