International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Innovations and Future Directions in Securing Digital Environments

Disha Sharma , Muskan Sikka , Simar Khurana , Vidushi Gupta

Department of Computer Science
Chandigarh University
Mohali, India
22bcs16291@cuchd.in

ARTICLE INFO

ABSTRACT

Introduction: Unprecedented opportunities and difficulties have arisen as a result of the quick expansion of digital environments, especially in the fields of cybersecurity and decision support systems. More clever and flexible strategies are required because traditional security measures frequently can't keep up with new threats. In intelligent decision support systems (IDSS), cognitive computing—which combines artificial intelligence (AI), machine learning (ML), natural language processing (NLP), and sophisticated data analytics—has become a disruptive force. These systems can process enormous volumes of structured and unstructured data, identify patterns, and offer proactive insights for improved decision-making in security-critical circumstances by simulating human cognitive processes. The reconfiguration of IDSS by cognitive computing to improve the security and resilience of digital ecosystems is examined in this chapter. In order to reduce cyber risks, we go over the use of AI-driven threat intelligence, real-time anomaly detection, and predictive risk assessment. Furthermore, we investigate how adaptive and self-learning algorithms in cognitive computing improve fraud detection, network security, and access control. By integrating explainable AI (XAI), security decision-making becomes transparent, resolving issues with trust and accountability in automated security systems. The chapter also explores new developments that will influence cognitive-driven IDSS in the future, such as federated learning for decentralised threat intelligence sharing, autonomous security agents, and the possible effects of quantum computing on cryptographic security. We also draw attention to the difficulties in putting cognitive security solutions into practice, including computational complexity, hostile AI model assaults, and moral dilemmas in automated decision-making.

Objectives: This study paper's main goal is to examine current developments, new trends, and potential paths for digital environment security. Modern cyber risks are addressed by this study's analysis of cutting-edge technology, developing cybersecurity frameworks, and clever defence measures. Additionally, the study looks into how security methods are changing as a result of developments in blockchain, zero-trust architecture, quantum cryptography, artificial intelligence, and cybersecurity automation. In order to improve the resilience, privacy, and integrity of digital systems in a world that is becoming more linked, the study also aims to highlight current issues and suggest possible solutions.

Methods: The qualitative research methodology used in this study includes a review of recent cybersecurity innovations-related literature, research articles, and case studies. Information was gathered from reliable sources, including industry publications, scholarly journals, and professional comments. In order to secure digital environments, the study compares traditional and modern security methods, analyses emerging technologies, and looks for future trends and solutions.

Results: According to the survey, cutting-edge technologies like blockchain, artificial intelligence (AI), quantum cryptography, and zero-trust architecture are all significantly improving cybersecurity. Blockchain guarantees safe data exchanges, while AI aids in danger detection and automatic responses. By doing away with implicit trust, zero-trust models are enhancing network security. Additionally, the study found that businesses are embracing cloud security and cybersecurity automation more and more. But there are still issues like changing cyberthreats, privacy issues, and the demand for qualified cybersecurity specialists. The results show a significant trend towards future security systems that are proactive, intelligent, and adaptable.

Conclusions: In conclusion, because of the quick development of technology and the constantly changing nature of cyberthreats, protecting digital environments is getting harder and harder. According to this study, advancements in artificial intelligence, blockchain, zero-trust architecture, and quantum cryptography are

revolutionising cybersecurity procedures. Better threat management, automation, and enhanced protection are provided by these technologies. However, creating future digital environments that are more secure will require ongoing research, the development of a skilled workforce, and the ability to adjust to new challenges. Organisations must embrace contemporary security solutions and keep abreast of emerging cybersecurity trends, according to the report.

Keywords: Cybersecurity, Digital Environments, Artificial Intelligence (AI), Blockchain, Quantum Cryptography, Zero-Trust Architecture, Cognitive Computing, Intelligent Decision Support Systems (IDSS), Cybersecurity Automation, Threat Intelligence, Anomaly Detection, Predictive Risk Assessment, Explainable AI (XAI), Cloud Security, Emerging Technologies.

