Innovative Computing Review (ICR)
Volume 5 Issue 1, Spring 2024
ISSN$_{(P)}$: 2791-0024, ISSN$_{(E)}$: 2791-0032
Homepage: https://journals.umt.edu.pk/index.php/ICR

Check for updates

Article QR

Title:	**Cybersecurity State of the Art: A Systematic Review of Current Trends and Future Developments**
Author (s):	Musharaf Hassan[1], Muhammad Shahid Azeem[2], Faisal Hameed[3], Mubeen Ashraf [4], and Atif Masih[5]
Affiliation (s):	[1]Department of Computer Science & Software Engineering University of Agriculture Faisalabad, Pakistan [2]Department of Computer Science Govt. Islamia Graduate College Kasur, Pakistan [3]Department of Computer Science Government College University Lahore, Pakistan [4]School of Cyber Security Xidian University, China [5]Department of Computer Science University of Central Punjab, Lahore, Pakistan
DOI:	https://doi.org/10.32350/icr.52.03
History:	Received: June 20, 2025, Revised: July 24, 2025, Accepted: August 18, 2025, Published: December 29, 2025
Citation:	M. Hassan, M. S. Azeem, F. Hameed, M. Ashraf, A. Masih, "Cybersecurity State of the Art: A Systematic Review of Current Trends and Future Developments," *Innov. Comput. Rev.*, vol. 5, no. 2, pp. 57-77, December. 2025, doi: https://doi.org/10.32350/icr.52.03.
Copyright:	© The Authors
Licensing:	This article is open access and is distributed under the terms of Creative Commons Attribution 4.0 International License
Conflict of Interest:	Author(s) declared no conflict of interest

A publication of
School of Systems and Technology
University of Management and Technology, Lahore, Pakistan

Cybersecurity State of the Art: A Systematic Review of Current Trends and Future Developments

Musharaf Hassan[1], Muhammad Shahid Azeem[2*], Faisal Hameed[3], Mubeen Ashraf[4], and Atif Masih[5]

[1]Department of Computer Science & Software Engineering University of Agriculture Faisalabad, Pakistan
[2]Department of Computer Science Govt. Islamia Graduate College Kasur, Pakistan
[3]Department of Computer Science Government College University Lahore, Pakistan
[4]School of Cyber Security Xidian University, China
[5]Department of Computer Science University of Central Punjab, Lahore, Pakistan

ABSTRACT In recent years, the need for organizations, researchers, and academics to focus on cyber security has increased significantly in order to effectively ensure the safety of information systems. As digitization expands, cyber threats continue to evolve, posing a constant risk to every person and business. Gain a bird's-eye perspective of cyber security today by reading this essay, which covers worldwide trends, present situations, and problems and methods. This study provides a comprehensive overview of the current cybersecurity landscape by examining global trends, existing challenges, and prevailing practices. We also discuss the future state of the cyber defenses with a focus on the possible strategies to fight the growing cyber threat environment, the new tendencies, and the development of technologies like ML and AI that can be used to respond to cyberattacks with automaticity. The essay also underscores the need to adopt and work with stakeholders in the cyber ecosystem continuously.

INDEX TERMS cyber-security, trends, challenges, state-of-the-art, future directions

I. INTRODUCTION

The exponential expansion of the internet over the last few decades has altered the fabric of our society, economy, and most essential public services. Many people now call this new era of technology the "cyber civilization" because of how it has altered our means of communication, commerce, and information dissemination. Due to the magnitude and velocity of this development, the Internet is now fundamental to contemporary life and an essential means of disseminating knowledge [1]. Many industries rely on technology for mission-critical operations, including finance, healthcare, education, government, smart cities, and grid systems. These duties are now easier to do than ever before, thanks to advancements in technology for information and communication. However, there are significant security concerns that must be addressed by individuals, governments, and organizations alike [2]. Individuals, communities, and businesses may be in danger from security breaches by rapidly developing technologies. Stakeholders often use cybersecurity dealings, legislative frameworks, and awareness as well as education efforts to encourage ethical activities and dishearten evil set on to lessen the impact of these security threats [3]. Defending against malicious online behavior is the goal of cybersecurity measures taken by individuals, groups,

*Corresponding Author: muhammadshahidazeem@gmail.com

businesses, and government agencies. Protecting the privacy, authenticity, and accessibility (CIA) of data stored on computers that belong to one company or that are linked to another's network is what cybersecurity is all about [4].

Data protection, privacy concerns, availability and reliability, and cyber safety are some of the important ideas to keep in mind when making sure that everything is secure, especially since 61% of all social and business interactions take place online [5]. Consequently, cybersecurity has surpassed all other measures as the primary tool for warding off cybercrime and cyberattacks, ensuring that all social and industrial contacts remain secure [6].

One of the most pressing global security concerns is the need to make the Internet a safer place and to safeguard Internet users [7]. The growing importance of a safe online environment has far-reaching consequences for people, companies, and countries regarding cyber security, especially as the digital world becomes more pervasive and integrated into our daily lives. Building safeguards for the Internet is now standard practice for any new government programs, services, and technology. There has to be a more thorough and secure strategy to combat cybercrime. As a result, technological safeguards are insufficient to prevent cybercrime [8]. Successful investigation and prosecution of cybercrime by law enforcement authorities is of the utmost importance [9]. To curb data breaches, some nations have enacted stringent cybersecurity regulations, including those in Pakistan.

Almost every aspect of our lives depends on technology to maintain economic and social security, making cybersecurity an essential component of today's digital society. Industries that rely on critical infrastructure, such as healthcare and energy, are particularly vulnerable to cyberattacks, which may have devastating consequences, including financial losses, damage to reputations, and even deaths [10]. Every sector of society relies on cyber security measures to keep sensitive information private and safe, including small businesses, government organizations, healthcare providers, schools, energy providers, and transportation networks [11], [12].

Machine learning (ML) and artificial intelligence (AI) have many potential applications in the areas of threat detection, network vulnerability discovery, and IT burden reduction [13], [14]. Another benefit of machine learning and AI is their capacity to automate certain cybersecurity processes, including vulnerability assessments, malware analysis, and intrusion detection [15]. This allows security personnel more time to concentrate on long-term planning. In response to increasingly complex cyber threats, many organizations rely on AI and Machine Learning (ML) as powerful cybersecurity weapons. There has been a dramatic shift in cyber defenses due to the advent of ML and AI, which we study in detail [16], [17]. Despite this, anti-ML assaults do exist. This study delves into the topic of cyber security and where researchers should take it going in the future, touching on topics like AI, ML, and extra cutting-edge methods for fighting cyber threats.

II. APPLICATION AREA OF CYBER SECURITY

Cyber defense, detection of intrusions, and encryption systems contribute to a more secure online environment by protecting sensitive information and preventing unauthorized access [18], [19].

