Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

The Evolution of Cybersecurity: Analyzing Modern Threats, Overcoming Challenges, and Shaping Future Directions

Ahmad Musa Bulama
Integral University, Dasauli, Bas-ha Kursi Road, Lucknow – 226026 Department of computer Application
[0009-0007-5543-8367]

Mohammad Faisal
Integral University, Dasauli, Bas-ha Kursi Road, Lucknow – 226026 Department of Computer Application
[0000-0002-6120-5259]

Abstract*— *Cyber security represents an emerging area that requires serious attention from experts, institutions, as well as the government, in order to protect information systems from advanced attacks. Owing to the accelerated process of digitalization, people as well as business entities have been presented with the dynamic nature of cyberspace threats that pose a high risk to the confidentiality, integrity, and availability of information. The paper presents an in-depth scientific review on the current state-of-the-art for the area of cybersecurity, as it identifies the key challenges as well as the strategic trends for the area in the next studies. The paper will also examine the application of Artificial Intelligence (AI) and Machine Learning (ML) approaches for the improvement of the effectiveness of the existing cybersecurity systems.

Keywords— Artificial intelligence, cyber-attacks, information role, information security.

I. INTRODUCTION

In relation, the rapid diffusion of internet technology, along with digital development, has profoundly changed world civilization in terms of ways of communication, as well as business and governmental functions and infrastructure [1]. This sort of digital transition is referred to as "cyber civilization," which is crucial for most sectors like banking, health and education, and smart infrastructures. With rapid expansion in digitalization, large-scale cybersecurity threats are emerging for which active protection methodologies are required at each scale of an organization [2].

Protecting computer systems, networks, and data against cyber threats means applying various techniques of cybersecurity with the purpose of preserving the confidentiality, integrity, and availability of the systems [3]. This is because the increasing use of digital communication stands at over 60% of the total communications of the world [4], making security an important area that organizations, governments, or institutions should focus on.

Network security is always relevant in the modern technological age, as technology supports every function of our lives. The effect of cyber-attacks could be catastrophic, leading to compensation, loss of reputation, and loss of life, especially within the medical and power sectors [5]. Data and vital infrastructure protection demand that the confidentiality and integrity of such information must be upheld. The application of network security, according to [6], must not only take place within the state and the military, small businesses, medical facilities, learning institutions, power companies, and transportation service providers, among others, need to apply this technology.

Artificial Intelligence (AI) and Machine Learning (ML) technology have proved vital for the detection of threats, scanning the networks for vulnerabilities, as well as decreasing the IT workloads [7]. There are numerous cybersecurity processes that can be made autonomous through the application of AI and ML, making room for experts to focus on other high-level tasks [8]. Organizations today have started to employ the applications of AI and ML as tools within the cybersecurity defense against advanced threats [9], AI and ML have revolutionized the field of cyber defense. But the recent trend of anti-ML attacks introduces new complexities. The need to explore new avenues of research related to the existing and prospective challenges faced by the field of cyber security is being highlighted in this paper, which focuses on AI, ML, and other advanced technologies being employed to counter cyber threats.

II. APPLICATION AREAS OF CYBERSECURITY

- **Cybersecurity in Smart Grids**.

Smart grids also consist of advanced technologies in computing and communication in an attempt to optimize the production of power as well as its transmission and consumption. Cyber-attacks such as denial of service and user access to vital information have the potential to affect the smart grid systems [10]. For the process to be effectively and successfully implemented, a vast number of devices have to be automated and traced. Analysis and control of an extremely high number of devices have to be done for the success of this particular process and therefore the aim of smart grid technology. This has to be accomplished by doing automation of the smart grid technology.

IoT is a network of interconnected, interdependent, physical objects that communicate among themselves and the external and internal environment through the Internet using embedded technology. They independently or collaboratively perceive, sense, analyze, control, and make decisions with other devices. They utilize two-way communication and high-speed control capabilities, important for both IoT and the smart grid [11]. Security in communications, data encryption, and threat

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

monitoring are necessary protocols to ensure the integrity and confidentiality of data in smart grids [12].