INTRODUCTION

Digital transformation and the quick development of technology have fundamentally altered how people, companies, and governments function. Digital environments have many advantages, but they are also now the main target of unwanted activity and cybercriminals. The rising dependency on digital systems, cloud computing, the Internet of Things (IoT), and mobile technologies has enlarged the threat landscape, demanding increasingly complex and inventive cybersecurity measures.

Modern threats are more complicated and dynamic than ever before, and traditional security measures like firewalls, antivirus software, and password protection are no longer adequate. Cyberattacks that take advantage of the flaws in antiquated security systems, like ransomware, phishing, data breaches, and advanced persistent threats (APT), are always evolving. Therefore, in order to better secure digital environments, there is an increasing demand for creative approaches and cutting-edge technologies.

In the field of cybersecurity, artificial intelligence (AI) and machine learning (ML) have become extremely effective technologies. Real-time monitoring, predictive analytics, automated threat identification, and quick incident response are all made possible by these technologies. Cybersecurity solutions powered by AI are quicker than human operators in spotting trends, spotting abnormalities, and eliminating threats. Natural Language Processing (NLP) also aids in threat intelligence enhancement, unstructured data analysis, and cybersecurity decision-making.

Digital security is further aided by the groundbreaking innovation of blockchain technology. Its tamper-resistant and decentralised architecture guarantees safe transaction processing and data storage. Supply chain management, healthcare, and finance are just a few of the industries where blockchain improves data accuracy, trust, and transparency. In addition, quantum cryptography is becoming a viable option for creating impenetrable encryption techniques, which will be essential for safeguarding private information from potential dangers posed by quantum computing.

Another popular strategy for protecting digital environments is zero-trust architecture. Under the tenet of "never trust, always verify," it makes sure that all users and devices, whether they are within or outside the company's network, have rigorous identity verification and access control. Through constant trust validation, this method lowers the likelihood of both internal and external breaches.

The cybersecurity industry still faces challenges despite advancements in security technologies, including a lack of qualified personnel, growing privacy concerns, sophisticated cybercriminal tactics, and ethical concerns with AIbased security systems. Additionally, enterprises must guarantee the security of cloud services, remote work environments, and internet-connected smart devices.

The goal of this study paper is to improve digital environments by examining the most recent advancements and potential paths in cybersecurity. It investigates how to improve security measures using AI, blockchain, zero-trust architecture, and quantum cryptography. The study also emphasises the necessity of proactive security measures, new trends, and current challenges. In order to create a safer and more secure digital future, it will be essential to adopt modern technologies, invest in cybersecurity research, and develop a skilled workforce.

OBJECTIVES

This study paper's main goal is to investigate and evaluate new developments and technologies in the field of digital environment security. Securing data, networks, and systems has become a top responsibility for both individuals and organisations as the digital landscape grows. The goal of this study is to offer insightful information on the technologies influencing cybersecurity's development and its potential future paths.

The study's particular goals are:

1. To research current cybersecurity issues in contemporary digital settings.
2. To investigate cutting-edge techniques and technologies that are revolutionising cybersecurity methods, such as blockchain, quantum cryptography, machine learning, and artificial intelligence (AI).
3. To investigate how Zero-Trust Architecture might improve digital security and its significance.
4. To examine upcoming developments and paths in cybersecurity to guard against new dangers and weaknesses.
5. To draw attention to the advantages, restrictions, and moral dilemmas associated with implementing cuttingedge security systems.
6. To suggest strategic methods for governments and organisations to fortify cybersecurity infrastructure and get ready for upcoming obstacles.

METHODS

This study examines the advancements and potential paths in digital environment security using a qualitative research technique. The study's foundation is a thorough analysis of secondary data gathered from numerous trustworthy sources, such as industry reports, white papers, research articles, journals, conference papers, and case studies about cybersecurity and new technologies. Online databases like IEEE Xplore, ScienceDirect, Springer, Google Scholar, and cybersecurity websites provided the study's data. The study examined new developments in artificial intelligence (AI), blockchain, machine learning (ML), zero-trust architecture, and quantum cryptography, among other technologies. The function, use, benefits, and drawbacks of these technologies in improving cybersecurity were investigated.