Cybersecurity is primarily relevant to the following domains due to the internet's centrality to business and social interactions.

A. CYBER SECURITY IN SMART GRID

By integrating cutting-edge communication and processing technologies, the smart grid is paving the way for more efficient and dependable power systems, which will likely include distributed computing, demand planning, and energy from renewable sources. Customers benefit from the smart grid's reduced response time delay, improved service quality, and speedier service implementation in the fight against the energy crisis [20], [21]. Cybersecurity poses a significant challenge to smart grids because of the extensive electronic equipment and communication networks that comprise the power infrastructure. Smart grids optimize electricity generation, distribution, and consumption via digital technologies [22], [23]. Among the numerous benefits of smart grids are efficiency and reliability.

Information interchange in energy infrastructure relies on mission-critical networks, and smart grid technology communication networks are no exception. Confidentiality, trustworthiness, and integrity are the primary cybersecurity objectives for the smart grid [24]. Encryption, network monitoring for suspicious activities, secure communication protocols, and authentication may contribute to a more secure cyber environment [25]. Cybersecurity for smart grids guarantees dependable and quick data access and utilization [26]. Cybersecurity measures may lessen the impact of advanced persistent threats (APTs), denial of service (DoS), and unauthorized data access while keeping the smart grid system trustworthy, private, and intact. Enhancing the online security of the Smart Grid is a top priority in the field of cybersecurity, which highlights the potential negative consequences of cyber-attacks on the system, such as power outages, financial losses, and accidents [27]. Stakeholder education on cyber security awareness and best practices, regular security audits and assessments, improved threat information and sharing, and state-of-the-art authentication and encryption methods are all recommended [28], [29].

B. PROTECTION STRATEGIES FOR VEHICULAR COMMUNICATIONS

Secure vehicle communication systems and infrastructure are essential for improving traffic flow, passenger comfort, and safety on the road. Securing the vehicle's internal components, including sensors, actuators, and electronic control units (ECUs), as well as the communication channels connecting cars to infrastructures like road units or traffic control centers, is of the utmost importance [30], [31]. An additional essential component of cybersecurity in this setting is the protection of user privacy and individual data. Regular testing and maintenance of all components is essential to guarantee the dependability and credibility of these systems [32], [30]. Additionally, failover and redundancy methods must be put in place. Ensuring the security, privacy, and reliability of the system is the foundation of cybersecurity in-vehicle communications, which in turn inspires trust among users and stakeholders [32], [33]. It is essential to include all parties involved in the ecosystem, including users, regulators, infrastructure providers, service providers, and manufacturers, in a comprehensive and proactive strategy.

C. CYBERSECURITY ACROSS SMART CITIES

An urban area that enhances the quality of life for its residents via the employment of modern technology and communication infrastructure is known as a smart city. To protect residents' personal information and vital infrastructure from cyber threats, smart cities must handle the increasing dependence on interconnected systems and gadgets [34]. Cybersecurity applications in smart cities safeguard essential services like water, electricity, transportation, and communications; safeguard linked IoT devices like cameras and sensors; guarantee citizens' privacy, including any personally identifiable information gathered; and safeguard disaster retrieval systems [35], [36].

D. CYBER PROTECTIONS FOR SMART EHEALTH

The collection of healthcare-related information from many sources, such as medical equipment and mobile apps, is largely dependent on devices with internet connections in healthcare services based on the Internet of Things (IoT), such as smart health and monitoring of patients remotely [37], [38]. Improved patient care is possible via the real-time tracking of vital signs by connecting medical devices to the Internet of Things [39]. Those in dire need of immediate precautionary action find this very useful. Over ten million documents have been compromised, including personal information of health care providers, medical records of patients, results of HIV tests, and social security numbers, as reported by the World Economic Forum. There have been incidents involving over 3 million medical records from 33 countries, with an average of 155,000 records impacted. There may be more papers compromised than what is currently believed. An efficient healthcare system must include safeguards to prevent cyberattacks, safe interaction between healthcare professionals and patients, and preserving private patient information [40].

III. STATE OF THE ART

Cybersecurity protects computer systems, networks, and data from unauthorized access, destruction, or alteration. Organizations in the private, public, and academic sectors and energy providers are protected against threats to their data's availability, privacy, and integrity that exist on the internet [41], [42]. This section gives a synopsis of cyber security, touching on current trends, recent advancements, and the techniques and technology used for security.

New cyber risks and trends develop regularly in today's cyber security scene; these threats and trends are always evolving and diversified, posing challenges to both persons and organizations. Social engineering, Malware, ransomware, phishing, data threats, availability threats, disinformation, distributed denial of service (DDoS), and supply chain targeting assaults are the most prominent cyber threats 2024 [43]. Losses in capital, interruptions in operations, harm to one's reputation, legal responsibility, bodily injury, and even dangers to national security are all possible outcomes of cyber threats. Companies in certain nations are taking measures to reduce the impact of cyberattacks, while in others, the degree of digital resilience varies by sector and country. Unfortunately, many companies still have difficulty putting adequate cybersecurity measures in place, which means they might be open to cyber-attacks. Intrusion detection and prevention systems, firewalls, antivirus software, encryption, and other security methods are used by

businesses and industries to enhance cyber security. Companies are also becoming serious about cyber security by instituting measures like regular software updates, stringent password policies, and cyber security training for employees [44]–[46].

New legislative frameworks, international cooperation, and innovation landscapes have emerged in response to the growing awareness of the importance and prevalence of cyber security worldwide. Several countries' legislative bodies have enacted measures to strengthen cyber defenses and protect citizens' personal information and academic records. The EU and the UN are only two of the international organizations that have developed rules and guidelines to promote cyber security and foster international cooperation [47]. The cyber security landscape is dynamic and ever-changing to account for newly emerging threats. Regarding cyber defense, new technologies like blockchain, cloud, and quantum computing provide both possibilities and threats [48], [49]. To make sure data is stored and shared safely, researchers are looking at these technologies. Improving the recognition and response to threats is being achieved via the use of AI and ML.

IV. RELATED WORK

A thorough review of AI in cybersecurity, including its applications, potential pitfalls, and advantages, is presented in the paper [50]. The researcher delves into artificial intelligence (AI) for cybersecurity, covering topics such as anomaly detection, intrusion detection, malware analysis, and its potential to tackle cybersecurity difficulties. Big data, the dangers of AI-based attacks, and the need for human supervision are some of the issues and possibilities that are addressed while talking about the usage of Artificial Intelligence in cyber-security. The essay wraps up by talking about the potential applications of AI in cyber-security and its future in the field.

In their comprehensive analysis of AI's role in cyber defense, the researchers [51] looked at the difficulties of smart medical and cybersecurity, such as the growing complexity and amount of data, the scarcity of trained personnel, and the escalating healthcare expense. Research on the possible uses of artificial intelligence (AI) in smart medical and cyber defense, as well as its ways to improve healthcare cybersecurity, is underway. Considerations such as the need for human supervision, the risks posed by AI-enabled attackers, and the dependence on massive volumes of data are all part of the analysis examining the pros and cons of using AI in various domains.