- **Cybersecurity in Vehicular Communication**

Information and telecommunications integration in road transportation systems is referred to as Intelligent Transportation Systems (ITS). Vehicular Ad-hoc Network (VANET) is applied for inter-vehicle communications through a wireless connection between vehicles. VANET applies two main communication systems, which include Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication. From V2V communications, a vehicle is capable of sharing information relating to traffic, such as speed, direction, road conditions, traffic congestion, and accidents, with other vehicles.

[13] Vehicle-to-vehicle communications' cybersecurity is a significant issue pertaining to safety, efficiency, as well as the privacy within the vehicle communications process. Damages such as those on the ECUs, sensors, as well as communications networks can affect the management of traffic flow by posing a danger to the passengers on board [14]. The following are significant factors considering vehicle communications' cybersecurity:

- **Cyber Security in Smart Cities**

The internet and communication technologies are growing in numbers, bringing about substantial changes in society and the economy, shaping the future of smart cities. With an exponential increase in the use of mobile devices and computers, which in turn contributes to enhanced data volumes, cutting-edge technologies are being developed in the forefront. These include fifth-generation wireless networks, also known as 5G, and the Internet of Things (IoT), which are improving wireless connectivity capabilities [15].

Smart cities are harnessing the potential of connected devices and infrastructure to create life in urban environments. Nevertheless, with the increasing use of IoT devices comes the challenge of potential surveillance and breaches of privacy and security. Cybersecurity efforts have to counter potential weaknesses in energy, water, transport, and communications infrastructure to guarantee privacy and protection from cyberattacks [16]. Some of the smart city services being implemented are characterized by near-zero latency to guarantee that they work flawlessly and perfectly. To guarantee that the privacy of smart grid data is maintained, there has to be proper security in communications and surveillance [17].

- **Cyber Security in eHealth Systems**

Advancements in information technology serve as a foundation for adopting the Internet of Things (IoT) across various aspects of our lives. One domain where IoT can have a transformative impact is healthcare, revolutionizing how services are delivered. Healthcare systems integrating IoT devices for remote monitoring and diagnostics are especially vulnerable to cyberattacks, as the data exchanged is highly sensitive and closely tied to patients' private lives [18]. Data breaches in this context can lead to the exposure of confidential patient information and the disruption of medical services. Unlike traditional computer networks, IoT introduces unique risks that require special attention. Consequently, robust encryption, secure communication protocols, and strict adherence to privacy regulations are essential for protecting healthcare data [19].

III. State of the Art.

In the early days of computing, cybersecurity primarily focused on protecting standalone systems from viruses and malware. Over time, it has become a growing concern requiring the attention of researchers and organizations to ensure the confidentiality, integrity, and security of information systems. By the 2000s, cyber threats had become more organized, with attacks such as phishing, ransomware, and advanced persistent threats (APTs) increasingly targeting businesses and governments. As digitalization continues to expand, both individuals and organizations face a growing variety of cyber threats, including newer forms such as misinformation campaigns and supply chain attacks [20]. To mitigate these risks, stakeholders commonly employ technologies such as intrusion detection systems, firewalls, and antivirus software, along with best practices like regular software updates and cybersecurity training [21].

IV. Related Work

Cybersecurity has undergone a significant transformation over the past few decades, evolving from basic antivirus programs to complex defence mechanisms against sophisticated cyber threats. [22] have explored the use of Artificial Intelligence in healthcare cybersecurity, emphasizing the need for big data and human oversight. While [23] & [24] in their studies proposed deep learning methods for threat detection in IoT and industrial environments. [25] & [26] investigated blockchain's potential in securing medical data and cloud-based health records. [27] & [28] in their research examined the impact of threat intelligence and strategic beliefs in cybersecurity policy and practice.