To determine the efficacy of new solutions, a comparative study between contemporary security innovations and conventional security methods was also conducted. In order for organisations to guarantee safe digital environments, the study concentrated on identifying current cybersecurity difficulties, prospective threats, and future trends. In addition, case studies, industry best practices, and expert opinions were examined to bolster the study and offer actual instances of creative cybersecurity solutions being successfully implemented in the real world. This method assisted in discovering gaps, potential avenues for further study, and tactical suggestions for enhancing cybersecurity infrastructure.

CURRENT INNOVATIONS IN CYBER SECURITY

New cybersecurity methodologies are evolving to incorporate innovative technology that offers improved automation, agility, and credibility in the wake of increased frequency and sophistication in cyberattacks. These trends not only make security systems quicker to detect and respond, but they also reframe the foundational concepts of safeguarding data and systems within an increasingly networked digital world.

Artificial Intelligence in Threat Detection

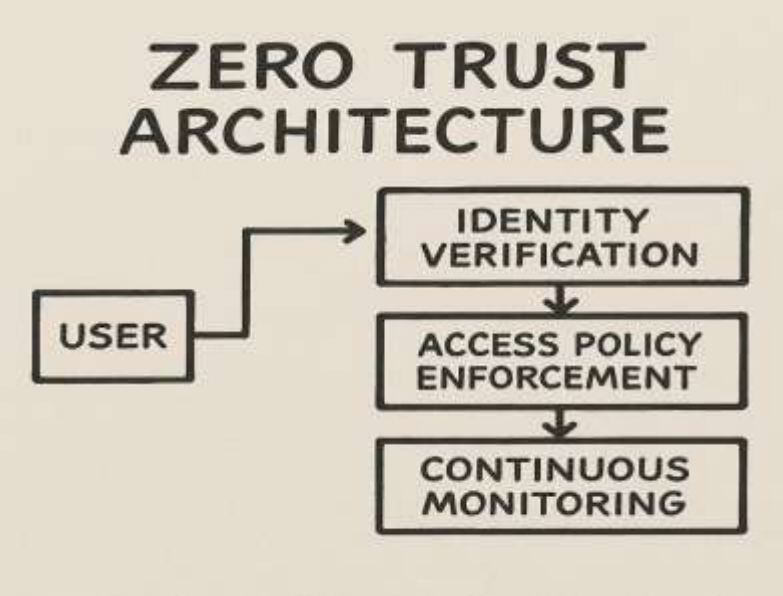
In the field of cybersecurity, artificial intelligence (AI) and machine learning (ML) are now crucial elements, especially when it comes to threat detection and response. Large amounts of data from network endpoints can be processed by AI-driven security solutions, which can also recognize intricate threat patterns and differentiate between malicious and legitimate activity. AI analyzes user activity logs, endpoint telemetry, and traffic patterns in real time using deep learning algorithms and neural networks. This makes it possible to identify irregularities early on that might indicate cyber intrusions like privilege escalation, lateral movement, or data exfiltration. ML models can continuously evolve by learning from historical incident data, thereby improving their ability to recognize zero-day threats and reducing the likelihood of false positives. AI also makes it easier to use Security Orchestration, Automation, and Response (SOAR) platforms, which allow automated containment actions like removing access privileges, isolating compromised systems, or starting backup procedures without human involvement. In addition to reducing the workload for security operations centers (SOCs), this speeds up incident response times, making AI a vital component of proactive cyber defense.

Blockchain for Data Integrity

Blockchain technology marks a paradigm shift in digital assets and data security. Blockchain is essentially a distributed ledger that maintains an immutable and open record of all transactions. Integrity of data is ensured because each block contains a cryptographic hash of the previous one, making it instantly evident if there has been any alteration and the next chain invalid. The fact that blockchain technology can resist tampering and unauthorized alteration is one of its primary strengths in cybersecurity. This is particularly beneficial in safeguarding private data in digital identities, financial systems, health records, and supply chains. Decentralized consensus systems also eliminate the requirement for centralized organizations, which reduces the risk of single points of failure. By executing pre-programmed actions automatically in response to preprogrammed conditions, smart contracts on blockchain platforms offer an added layer of security without

the involvement of middlemen. Already being applied in secure voting systems, access control systems, and identity verification systems, such contracts enhance trust and transparency in online interactions.