Cybersecurity risks and possible countermeasures for smart grids are covered in the research paper [52]. The study delves into several cyber risks that the smart grid encounters, including DoS assaults, phishing attempts, malware attacks, and insider threats. Additionally, they provide solutions to these cybersecurity issues. The study suggests training staff about cybersecurity risks and remedies and establishing security procedures as possible answers.

Internet of Things (IoT) device cyber threat recognition using (DL) techniques was the subject of study [53]. The study presents a joined deep learning (DL) strategy for identifying malware- and pirated-files across IoT networks, with an improved classification performance and a 97.46% success rate in detecting cyber security threats.

Explore the significant role that Artificial Intelligence plays in cyber-security by

identifying, preventing, and mitigating virtual risks [54]. The study examines the function, current status, and potential future applications of AI cutting-edge to reduce cyber threats. These applications include malware detection, vulnerability scanning, risk assessment, network intrusion detection systems, and security automation. This research builds on previous work showing how artificial intelligence (AI) may enhance decision-making, automate processes, and identify risks more efficiently in cyber security.

Another group that looked at virus detection using the Internet of Things (IoT) utilizing deep recurrent neural network techniques [55]. In response to the exponential increase of malware, the researchers have proposed a DNN to learn the differences between legitimate as well as mischievous apps on IoT devices since standard methods of malware detection have proven ineffective. Compared to more conventional signature-based approaches, the suggested model outperforms them when it comes to detecting malware in IoT devices, according to the researcher. However, the author fails to take into account the influence of evasion techniques, which render malware more evasive to conventional signature-based methods of detection, as well as the suggested DRNN models; hence, it is necessary to test the approaches on various IoT devices.

Using proprietary measures, [56] present a new approach to assessing the security of cyber-physical systems. The study's author suggests a method that employs a top-down hazard analysis tool called Systems-Theoretic Process investigation (STPA) and tailored matrices to guarantee a more thorough examination of safety and security. In order to address STPA's shortcomings, the researcher plans to combine STPA with custom measures. Risky control situations that might cause unanticipated losses can be identified using STPA. By using the custom matrices, we next investigate the likelihood that malicious actors may exploit these instances.

Investigated the use of blockchain technology to enhance the cyber defences of the medical IoT via the use of artificial intelligence [57]. The author explains how medical IoT might benefit from blockchain and artificial intelligence (AI) to make it more secure online. The authors argue that blockchain technology, in conjunction with artificial intelligence (AI) that can detect and prevent cyberattacks by recognizing patterns, may provide a secure and uncheckable way to store and transfer medical records.

In order to reduce data dimensionality and emphasize important characteristics, [58] suggest utilizing the AE model in conjunction with a cooperative DL model to identify abnormalities in cutting-edge IIoT information by learning long-term data associations. Using two real-world industrial IoT datasets, the researcher tests the model. Two datasets were used: one for water treatment and the other for gas pipelines. With a gas pipeline dataset accuracy of 99.3% and a water treatment dataset accuracy of 99.7%, the model proved to be quite accurate.

The potential monetary gains firms may get by receiving and analyzing cyber threat information (Cyber Threat Information CTI) provided through the US administration were the subject of study by [59]. Using a theoretical model, the researcher shows how the benefit of getting a CTI is proportional to the discrepancy between the CTI's degree of risk and the receiving organization's previous

assessment of that level of danger. The authors conclude that government agencies should not prioritise providing CTI for vulnerabilities rated as very dangerous. Rather, the government should prioritize spreading CTI, as it will most effectively target enterprises with reduced risk perceptions.

Using a qualitative approach, [60] examined the effect of beliefs on US cyber policy by following the evolution of public opinion on the cyber capabilities of the US military. While they mostly covered the CISA Plan for Defending the Nation's Vital Infrastructure (2020) and other CISA cyber plans, they did go back ten years to the US military's cyber strategies, beginning with the 2011 Cyber Operations Strategy. To identify key themes and gaps in US cyber policy, the author analyzed several cyber strategy subject areas.

V. METHODOLOGY

A. ELIGIBILITY CRITERIA FOR PAPER SELECTION

Using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses statement as a guide, this systematic review searches for scholarly works published between 2013 and 2024. Since there are numerous articles published in respectable journals, this study only reviewed those published during the last decade. Publications in English-language peer-reviewed journals are also taken into account. Lastly, it excludes studies that do not address cyber security, its applications, or the difficulties associated with it.

B. INFORMATION SOURCES

If you want to cover all the bases regarding cybersecurity or any other specialized subject, using numerous databases is a typical and efficient way to do so. Four databases—Scopus, SpringerLink, IEEE Xplore, as well as Web of Science—have been selected for this example. Because these databases provide a variety of scholarly sources pertinent to your issue, they make a solid choice.

C. SEARCH

Before searching several databases for relevant material, it is important to create an organized exploration policy with appropriate keywords, Boolean operators, and inclusion/exclusion criteria. To further organize and manage the articles you uncover throughout your exploration, you may want to explore utilizing reference management solutions. We use appropriate keyword-searching algorithms in this piece. By using keyword (search string) approaches, we were able to gather 200 papers.

D. SELECTION PROCESS

The study used abstract analysis to review the search results and find the relevant ones. The article was considered relevant if its abstract suggested a connection to cybersecurity. The article was deemed suitable for further review after this first screening if the abstract included cyber risk factors and related actions. We went from 200 to 40 items after the first screening. Following the reduction of articles, a comprehensive evaluation was carried out. Each of the forty articles chosen were read in its entirety. This exhaustive examination made a more thorough evaluation of the substance of each item possible.

VI. CHALLENGES OF CYBER SECURITY

Everyone, from individuals to governments, is very worried about cyber security in this digital age. Protecting data, networks, and electronic devices against unauthorized access, theft, or destruction is more important than ever due to the

proliferation of digital tools and gadgets. Cybersecurity, safeguarding a company's data, systems, and personnel against cyber-attacks, is encountering new difficulties due to technological progress. The article focuses on the cybersecurity industry's current problems and potential solutions for the future.

A. THE COMPLEXITY OF CYBER-ATTACKS

A major obstacle in cyber security is the complexity of cyber-attacks, which aim to get illegal access to computer systems and networks. Hackers and other cybercriminals create and use complex methods to breach security and steal sensitive information. Attacks such as multi-vector, polymorphic, file-less, zero-day, and advanced persistent employ sophisticated methods to get past defenses and exploit vulnerabilities.