[29] Their studies provide a comprehensive overview of the use of artificial intelligence (AI) in cybersecurity and discuss the challenges and opportunities of using artificial intelligence (AI) in cybersecurity. They discuss how artificial intelligence (AI) can help tackle cybersecurity challenges, focusing on its applications in areas like anomaly detection, intrusion detection, and malware analysis. The discussion highlights both the opportunities and challenges of applying artificial intelligence (AI) in cybersecurity. Key concerns include the reliance on large datasets, the risk of adversaries exploiting AI, and the continued need for human oversight to ensure its responsible and effective use. The article concludes by exploring how AI could shape the future of cybersecurity and enhance its overall effectiveness.

V. Methodology

- **Selection Criteria**

This review was conducted in line with the PRISMA guidelines [30], which offer updated standards for reporting systematic reviews. The PRISMA 2020 framework reflects the latest methodologies for identifying, selecting, evaluating, and synthesizing relevant research. For this review, we focused on peer-reviewed articles published in English between 2011 and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

2023, specifically those addressing cybersecurity applications, challenges, and emerging technologies.

- **Information Sources**

To ensure comprehensive coverage of the field, we drew from well-established academic databases, including IEEE Xplore, Scopus, SpringerLink, and Web of Science. These platforms offer a broad range of high-quality literature in the area of cybersecurity.

- **Search Strategy**

A combination of targeted keywords and Boolean operators was used to search for relevant studies. The articles that were selected for inclusion were selected from a pool of 100 articles based on their relevance, and their full-text results were also taken into account for their inclusion.

VI. CHALLENGES IN CYBERSECURITY

Cybersecurity has become more important than ever in our increasingly internet-connected world. As people, businesses, and government organizations depend more on digital tools and technologies to protect devices, networks, and sensitive data from cyber threats has become a top priority. while technology continues to advance rapidly, so do the methods used by cybercriminals. This makes it a constant challenge for organizations to keep their systems secure and their people and assets protected. In this article, we'll take a closer look at the major challenges facing the cybersecurity industry today and explore where the field is headed.

- **Advanced Persistent Threats (APT)**

APT is a type of attacks that involve sophisticated and targeted operations, often by state-sponsored actors, aiming to infiltrate critical sectors like defense and energy [31]. It is the authors' intent to provide researchers and practitioners with a formal definition of malicious, coordinated, highly skilled entities that conduct long-term or repetitive network penetrations and exploitations to obtain data from a target organization, destroy its operations, or both. Zero-day exploits, used in APTs, remain undetected due to unpatched software vulnerabilities [32].

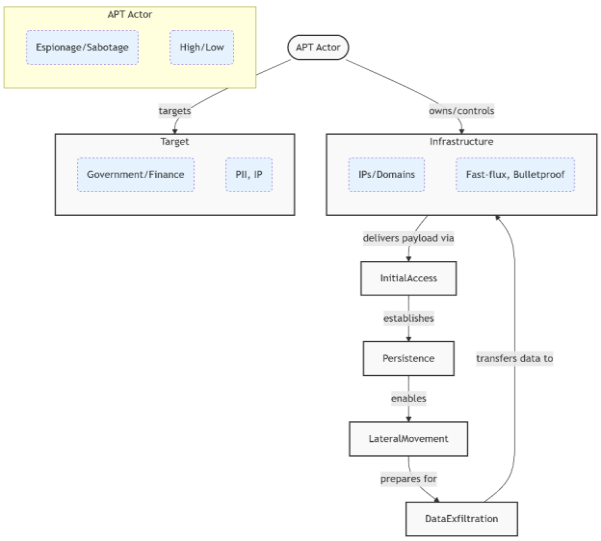

Fig 1. A conceptual skeleton diagram for Advanced Persistent Threats (APT)

- **IoT Security**

Internet of Things (IoT) is a prominent technology that profoundly influences various aspects, such as connectivity, business, healthcare, and economy. Today, IoT has great potential in enhancing life in different aspects, ranging from smarter cities to class environments, with capabilities that include automating activities, enhancing production, and reducing stress levels. Despite being vulnerable because of minimal processing power, outdated firmware, and insecure communication, security is a serious threat to these devices since they contain precious data that could result in network breaches [33].