Zero-Trust Architecture



A basic shift from the traditional "trust but verify" paradigm to a more rigorous "never trust, always verify" security architecture is embodied in Zero-Trust Architecture (ZTA). Because ZTA assumes that the threats may also be from within the company network, no user or device, even one that is within the perimeter, is inherently trusted.

With methods such as device posture assessment, behavioral analysis, and multi-factor authentication (MFA), this model imposes continuous authentication and authorization. Context such as user identity, location, health of the device, and sensitivity of the requested resource is utilized to dynamically evaluate every attempt at access. Least Privilege Access (LPA) and Role-Based Access Control (RBAC) are two foundational components of ZTA. By ensuring users and apps are given no more than the absolute minimum required access to fulfill their functions, these practices minimize the attack surface and limit lateral mobility in case of a compromise. Used with granular policy enforcement and micro-segmentation, Zero Trust significantly enhances organizational resilience to both insider and outsider threats.

Quantum Cryptography

A new discipline known as quantum cryptography is transforming secure communication by implementing the concepts of quantum mechanics. By leveraging the physical properties of quantum particles, quantum cryptography offers provably secure channels for information transfer, unlike classical encryption, which is based on complex mathematical algorithms.Quantum Key Distribution (QKD), under which two parties are able to establish a shared secret encryption key that cannot be copied or intercepted covertly, is the most widely researched application. By leveraging quantum properties such as superposition and entanglement, QKD protocols such as BB84 and E91 ensure that any eavesdropping effort causes detectable abnormalities in the quantum state of particles being transmitted. Conventional public-key cryptosystems such as RSA and ECC are becoming increasingly vulnerable to decryption with the growth of quantum computing. Quantum cryptography, a post-quantum secure alternative that is immune to attacks by even the strongest quantum computers, is used to combat this. In sectors where confidentiality and integrity of communications are of high importance, such as defense, finance, and critical infrastructure, its use is currently being researched.

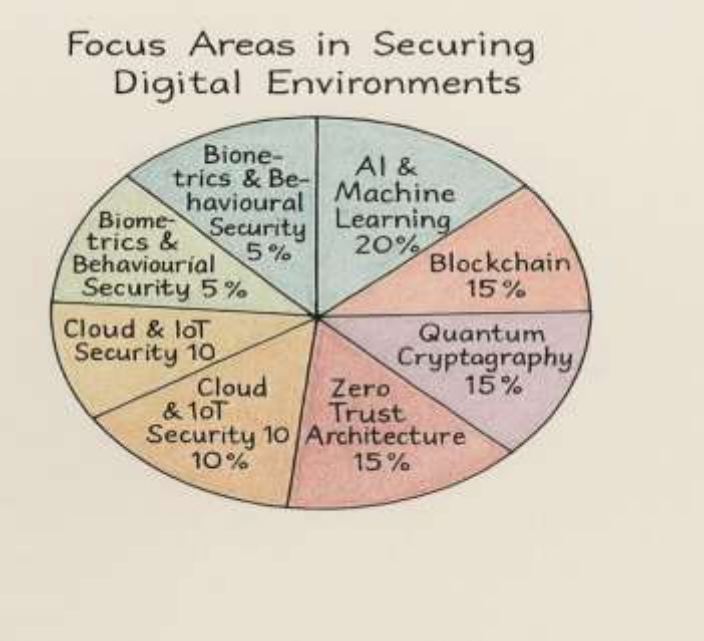


Figure 1. In the chart, authors abstractionally differentiate between areas of greater attention or priority in cybersecurity strategies today.