The chemical industry, the diplomatic community, the information technology industry, and the military services are all targets of advanced persistent threats (APTs), which are highly planned and sophisticated assaults with the express purpose of stealing sensitive data and causing harm. Criminal groups and governments often work together in state-sponsored assaults to steal information and assets from weak points in infrastructure and other sectors in order to gain political, economic, and strategic benefits. All government buildings, factories, embassies, and military bases fall under this category. In 2009, there was an APT known as the "Aurora operation" that hit hard at influential IT and IT firms like Juniper Networks, Adobe, Google, and Google. This sophisticated assault used cutting-edge methods to breach these companies' network defenses, resulting in substantial IP theft.

An assault that takes advantage of a vulnerability that has just been discovered and has not been patched by software developers is known as a zero-day exploit. When hackers exploit security holes and then sell or utilize them, organizations are left vulnerable. To detect and prevent zero-day vulnerabilities, one needs advanced threat intelligence, behavior-based analysis, and rapid software patching. The number 33. There are five distinct phases to a 0-day exploit vulnerability attack's life cycle:

- **Zero-Day Attacks:** These assaults are the first to target software or hardware vulnerabilities that neither the general public nor the manufacturer of the affected product is aware of. Malicious actors, sometimes known as "black hat hackers," often find these vulnerabilities and keep them a secret from both the public and the party directly impacted. Situation: The Iranian nuclear facilities were the primary targets of the extremely advanced computer worm Stuxnet, which attacked supervisory control and data acquisition (SCADA) systems. It damaged uranium enrichment centrifuges by gaining access to industrial systems and manipulating them via several zero-day vulnerabilities.
- **Pseudo-Zero-Day Attacks:** When an exploit is still in the dark, but only a small group of malicious actors have found it, this is called a pseudo-zero-day assault. Although the vulnerability is still unknown, it is less of a mystery than in the first phase.
- **Potential for Pseudo-Zero-Day Attack:** While a vulnerability may have been discovered, it has not been extensively exploited. When security

researchers or companies notice anything unusual, it might be a sign of a vulnerability.

- **Passive:** This phase encompasses the time after a vendor has found, disclosed, and fixed or mitigated a vulnerability. Once this window has passed, the vulnerability is no longer considered a zero-day, and businesses must take action to secure their systems by implementing patches or remedies [61].

Zero-day assaults are very difficult to spot because they aim for flaws that defenders don't know about [62]. Intrusion detection systems, proactive security measures, and quick responses to newly found vulnerabilities are typically necessary to identify and protect against these assaults.

B. IOT SECURITY

IoT is an up-and-coming network that links billions of electronic items to the web. Through the use of Internet protocols, sensors and computing equipment are linked in this Network [63], [64]. Because of its weaknesses, the IoT has many major cybersecurity issues [65].

Hardware weakness Due to their low memory and processing capacities, Internet of Things (IoT) devices are prone to security vulnerabilities. Cybercriminals often target devices with inadequate default settings, outdated firmware and software, and no security updates [66], [67].

Devices connected to the internet collect and transmit vast amounts of personal and sensitive data. Keeping this information private and secret is of the utmost importance. Many IoT devices depend on cellular networks, Wi-Fi, Bluetooth, or other wireless communication protocols to provide network security. Intruders could eavesdrop, intercept, or alter data over various communication paths. The safety of an IoT network can be at risk due to inadequate encryption or a poorly configured network [68], [69].

C. AI-DRIVEN ATTACK

The rising digitization in many fields and the fast expansion of technical innovation have made cybersecurity a more complicated and hard issue. The use of machine learning and artificial intelligence (AI) is one of the new trends in cyberattacks. These technologies are considered technological advances. While AI may have some beneficial effects on cyber defense, it also has some harmful effects in the form of assaults that AI leads. There are two main categories of attacks that include AI: 1) an AI-assisted attack, in which human attackers are aided in the planning and execution of cyberattacks by AI and machine learning techniques, and 2) an AI-autonomous attack, in which agents powered by AI and machine learning attacks different industries independently of human intervention. Artificial intelligence (AI) assaults pose risks in many ways, including:

By using AI and ML to create convincingly realistic pictures, videos, audio, or text, deep fake assaults [70] may fool or mimic people or systems in social engineering schemes. Malicious actors may use deep fakes for various purposes, such as spreading misinformation, blackmailing, impersonating biometric identification, etc. Intentionally manipulating AI-generated media such as images, videos, audio, and texts can compromise cyber security systems that rely on AI and ML, such as those that detect malware, filter spam, recognize faces, and implement other biometric security measures [71].

Cybercriminals use botnets, which are networks of linked devices, to launch a

variety of assaults against a specific location [72]. Botnets launch a wide variety of assaults, including distributed denial of service attacks, spamming, data theft, and more. Botnet attacks employ AI and ML to automate and scale up assaults, discover targets, coordinate attacks, and elude detection, all while patching security flaws [73].

With reinforcement learning, the agent may gain knowledge from its surroundings by observing and responding to its actions and the rewards it gets. Cyberattacks enabled by autonomous AI may automate the procedures of patching and exploiting vulnerabilities and adapt, learn, and refine their plans depending on input and reaction from the targeted system, all thanks to RL machine learning technology [74].

Cybersecurity and society face a new threat from more sophisticated cyberattacks powered by artificial intelligence. It is difficult to identify and assign responsibility for the assaults since they conceal and alter their circumstances. Assaults powered by artificial intelligence automate rapidly scaling up assaults, rendering them defenseless and destroying the targeted resources.

D. CLOUD COMPUTING ESSENTIALS

As more and more businesses rely on cloud services, they expose themselves to new security risks. There are several cyber security issues that businesses rely on, including unauthorized access, data breaches, insecure APIs, shared infrastructures that pose data loss, security risks, service disruption that causes critical services to be unavailable, and other similar issues [75].

VII. OPPORTUNITIES, FUTURE RESEARCH DIRECTIONS

Academics and innovators face several challenges and opportunities in the ever-changing subject of cybersecurity. To overcome the challenges that the cybersecurity sectors are now facing, several possible solutions are being explored.

Utilizing state-of-the-art AI and ML methods, we can fortify cyber defenses, enhance the detection of cyber threats, automate security procedures, and forestall cyberattacks. Cyber threat detection systems powered by real-time AI assist cyber experts in sifting through massive amounts of data, searching for patterns of cyber-attacks, threats, and abnormalities. These systems can then automate security actions, allowing a more effective reaction to cyber assaults. In order to protect the specified sectors, biometric authentication is second only to AI and ML in terms of effectiveness. Biometric authentication may enhance security, which verifies a user's identity via distinct biological characteristics like fingerprints or face recognition. Hackers will have a more difficult time gaining access to networks and data when biometric authentication is used with traditional security methods like passwords.