Cyber-attacks & threats, in contrast, have gravity concerning IoT applications that involve intelligent networks. Many of the typical methods being used in protecting IoT are currently not applicable because of new threats & vulnerabilities. It is one of the most important requirements concerning the security processes that future IoT models should uphold, & it is supported by AI-efficient machine learning & deep learning models [34]

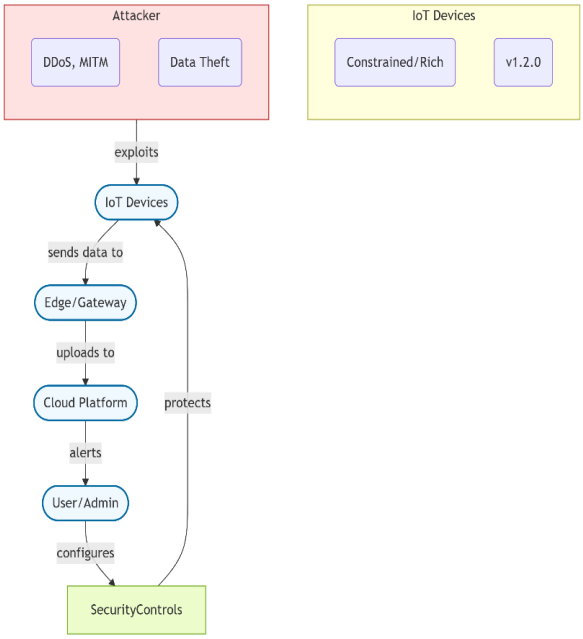

Fig 2. A conceptual skeleton diagram for IoT Security

- **AI-Driven Attacks**

Artificial intelligence (AI)-driven methods and technologies have emerged as powerful tools for enhancing cyber defence capabilities. AI now plays a critical role in both cyberattacks and defensive strategies [35]. Leveraging big data, machine learning, and deep learning, AI enables the identification of patterns, the prediction of threats, and more effective responses to potential attacks. It enhances the accuracy of authentication and access control systems while also improving network monitoring and incident response. However, the same technologies that bolster cyber defence can also be weaponized. Tools such as deepfake technology, AI-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

generated malware, and autonomous botnets can bypass detection systems and intensify cyberattacks [36].

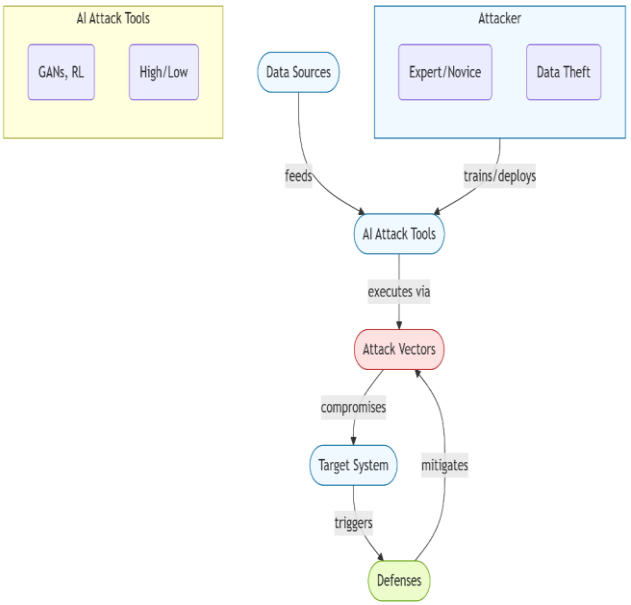

Fig 3. A conceptual skeleton diagram for AI-Driven Attacks

- **Cloud Computing**

Cloud computing has revolutionized the way data storage, processing, and retrieval are done in organizations. Cloud computing presents an unparalleled level of flexibility and scalability. However, this new trend in computing has also posed a variety of security threats and hurdles that must be countered in order for data integrity and availability to be ensured [37]. Cloud computing faces threats such as data breaches, API security threats, and resource sharing threats. Strong security systems must be put in place to counter such threats [38].