FUTURE DIRECTIONS IN DIGITAL SECURITY

Rapid technological breakthroughs and the growing complexity of cyber threats are predicted to influence the direction of digital security in the future. Securing data and systems has become a primary responsibility as digital environments continue to increase due to the rise of cloud computing, the Internet of Things (IoT), and artificial intelligence (AI). Some important avenues for future development in digital security include the following:

1. **Combining Machine Learning and Artificial Intelligence**
   It is anticipated that machine learning (ML) and artificial intelligence (AI) would form the foundation of cybersecurity frameworks in the future. These technologies give systems the ability to recognise possible risks, detect anomalies automatically, and react proactively to cyber disasters. AI-driven security solutions learn from data trends and continuously enhance their capacity to identify complex assaults like ransomware, phishing, and advanced persistent threats (APTs), in contrast to traditional systems that depend on pre-established rules. Additionally, AI will be crucial for fraud detection, behavioural analysis, and real-time network traffic monitoring.

2. **Decentralised Security with Blockchain**
   By offering secure identity management, tamper-proof transaction records, and decentralised data storage, blockchain technology will completely transform digital security. Blockchain will be used by future digital systems to secure peer-to-peer communication, validate digital identities, and safeguard sensitive data. By lowering fraud and guaranteeing data integrity, this technology will be especially helpful to the financial industry, supply chain management, healthcare, and digital voting systems.

3. **Quantum Cryptography's Development**
   Traditional encryption methods face a serious threat from the emergence of quantum computing. Existing cryptography techniques may be broken by increasingly potent quantum computers. As a result, quantum cryptography is becoming a promising avenue for cybersecurity in the future. Unbreakable encryption will be ensured by technologies such as Quantum Key Distribution (QKD), adding another line of defence against cyberattacks made possible by quantum technology.

4. **Architecture of Zero Trust**
   Based on the tenet of "never trust, always verify," the Zero Trust Security Model will be a norm in cybersecurity tactics going forward. Regardless of whether they are inside or outside the network perimeter, this architecture makes sure that every user, device, and application trying to access organisational resources is constantly validated. Zero Trust will be essential for protecting cloud computing, hybrid networks, and remote work settings.

5. **Automation of Cybersecurity and Threat Intelligence**
   Cybersecurity process automation is becoming crucial to managing the increasing complexity and number of cyberthreats. Real-time incident response, effective vulnerability management, and quicker threat detection are all benefits of automated security solutions. Furthermore, AI-powered threat intelligence platforms will gather, examine, and disseminate data on new dangers worldwide, assisting businesses in becoming ready beforehand.

6. **Technologies that Improve Privacy**
   Future digital security will prioritise the development of privacy-enhancing technologies (PETs) due to growing worries about data privacy. Techniques like differential privacy, safe multi-party computation, and homomorphic encryption will make it possible to process and analyse sensitive data without disclosing it to unauthorised parties.

7. **Improving Cloud and IoT Security**
   New attack surfaces are brought up by the quick growth of cloud computing and IoT devices. Securing IoT ecosystems, guaranteeing device authentication, safeguarding cloud data, and putting strong access restrictions in place will be the main goals of future developments in digital security. Privacy protection in smart cities and homes, edge computing security, and smart device security will all become more crucial.

8. **Awareness and Development of Cybersecurity Skills**
   Digital security still relies heavily on human skills. Future plans will emphasise talent development, cybersecurity education, and increasing public awareness of changing risks. Businesses will spend money on educating cybersecurity experts and cultivating specialised knowledge in quantum cryptography, cloud security, and artificial intelligence.

9. **Sharing of Cyber Threat Intelligence**
   Cooperation between governments, cybersecurity companies, and organisations will improve the ability to detect and respond to threats. In order to facilitate quicker threat identification and coordinated defence strategies worldwide, future systems will concentrate on developing safe channels for exchanging real-time cyber threat intelligence.

10. **Awareness of Cybersecurity and the Development of Skills**
    One important component of cybersecurity is still the human element. To establish a workforce that is aware of cybersecurity, future directions will prioritise frequent cybersecurity training, awareness campaigns, and skill development. To effectively combat evolving cyber threats, it will be crucial to develop cybersecurity skills with knowledge of emerging technology.