There has to be quantum-resistant encryption technology to identify and react to any assaults connected to the development of quantum computers, which pose a risk to the cyber security of current cryptographic systems. To guarantee the long term security of critical cryptographic information, future researchers should concentrate on encryption algorithms resistant to quantum computers. The shortage of trained experts and general public ignorance of cyber threats are two additional major issues with cyber security. Academics, researchers, and policymakers should prioritize cyber education and awareness-raising in the future (human-

centric security). In the future, governments, academics, and researchers should put much effort into understanding how human behavior affects cyber security. Advocating for best practices in cyber security, creating user interfaces for security that are more participatory (like Chabot apps), and studying the socio-technical elements of cyber security are all parts of human-centric security.

In order to automate the reaction to cyber threats, the automation of security procedures is an extremely important aspect of the cyber business. Security process automation and orchestration may enhance organizations' attack response capabilities. The development of security monitoring platforms and the automation of cyber security processes are essential, but so is the establishment of a threat intelligence mechanism and a system for the exchange of information amongst businesses, governments, and other organizations in order to better prepare for and react to cyber-attacks. Scholars, researchers, and cyber security professionals should work together to establish common frameworks and platforms for the exchange of cyber risks and the establishment of joint cyber defense mechanisms for governmental agencies, businesses, and nonprofits.

In today's interconnected world, safeguarding personal information and preventing unauthorized access is paramount. Consequently, there has to be an improvement and strengthening of privacy rules as well as data protection and privacy preservation measures. Consequently, the study's emphasis should be on privacy-reserving methods that make use of homomorphic encryption and multi-party computing in order to fortify privacy rules. Along these lines, one of the most pressing issues in bolstering a company's cyber defenses is the development of blockchain technology. Researchers have looked at using blockchain technology in many cybersecurity domains, including transactions supply chains [76], and medicine [77], [78]. Distributed ledger systems and blockchain technology provide a fantastic option for decentralized systems and security. Despite blockchain technology's significant contributions to cyber security, it has its share of problems. For example, smart contracts are susceptible to attacks, consensus protocols like PoS and PoW are vulnerable, and blockchain technology relies on external systems like oracles, leading to inconsistencies and vulnerabilities. A secure and reliable system must be built by weighing the advantages of blockchain and DLT against the associated cybersecurity risks (Figure. 1 and Table 1).

VIII. CONCLUSION

Cybersecurity refers to the practice of keeping information systems secure against dangers that can compromise its accessibility, integrity, or secrecy. Individuals and businesses rely heavily on digital technology, making cyber security a must-have for their protection. Healthcare facilities, banks, government agencies, educational institutions, smart cities, grid systems, and the armed forces are just a few places where cyber security may be useful. A wide variety of threats, including hackers, thieves, terrorists, state actors, and even insiders, provide unique difficulties to cyber security. Some of the problems the cyber security sector has to deal with include advanced cyber-attacks, cyber-attacks that use reinforcement learning, malware that is enabled by AI, the susceptibility of IoT technology, cloud security concerns, and the use of encryption. Nonetheless, these problems may be amenable to future developments in

cybersecurity, such as biometric identification, sophisticated AI, ML, and quantum computing (quantum-secure encryption). Cybersecurity must remain a priority for people, organizations, and governments to protect our digital assets, networks, and data from cybercriminals.

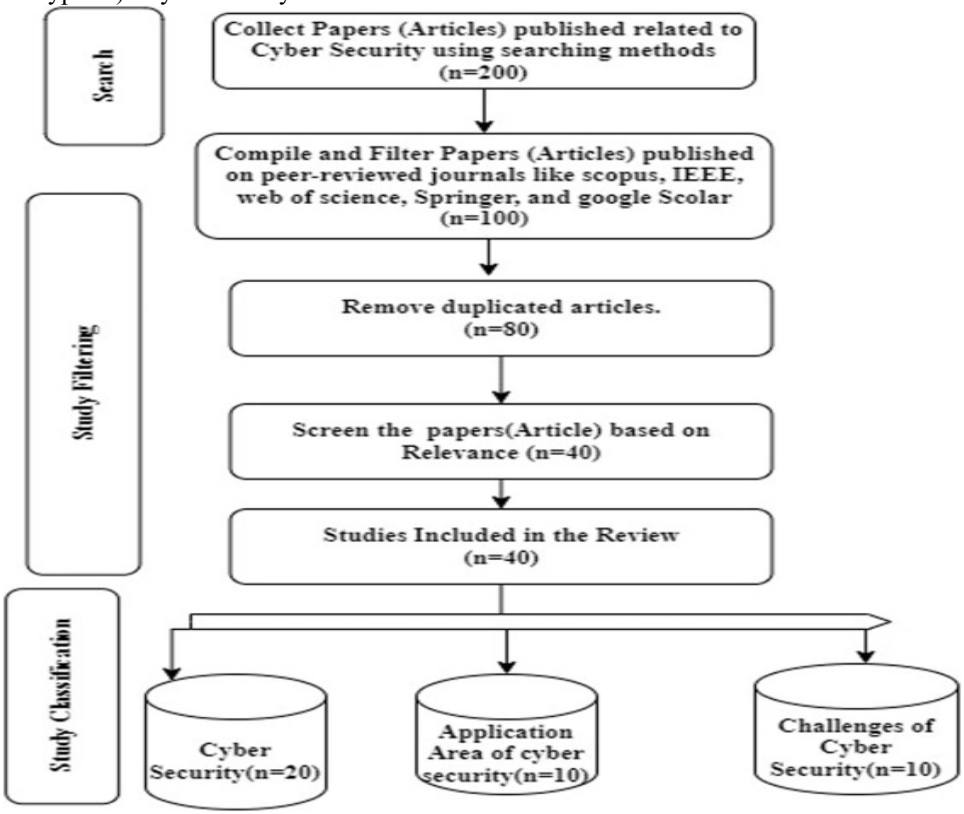

FIGURE 1. Process for searching literature and classifying studies

TABLE I

COMPILATION OF RELEVANT STUDIES

Study	Methodology	Conclusions	Challenges	Ref.
Utilization of Blockchain Technology for Enhanced Cybersecurity in Medical Applications	Integrated Blockchain and AI strategies	The study highlighted the effectiveness of blockchain technology in safeguarding medical records and IoT medical devices.	The study's limitations include a lack of comprehensive data on medical device security, questioning the scalability of the proposed solutions.	[74]