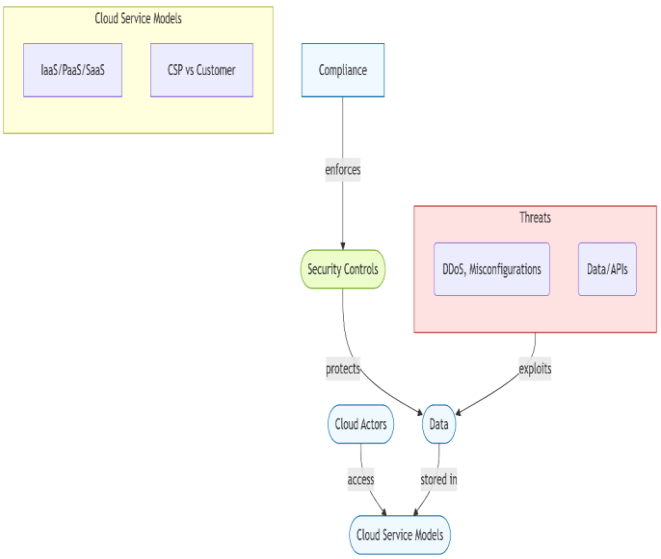

Fig 4. A conceptual skeleton diagram of Cloud Computing Security

VII. Opportunities and Future Research Directions

Cybersecurity is viewed as becoming increasingly complex due to the rapid growth and evolution of devices, computer systems, and computer networks. Furthermore, the evolution of the digital economy and infrastructure has heightened the rise of cyberattacks that have dangerous impacts on individuals and institutions alike. There is, however, evidence that new forms of nation-based and cyber criminals, as well as the sophistication of cyberattacks, are finding innovative ways to breach the savviest of victims [39]. AI and ML present opportunities to automate cyber defense, detect anomalies, and predict attacks in real-time [40]. Quantum-resistant cryptographic methods are essential in preparing for quantum computing threats. Additionally, increasing cybersecurity awareness and education is necessary to address the human factors in security [41].

This change is propelling an ever-increasing number of cyberattacks towards greater scale and effect, thus requiring the adoption of intelligence-led cyber security to offer a constantly evolving shield against ever-evolving cyber-attacks and to manage big data. Blockchain can support secure data sharing in sectors like finance, healthcare, and supply chains. However, limitations such as protocol vulnerabilities and smart contract weaknesses must be addressed [42].

VIII. Conclusion

Cyber Security plays an important role in securing digital resources in different sectors. Given the increasing complexity of cyber threats, there arises an urgent need to leverage emerging technologies such as AI, ML, and Blockchain. Cyber Security has different applications in different fields such as medical centers, banks, Smart Cities, goverment departments, educational institutions, and the defense sectors, to name a few. There also arise several other challenges to Cyber Security from different quarters such as cyber criminals, hackers, governments, and insiders. There also appear different challenges to the field of Cyber Security such as use of defense AI and machine learning technology, complex cyber threats, reinforcement learning-based cyber threats, AI-powered malware, vulnerabilities in Internet of Things technologies, cloud security-related concerns, and use of cryptography in this field. But emerging areas in Cyber Security such as Quantum Computing (Quantum-secure encryption), Biometric Authentication, Advanced Artificial Intelligence (AI), and Machine Learning (ML) may be able to overcome these challenges. In order to keep our digital gadgets, computer networks, and data safe from cyber attacks. There arises an urgent need to invest in Cyber Security.

References

[1] H. Kavak, J. J. Padilla, D. Vernon-Bido, S. Y. Diallo, R. Gore, and S. Shetty, “Simulation for cybersecurity: state of the art and future directions,” Journal of Cybersecurity, vol. 7, no. 1, pp. 1–13, 2021, doi: 10.1093/cybsec/tyab005.

[2] [2] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” Computer Networks, vol. 169, p. 107094, 2020..

[3] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-Turjman, and L. Mostarda, “Cyber security threats detection in internet of things

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

using deep learning approach," IEEE Access, vol. 7, pp. 124379–124389, 2019.