11. **Behavioural Security and Biometric Authentication**
    Digital security will depend more and more on biometric technology like voice recognition, facial recognition, fingerprint scanning, and retinal scans. Another level of user authentication will be provided by behavioural biometrics, which monitor mouse movements, typing patterns, and

navigational behaviours. This will offer continuous and multi-factor authentication techniques that are difficult for hackers to imitate.

12. **Safe Access Using Edge Computing and 5G**
New security issues will surface as edge computing and 5G networks grow. Future security strategies will concentrate on safeguarding edge devices, securing decentralised networks, and guaranteeing encrypted communication over quick and extensive networks. Enhanced monitoring of 5G-enabled devices, localised data processing, and adaptive encryption will all be part of the security plans.

13. **Cybersecurity Laws and the Development of Compliance**
Stricter cybersecurity laws will be developed by governments and international organisations to safeguard private information and vital infrastructure. Global cybersecurity standards, obligatory data breach reports, harsher sanctions for non-compliance, and legislation addressing AI, IoT, and new tech security issues are some examples of future trends.

14. **Protecting Critical Infrastructure and Smart Cities**
Integrating cybersecurity into municipal infrastructure will become crucial as smart cities grow. Future plans will concentrate on defending against cyberthreats like ransomware, sabotage, and data breaches in order to safeguard electricity grids, public transportation, surveillance systems, traffic control systems, and healthcare networks.

15. **Extension of Ethical Hacking and Bug Bounty Programs**
Organisations will increasingly invest in bug bounty and ethical hacking initiatives to keep ahead of cybercriminals. As a normal security practice, encouraging security researchers and ethical hackers to identify flaws before malevolent actors do can enhance proactive defence tactics.

CONCLUSION

In conclusion, in today's technologically advanced world, protecting digital environments has emerged as one of the most important issues. The risk of cyber threats has greatly increased because to the quick rise in digital transformation, online transactions, smart gadgets, and data generation. Digital security innovations are always changing to preserve networks, protect sensitive data, and guarantee the privacy and confidence of people everywhere.

The design and implementation of cybersecurity solutions are changing as a result of emerging technologies like blockchain, quantum cryptography, machine learning, and artificial intelligence. These technologies improve the overall security environment by offering stronger encryption methods, automatic responses, real-time monitoring, and enhanced threat detection. Furthermore, new guidelines for safeguarding digital assets are being established by strategies like Zero Trust Architecture, Privacy Enhancing Technologies, and Cloud Security developments.

In addition to technology innovation, future paths in digital security will emphasise legislative development, human awareness, and international cooperation. A more secure digital future is being paved by the growing significance of ethical hacking, cybersecurity laws, threat intelligence exchange, and the training of cybersecurity experts. The need to create strong security plans that tackle new risks is increasing as smart cities, IoT devices, 5G networks, and edge computing continue to increase.

In the end, a multifaceted strategy integrating state-of-the-art technology, proactive security procedures, and ongoing learning will be needed for cybersecurity in the future. Building resilient digital environments

requires collaboration between individuals, governments, and organisations. To make the digital world safer and more reliable, investments in cybersecurity research, innovation, and education will be crucial.

Therefore, in order to properly protect the digital ecosystem from ever-evolving dangers, the future of digital security rests on embracing innovation, remaining watchful, and cultivating a culture of cybersecurity awareness.

REFERENCES

1. Ahmad, A., Maynard, S. B., & Park, S. (2014). *Information security strategies: Towards an organizational multi-strategy perspective*. Journal of Intelligent Manufacturing, 25(2), 357-370.

2. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). *Internet of Things security and forensics: Challenges and opportunities*. Future Generation Computer Systems, 78, 544-546.

3. Kshetri, N. (2017). *1 Blockchain's roles in strengthening cybersecurity and protecting privacy*. Telecommunications Policy, 41(10), 1027-1038.

4. Shackleford, D. (2019). *Security automation: Integrating AI and machine learning into the cybersecurity ecosystem*. SANS Institute InfoSec Reading Room.