Study	Methodology	Conclusions	Challenges	Ref.
Systemic Analysis of Safety and Security in Cyber-Physical Systems Using a Novel Matrix Approach	Application of system-theoretic matrix	This framework was efficient in identifying potential risks and aiding in the development of countermeasures for system vulnerabilities.	Limitations arise due to the singular focus on case study analysis, necessitating further empirical research for broader applicability.	[75]
Predictive Modeling for Cyber Threat Detection in Industrial IoT Using Advanced Neural Networks	LSTM and AE-based neural network models	The proposed model showcased high precision in identifying cyber threats within IIoT environments.	The evaluation of the model was confined to IIoT datasets, suggesting a potential limitation in generality across diverse industrial systems.	[77]
Advancing Healthcare 4.0: Blockchain Integration for Secure EHR Systems	Implementation of blockchain within healthcare IT to enhance EHR security	The development introduced a robust model offering secure and efficient access to EHRs, leveraging blockchain technology.	The adoption of this model is challenged by high costs, the necessity for skilled personnel, and the absence of unified data exchange standards.	[75]
Optimizing Interagency Cyber Threat Intelligence Sharing Through Theoretical Analysis	Theoretical framework for optimizing intelligence sharing among agencies	The research posits that the effectiveness of cyber threat intelligence sharing is not contingent solely on the amount shared but also on the organizational culture.	The study concludes with theoretical analysis without empirical data to substantiate the findings.	[78]
Assessment of Belief Influence on US Cyber	Qualitative assessment of belief systems on US cyber	The study uncovered significant strategic gaps	The insights are tailored to the U.S. military cyber departments, limiting wider relevance.	[78]

Study	Methodology	Conclusions	Challenges	Ref.
Strategy Evolution	strategy	within the U.S. cyber strategy by tracing its evolution and belief influences.		
Classification Strategies for Cyber Threats in IoT Using Deep Learning	Cyber threat identification via deep learning models	The classification method proves effective for recognizing malicious cyber activities within IoT networks.	The method's viability is curtailed by computational demands and potential bias in the dataset used for model training.	[31]

Author Contribution

Musharaf Hassan: conceptualization, methodology, investigation, writing – original draft. **Muhammad Shahid Azeem:** supervision, validation, writing – review & editing, project administration. **Faisal Hameed:** data curation, formal analysis, investigation. **Mubeen Ashraf:** software, visualization, validation. **Atif Masih:** investigation, writing – review & editing, validation.

Conflict of Interest

The authors of the manuscript have no financial or non-financial conflict of interest in the subject matter or materials discussed in this manuscript.

Data Availability Statement

Data supporting the findings of this study will be made available by the corresponding author upon request.

Funding Details

No funding has been received for this research.

Generative AI Disclosure Statement

The authors did not use any type of generative artificial intelligence software for this research.

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," *J. Cybersecurity*, vol. 7, no. 1, 2021, Art. no. tyab005, doi: https://doi.org/10.1093/cybsec/tyab005.

[2] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, 2020, Art. no. 107094, doi: https://doi.org/10.1016/j.comnet.2019.107094.

[3] S. Colabianchi, "*Humans in Cyber Resilience: Managerial and Operational Opportunities*," Uniroma Research Catalog, 2023.

[4] 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 using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, Aug. 2019, doi: https://doi.org/10.1109/ACCESS.2019.2937347.

[5] J. Kaur and K. R. Ramkumar, "The recent trends in cyber security: A review," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5766–5781,

Sep. 2022, doi: https://doi.org/10.1016/j.jksuci.2021.01.018.

[6] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," *Arab. J. Sci. Eng.*, vol. 45, no. 4, pp. 3171–3189, Jan. 2020, doi: https://doi.org/10.1007/s13369-019-04319-2.

[7] M. Alshehri, "Blockchain-assisted cyber security in medical things using artificial intelligence," *Electron. Res. Arch.*, vol. 31, no. 2, pp. 708–728, 2023, doi: https://doi.org/10.3934/era.2023035.

[8] A. Tomer, J. K. Gautam, J. K. Gupta, H. Singh, and A. Deshwal, "Psychological, economical, privacy and personnel impacts of cybercrime: Is cyber crime exploits technology and digital platforms," *J. ReAttach Ther. Dev. Divers.*, vol. 6, no. 8s, pp. 114–133, 2023.

[9] E. O. Obidimma and O. Ishiguzo, "Cybercrime investigation and prosecution in Nigeria," *African J. Criminal Law Jurisprud.*, vol. 8, 2023.

[10] K. J. Raval, N. K. Jadav, T. Rathod, S. Tanwar, V. Vimal, and N. Yamsani, "A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions," *Int. J. Crit. Infrastruct. Prot.*, vol. 41, 2023, Art. no. 100601, doi: https://doi.org/10.1016/j.ijcip.2023.100601.

[11] J. Kaur, "IoT empowered smart cities for green healthcare," in *Proc. ICCCIS*, 2023, doi: https://doi.org/10.4018/979-8-3693-2373-1.ch016.

[12] P. Mishra and G. Singh, "Energy management systems in smart cities and smart homes: A technical review," *Energies*, vol. 16, no. 19, Sep. 2023, Art. no. 6903, doi: https://doi.org/10.3390/en16196903.

[13] O. A. Ajala and O. A. Balogun, "Leveraging AI/ML for anomaly detection, threat prediction, and automated response," *World J. Adv. Res. Rev.*, vol. 21, no. 1, pp. 2584–2598, 2024, doi: https://doi.org/10.30574/wjarr.2024.21.1.0287.

[14] M. Ozkan-Okay et al., "A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions," *IEEE Access*, vol. 12, pp. 12229–12256, Jan. 2024, doi: https://doi.org/10.1109/ACCESS.2024.3355547.

[15] A. Manoharan and M. Sarker, "Artificial intelligence and machine learning for next-generation threat detection and response in cybersecurity," 2023.

[16] A. Chakraborty, A. Biswas, and A. K. Khan, "Artificial intelligence for cybersecurity: Threats, attacks and mitigation," in *Artificial Intelligence-based Cybersecurity: Protecting Critical Infrastructure*, Springer, 2023, doi: https://doi.org/10.1007/978-3-031-12419-8_1.

[17] M. J. Khan, "Securing network infrastructure with cybersecurity frameworks and AI," *World J. Adv. Res. Rev.*, vol. 17, no. 2, 2023, pp. 803–813, doi: https://doi.org/10.30574/wjarr.2023.17.2.0308.

[18] M. Mijwil, O. J. Unogwu, Y. Filali, I.

Bala, and H. Al-Shahwani, "Exploring the top evolving cybersecurity trends," *Mesopotamian J. Cybersecurity*, vol. 3, no. 1, 2023, Art. no. 10, doi: https://doi.org/10.58496/MJCS/2023/010.

[19] M. S. Bakare, A. Abdulkarim, M. Zeeshan, and A. U. Shuaibu, "Residential demand-side energy management in smart grid: A survey," *Energy Inform.*, vol. 6, no. 1, Mar. 2023, Art. no. 4, doi: https://doi.org/10.1186/s42162-023-00262-7.

[20] T. Kataray, B. Nitesh, B. Yarram, S. Sunil, B. C. Seet, and O. Olugbenga, "Integration of smart grid with renewable energy sources: Opportunities and challenges," *Sustain. Energy Technol. Assess.*, vol. 58, Aug. 2023, Art. no. 103363, doi: https://doi.org/10.1016/j.seta.2023.103363.