[4] J. Kaur and K. R. Ramkumar, "The recent trends in cyber security: A review," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 8, pp. 5766–5781, 2022.

[5] R. Sharma, "Study of latest emerging trends on cyber security and its challenges to society," International Journal of Scientific & Engineering Research, vol. 3, no. 6, p. 1, 2012.

[6] A. Arabo, "Cybersecurity challenges within the connected home ecosystem futures," Procedia Computer Science, vol. 61, pp. 227–232, 2015, doi: 10.1016/j.procs.2015.09.201.

[7] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 973–993, 2014.

[8] [8] S. O. Hwang, T. Kwon, W. C. Yau, and D. Nyang, "Guest editorial: Special issue on cyber security and AI," ETRI Journal, vol. 41, no. 5, pp. 557–559, 2019.

[9] [9] R. Maeda and M. Mimura, "Automating post-exploitation with deep reinforcement learning," Computers & Security, vol. 100, p. 102108, 2021.

[10] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Computer Networks, vol. 169, p. 107094, 2020.

[11] W. Meng, R. Ma, and H. H. Chen, "Smart grid neighborhood area networks: A survey," IEEE Network, vol. 28, no. 1, pp. 24–32, 2014.

[12] [12] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," International Journal of Critical Infrastructure Protection, vol. 25, pp. 36–49, 2019.

[13] N. Ullah, S. Khan, M. Niazi, M. Esposito, A. A. Khan, and J. A. Nasir, "Solutions to cybersecurity challenges in secure vehicle-to-vehicle communications: A multivocal literature review," Information and Software Technology, p. 107639, 2024.

[14] G. Sabaliauskaite, L. S. Liew, and J. Cui, "Integrating autonomous vehicle safety and security analysis using STPA method and the six-step model," International Journal on Advances in Security, vol. 11, no. 1&2, pp. 160–169, 2018.

[15] M. C. Lucic, O. Bouhamed, H. Ghazzai, A. Khanfor, and Y. Massoud, "Leveraging UAVs to enable dynamic and smart aerial infrastructure for ITS and smart cities: An overview," Drones, vol. 7, no. 2, p. 79, 2023.

[16] G. D. Rodosek and M. Golling, "Cyber security: Challenges and application areas," in Supply Chain Safety Management: Security and Robustness in Logistics, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 179–197.

[17] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," International Journal of Critical Infrastructure Protection, vol. 25, pp. 36–49, 2019.

[18] S. Ksibi, F. Jaidi, and A. Bouhoula, "A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach," Mobile Networks and Applications, vol. 28, no. 1, pp. 107–127, 2023.

[19] A. Arabo, "Cybersecurity challenges within the connected home ecosystem futures," Procedia Computer Science, vol. 61, pp. 227–232, 2015, doi: 10.1016/j.procs.2015.09.201.

[20] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," Arabian Journal for Science and Engineering, vol. 45, no. 4, pp. 3171–3189, 2020.

[21] G. Srivastava, R. H. Jhaveri, S. Bhattacharya, S. Pandya, P. K. R. Maddikunta, G. Yenduri, and T. R. Gadekallu et al., "XAI for cybersecurity: State of the art, challenges, open issues and future directions," arXiv preprint arXiv:2206.03585, 2022.

[22] Y.-L. Cheng, C.-Y. Lee, Y.-L. Huang, C. A. Buckner, R. M. Lafrenie, J. A. Dénommée, J. M. Caswell, D. A. Want, G. G. Gan, Y. C. Leong, P. C. Bee, E. Chin, A. K. H. Teh, S. Picco, L. Villegas, F. Tonelli, M. Merlo, J. Rigau, D. Diaz, and R. H. J. Mathijssen, "Smart health and cybersecurity in the era of artificial intelligence," in Advanced Biometric Technologies, Intech, vol. 11, p. 13, 2016.

[23] H. HaddadPajouh, A. Dehghantanha, R. Khayami, and K. K. R. Choo, "A deep recurrent neural network based approach for internet of things malware threat hunting," Future Generation Computer Systems, vol. 85, pp. 88–96, 2018.