5. Mavroeidis, V., & Bromander, S. (2017). *Cyber security and threat intelligence: Challenges and opportunities*. 2017 European Intelligence and Security Informatics Conference (EISIC), IEEE.

6. Chatterjee, S., Rana, N. P., Tamilmani, K., & Sharma, A. (2020). *The role of artificial intelligence in cybersecurity: A structured literature review and future research agenda*. The Bottom Line, 33(4), 297-320.

7. Singh, S., Jeong, Y. S., & Park, J. H. (2017). *A survey on cloud computing security: Issues, threats, and solutions*. Journal of Network and Computer Applications, 75, 200-222.

8. Das, A., Bapat, S., & Aggarwal, R. (2021). *Zero Trust Security Model: A systematic literature review*. Procedia Computer Science, 192, 2430-2439.

9. Tripathi, S., & Joshi, S. C. (2020). *Future Trends in Cybersecurity*. International Journal of Advanced Research in Computer Science, 11(3), 17-22.

10. Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2021). *Handbook of Computer Networks and Cyber Security*. Springer.

11. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023). Cyber security: State of the art, challenges and future directions. *Computer Science Advances*, 100031.

12. Schmitt, M. (2023). Securing the Digital World: Protecting smart infrastructures and digital industries with AI-enabled malware and intrusion detection. *arXiv preprint arXiv:2401.01342*.

13. Schmitt, M., & Koutroumpis, P. (2025). Cyber Shadows: Neutralizing Security Threats with AI and Targeted Policy Measures. *arXiv preprint arXiv:2501.09025*.

14. Shankar, G., Uddin, M. R., Mukta, S., Kumar, P., Islam, S., & Islam, A. K. M. N. (2024). Blockchain Based Information Security and Privacy Protection: Challenges and Future Directions using Computational Literature Review. *arXiv preprint arXiv:2409.14472*.

15. Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero Trust: Applications, Challenges, and Opportunities. *arXiv preprint arXiv:2309.03582*.

16. Hassan, W. U., Bates, A., & Bhattacharya, A. (2019). Detecting Credential Leakage from Smart Devices using Machine Learning. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS 2019)*, 826-841.

17. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78, 544-546.

18. Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: a security point of view. *Internet Research*, 26(2), 337-359.

19. Suciu, G., Vulpe, A., Suciu, V., Fratu, O., Halunga, S., & Dragan, F. (2013). Smart cities built on resilient cloud computing and secure Internet of Things. *Proceedings of the 19th International Conference on Control Systems and Computer Science*, 513-518.

20. Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain Technology: A Survey on Applications and Security Privacy Challenges. *Internet of Things*, 8, 100107.

21. Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP)*.

Wazid, M., Das, A. K., Kumar, N., Conti, M., & Vasilakos, A. V. (2019). Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Things environment. *Future Generation Computer Systems*, 91, 715-731.

22. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Blockchain-based IoT security and forensic framework. *IEEE Internet of Things Journal*, 6(5), 8005-8018.

23. Zhang, Y., Deng, R. H., & Liu, D. (2019). Blockchain-based secure data sharing for healthcare. *IEEE Transactions on Industrial Informatics*, 15(6), 3652-3661.

24. Gai, K., Wu, Y., Zhu, L., Xu, L., & Zhu, Y. (2019). Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. *IEEE Internet of Things Journal*, 6(5), 79928004.

25. Beye, M., & Jehl, P. (2020). Privacy threats in smart cities: The role of data brokers. *Computer Law & Security Review*, 36, 105392.

26. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, 4(6), 1802-1831.

27. Jain, A., Kumar, P., Liao, H. C., & Obaidat, M. S. (2017). Security solutions for smart cyber physical systems: Challenges and research opportunities. *IEEE Communications Magazine*, 55(9), 62-69.

28. Salah, K., Habib Ur Rehman, M., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access*, 7, 10127-10149.

29. Zeng, X., Zhang, W., Xue, R., Cai, Z., & Li, H. (2020). Blockchain-based data auditing for Internet of Things. *IEEE Network*, 34(6), 88-93.