[21] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems," *Electr. Power Syst. Res.*, vol. 223, 2023, Art. no. 109510, doi: https://doi.org/10.1016/j.epsr.2023.109510.

[22] A. Rekeraho, D. T. Cotfas, P. A. Cotfas, T. Acheampong, and R. Balan, "Cybersecurity threats and challenges in IoT-based renewable energy systems," *Int. J. Inf. Secur.*, vol. 23, pp. 679–698, 2024, doi: https://doi.org/10.1007/s10207-023-00762-3.

[23] D. Mashima, Y. Chen, M. M. Roomi, K. Kandasamy, and A. Chattopadhyay, "Cybersecurity for modern smart grids: Challenges and perspectives," *arXiv*, 2024, doi: https://doi.org/10.1561/9781638282952.

[24] R. K. Jha, "Cybersecurity and cyber forensic for smart grid," *Recent Res. Rev. J.*, vol. 23. no. 7, 2023.

[25] A.-A. Bouramdane, "Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options," *J. Cybersecurity Privacy*, vol. 3, no. 4, pp. 662–707, 2023, doi: https://doi.org/10.3390/jcp3040031.

[26] M. Liu, F. Teng, Z. Zhang, L. Chen, and Z. Wang, "Cyber-resiliency of DER-based microgrids: A review," *IEEE Trans. Smart Grid*, vol. 15, no. 5, pp. 4998–5030, 2024, doi: https://doi.org/10.1109/TSG.2024.3373008.

[27] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Secur. Appl.*, vol. 2, Art. no. 100031, 2024.

[28] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Secur. Appl.*, vol. 2, 2024, Art. no. 100031, doi: https://doi.org/10.1016/j.csa.2023.100031.

[29] A. Manimuthu, T. Ngo, and A. Chattopadhyay, *Internet of Vehicles Security*, Springer, 2023.

[30] M. Sadaf, Z. Iqbal, A. R. Javed, I. Saba, and M. Krichen, "Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects,"

Technologies, vol. 11, no. 5, Sep. 2023, Art. no. 117, doi: https://doi.org/10.3390/technologies11050117.

[31] A. Habbal, M. K. Ali, and M. A. Abuzaraida, "Artificial intelligence trust, risk and security management (AI TRiSM): Frameworks, applications, challenges and future research directions," *Expert Syst. Appl.*, vol. 240, Apr. 2024, Art. no. 122442, doi: https://doi.org/10.1016/j.eswa.2023.122442.

[32] M. Krichen, "Formal methods and validation techniques for ensuring automotive systems security," *Information*, vol. 14, no. 1, Jan. 2023, Art. no. 35, doi: https://doi.org/10.3390/info14010035.

[33] V. Demertzi, S. Demertzis, and K. Demertzis, "An overview of privacy dimensions on the industrial internet of things (IIoT)," *Appl. Sci.*, vol. 13, no. 3, Jan. 2023, Art. no. 1465, doi: https://doi.org/10.3390/app13031465.

[34] M. N. Birje and S. S. Hanji, "Internet of things based distributed healthcare systems: A review on security challenges and recent solutions," *J. Data Inf. Manag.*, vol. 2, pp. 149–165, May 2020, doi: https://doi.org/10.1007/s42488-020-00027-x.

[35] B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-based applications in healthcare devices," *J. Healthcare Eng.*, vol. 2021, 2021, Art. no. 6632599, doi: https://doi.org/10.1155/2021/6632599.

[36] S. Basheer, A. S. Alluhaidan, and M. A. Bivi, "Real-time monitoring system for IoT heart-disease prediction using machine learning," *Soft Comput.*, vol. 25, pp. 10591–10606, May 2021, doi: https://doi.org/10.1007/s00500-021-05865-4.

[37] K. Balasamy, N. Krishnaraj, J. Ramprasath, and K. Abitha, "Evolving a secure framework for internet of things with medical devices," 2022.

[38] T. Gebremichael et al., "Security and privacy in the industrial internet of things: Current standards and future challenges," *IEEE Access*, vol. 8, pp. 152351–152366, Aug. 2020, doi: https://doi.org/10.1109/ACCESS.2020.3016937.

[39] M. M. Mogadem, Y. Li, and D. L. Meheretie, "A survey of internet of energy security based on heterogeneous network," *Cluster Comput.*, vol. 25, pp. 3983–4002, 2022, doi: https://doi.org/10.1007/s10586-021-03423-z.

[40] O. I. Falowo and J. B. Abdo, "DDoS threat projection in a 6G mobile heterogeneous network using deep learning," *IEEE Access*, vol. 12, pp. 39221–39237, Mar. 2024, doi: https://doi.org/10.1109/ACCESS.2024.3376682.

[41] S. Saeed, S. A. Altamimi, N. A. Alkayyal, A. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," *Sensors*, vol. 23, no. 15, July 2023, Art. no. 6666, doi: https://doi.org/10.3390/s23156666.

[42] M. A. Afifi, "Information security vulnerabilities and solutions," *J. Comput. Sci.*, vol. 16, no. 8, pp. 1165–1173, 2020.

[43] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity enterprises policies: A comparative study," *Sensors*, vol. 22, no. 2, Jan. 2022, Art. no. 538, doi: https://doi.org/10.3390/s22020538.

[44] F. R. Bechara and S. B. Schuch, "Cybersecurity regulatory challenges," *J. Financial Crime*, vol. 28, no. 3, pp. 706–717, 2021, doi: https://doi.org/10.1108/JFC-10-2020-0208.

[45] S. Balogh, O. Gallo, R. Ploszek, P. Spacek, and P. Zajac, "IoT security challenges: Best practices and recent advances," *Electronics*, vol. 10, no. 21, Oct. 2021, Art. no. 2665, doi: https://doi.org/10.3390/electronics10212665.

[46] T. d BH, F. Lehara, and B. Sarajevo, "Future cyber technologies and their impact on society," 2022.

[47] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, "The impact and limitations of artificial intelligence in cybersecurity: A literature review," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 11, no. 9, 2022, doi: https://doi.org/10.17148/IJARCCE.2022.11909.

[48] Z. Zhang et al., "Artificial intelligence in cyber security: Research advances, challenges, and opportunities," *Artif. Intell. Rev.*, vol. 55, pp. 1029–1053, 2022, doi: https://doi.org/10.1007/s10462-021-09976-0.

[49] N. N. Abbas, T. Ahmed, and S. H. U. Shah, "Investigating the applications of artificial intelligence in cyber security," *Scientometrics*, vol. 121, pp. 1189–1211, 2019, doi: https://doi.org/10.1007/s11192-019-03222-9.

[50] S. Riaz et al., "Malware detection in internet of things (IoT) devices using deep learning," *Sensors*, vol. 22, no. 23, 2022, Art. no. 9305, doi: https://doi.org/10.3390/s22239305.