[24] A. Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial internet of things," Digital Communications and Networks, vol. 9, no. 1, pp. 101–110, 2023.

[25] M. Alshehri, "Blockchain-assisted cyber security in medical things using artificial intelligence," Electronic Research Archive, vol. 31, no. 2, 2023.

[26] H. B. Mahajan, A. S. Rashid, A. A. Junnarkar, N. Uke, S. D. Deshpande, P. R. Futane, B. Alhayani et al., "Retracted article: Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," Applied Nanoscience, vol. 13, no. 3, pp. 2329–2342, 2023.

[27] J. Dykstra, L. A. Gordon, M. P. Loeb, and L. Zhou, "Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments," Journal of Cybersecurity, vol. 9, no. 1, p. tyad003, 2023.

[28] [28] E. D. Lonergan and J. Schneider, "The power of beliefs in US cyber strategy: The evolving role of deterrence, norms, and escalation," Journal of Cybersecurity, vol. 9, no. 1, p. tyad006, 2023.

[29] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, K. K. R. Choo et al., "Artificial intelligence in cyber security: Research advances, challenges, and opportunities," Artificial Intelligence Review, vol. 55, no. 2, pp. 1029–1053, 2022.

[30] [30] E. S. Barry, J. Merkebu, and L. Varpio, "State-of-the-art literature review methodology: A six-step approach for knowledge synthesis," Perspectives on Medical Education, vol. 11, no. 5, pp. 281–288, 2022, doi: 10.1007/s40037-022-00725-9.

[31] C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network Security, vol. 2011, no. 8, pp. 16–19, 2011.

[32] R. Kaur and M. Singh, "A survey on zero-day polymorphic worm detection techniques," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1520–1549, 2014.

[33] J. Clark and P. C. Van Oorschot, "SoK: SSL and HTTPS," in Proc. IEEE Symp. Security and Privacy, 2013, pp. 511–525, doi: 10.1109/SP.2013.41.

[34] T. Mazhar, D. B. Talpur, T. A. Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, H. Hamam et al., "Analysis of IoT security challenges and its solutions using artificial intelligence," Brain Sciences, vol. 13, no. 4, p. 683, 2023

[35] Y. Gao, "Cyber attacks and defense: AI-driven approaches and techniques," Academic Journal of Computing & Information Science, vol. 7, no. 7, pp. 41–46, 2024.

[36] A. M. Bulama and M. Faisal, "Human-AI collaboration in education: Enhancing learning environments," in Proc. Int. Conf. Trends and Development in Science and Engineering, Sep. 29, 2025, doi: 10.17577/IJERTCONV13IS06039.

[37] A. K. Y. Yanamala, "Emerging challenges in cloud computing security: A comprehensive review," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 4, pp. 448–479, 2024.

[38] K. Thakur, M. Qiu, K. Gai, and M. L. Ali, "An investigation on cyber security threats and security models," in Proc. IEEE 2nd Int. Conf. Cyber Security and Cloud Computing, Nov. 2015, pp. 307–311.

[39] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Information Fusion, vol. 97, p. 101804, 2023.

[40] R. Maeda and M. Mimura, "Automating post-exploitation with deep reinforcement learning," Computers & Security, vol. 100, p. 102108, 2021.

[41] L. B. Naik, B. AsSadhan, J. M. F. Moura, T. Saadawi, A. El-Desouki, A. S. Elmaghraby, M. M. Losavio, U. S. Rao, R. Swathi, V. Sanjana, L. Arpitha, K. Chandrasekhar, Chinmayi, P. K. Naik, M. Alshehri, N. Ben-asher, C. Gonzalez, M. Alshehri, C. Hemminghaus, and S. Ddos, "Special issue on cyber security and AI," *Journal of Advanced Research*, vol. 41, no. 5, pp. 557–559, 2019, doi: 10.4218/etr2.12236.

[42] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in Banking Beyond Banks and Money, Springer International Publishing, 2016, pp. 239–278

.