[51] L.-S. Liew, G. Sabaliauskaite, N. K. Kandasamy, and W. K. G. Seah, "A novel system-theoretic approach for safety and security co-engineering of cyber-physical systems," *Telecom*, vol. 2, no. 2, pp. 168–184, 2021, doi: https://doi.org/10.3390/telecom2020012.

[52] S. Latif et al., "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network," *IEEE Access*, vol. 8, pp. 89337–89350, 2020, doi: https://doi.org/10.1109/ACCESS.2020.2994079.

[53] M. Alshehri, "Blockchain-assisted cybersecurity for internet of things in energy internet: A survey," *Electron. Res. Arch.*, vol. 31, no. 2, pp. 708–728, 2023, doi: https://doi.org/10.3934/era.2023035.

[54] A. Yazdinejad et al., "An ensemble deep learning model and explainable AI for joint cyber-threat hunting and explainability in industrial internet of things," *Digit. Commun. Netw.*, vol. 9, no. 5, pp. 1123–1130, 2023, doi: https://doi.org/10.1016/j.dcan.2022.09.008.

[55] J. Dykstra, L. A. Gordon, M. P. Loeb, and W. Zhou, "The role of information asymmetry in cybersecurity policy and markets," *J. Cybersecurity*, vol. 9, no. 1, 2023, doi: https://doi.org/10.1093/cybsec/tyac016.

[56] E. D. Lonergan and J. Schneider, "Signaling and cyber conflict: Why sending the right message matters in cyberspace," *J. Cybersecurity*, vol. 9, no. 1, 2023, doi: https://doi.org/10.1093/cybsec/tyad003.

[57] E. S. Barry, J. Merkebu, and L. Varpio, "The what, the why and the how: A review of the use of narrative literature in health professions education research," *Perspect. Med. Educ.*, vol. 11, pp. 5–12, Sep. 2022, doi: https://doi.org/10.1007/S40037-022-00725-9.

[58] A.-A. M. AL-Hawamleh, "Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 2, 2023, doi: https://doi.org/10.14569/IJACSA.2023.0140289.

[59] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues," *Comput. Secur.*, vol. 125, Feb. 2023, Art. no. 103028, doi: https://doi.org/10.1016/j.cose.2022.103028.

[60] A. Aslam, K. N. Qureshi, and T. Newe, Future Privacy and Trust Challenges for AIoT Networks, in *Artificial Intelligence of Things (AIoT) New Standards, Technologies and Communication Systems*, K. N. Qureshi, T. Newe, Eds. CRC Press, 2024.

[61] A. N. Lone, S. Mustajab, and M. Alam, "A comprehensive study on cybersecurity challenges and opportunities in the IoT world," *Secur. Privacy*, vol. 6, no. 6, Dec. 2023, Art. no. 318, doi: https://doi.org/10.1002/spy2.318.

[62] Ö. Aslan et al., "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, Mar. 2023, Art. no. 1333, doi: https://doi.org/10.3390/electronics12061333.

[63] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and Y. Zhang, "Advances in IoT security: Vulnerabilities, enabled criminal services, attacks, and countermeasures," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11224–11239, Mar. 2023, doi: https://doi.org/10.1109/JIOT.2023.3252249.

[64] H. Verma, N. Chauhan, and L. K. Awasthi, "Comprehensive analysis of IoT-based patient health monitoring system: A systematic review," *Comput. Sci. Rev.*, vol. 47, 2023, Art. no. 100529, doi: https://doi.org/10.1016/j.cosrev.2022.100529.

[65] B. Guembe et al., "The emerging threat of AI-driven cyber attacks: A review," *Appl. Artif. Intell.*, vol. 36, no. 1, Mar. 2022, Art. no. 2037254, doi: https://doi.org/10.1080/08839514.2022.2037254.

[66] B. Bera, A. K. Das, M. S. Obaidat, P. Vijayakumar, P. Hsiao-Hwa, and A. K. Sangaiah, "AI-enabled blockchain-based access control for malicious attacks detection and mitigation in IoE," *IEEE Consum. Electron. Mag.*, vol. 10, no. 4, pp. 82–92, 2021, doi: https://doi.org/10.1109/MCE.2020.3040541.

[67] N. J. Singh et al., "Detection of various

IoT attacks using botnet: A review," *Secur. Privacy*, vol. 7, no. 1, 2024, doi: https://doi.org/10.1002/spy2.355.

[68] V. Vouvoutsis, F. Casino, and C. Patsakis, "IoT-aware anti-evasion scheme based on binary emulation for malware identification," *J. Inf. Secur. Appl.*, vol. 68, 2022, Art. no. 103268, doi: https://doi.org/10.1016/j.jisa.2022.103268.

[69] R. Maeda and M. Mimura, "Automating post-exploitation with deep reinforcement learning," *Comput. Secur.*, vol. 100, 2021, Art. no. 102108, doi: https://doi.org/10.1016/j.cose.2020.102108.

[70] A. Bécue, I. Praça, and J. Gama, "Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities," *Artif. Intell. Rev.*, vol. 54, pp. 3849–3886, Feb. 2021, doi: https://doi.org/10.1007/s10462-020-09942-2.

[71] A. Chakraborty, A. Biswas, and A. K. Khan, *Artificial Intelligence for Cybersecurity*, Springer, 2023, doi: https://doi.org/10.1007/978-3-031-28552-6.

[72] R. Naveenan and G. Suresh, *Cyber Risk Management in the Financial Sector*. Routledge, 2023.

[73] A. K. Yadav and D. Kumar, "Blockchain in pharmaceutical supply chain management for Covid-19 vaccine," *Int. J. Prod. Econ.*, vol. 255, 2023, Art. no. 108666, doi: https://doi.org/10.1016/j.ijpe.2022.108666.

[74] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.018.

[75] H. Miriam, D. Doreen, D. Dahiya, and T. Robin, "Secured cyber security algorithm for healthcare system using blockchain technology," *Intell. Autom. Soft Comput.*, vol. 35, no. 2, pp. 1889–1906, 2023, doi: https://doi.org/10.32604/iasc.2023.028850.

[76] S. Latif *et al.*, "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network," *IEEE Access*, vol. 8, pp. 89337–89350, May 2020, doi: https://doi.org/10.1109/ACCESS.2020.2994079.

[77] B. Shin and P. B. Lowry, "A review and theoretical explanation of the cyber-threat intelligence (CTI) capability that needs to be fostered in information security practitioners and teams," *Comput. Secur.*, vol. 96, 2020, Art. no. 101761, doi: https://doi.org/10.1016/j.cose.2020.101761.

[78] B. Lilly and J. Cheravitch, "The past, present, and future of Russia's cyber strategy and forces," in *Proc. 12th Int. Conf. Cyber Conflict (CyCon)*, pp. 129–155, 2020, doi: https://doi.org/10.23919/CyCon49761.2020.9131723.