An Overview of Cybersecurity: Key Issues and Emerging Solutions

Review Paper

Medha Wyawahare*
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
medha.wyawahare@vit.edu

Milind Rane
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
milind.rane@vit.edu

Sharvari Bodas
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
sharvari.bodas21@vit.edu

Swarali Damle
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
sharvari.bodas21@vit.edu

*Corresponding author

Shoumik Daterao
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
shoumik.daterao21@vit.edu

Arya Chopda
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
arya.chopda21@vit.edu

Siddharth Bhorge
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
siddharth.bhorge@vit.edu

Abstract *– In an age where digital interconnectivity permeates every aspect of daily life, cyber threats have grown more advanced, and as a result, they pose very dangerous threats to individuals, enterprises, and governments all the same. This review offers a systematic synthesis of cyber threats, new attack surfaces, and new defense techniques, with emphasis on the convergence of artificial intelligence (AI) and domain-specific issues within cloud, IoT, and mobile networks. Upcoming new technologies like quantum and 5G further present risks that require further new developments in cryptography and solutions in network security. In addition to providing an overview of current work, this paper makes an original contribution by presenting a comparison of prominent methods and studies, divided by defense strategy, domain, and performance measures. The approach for the study focuses more on the requirement of technical innovation to be blended with frameworks that are ethical and regulatory in nature, addressing complex and dynamic threats in the nature of cybersecurity. Recommendations for further research in the future include quantum-resistant algorithms, improved AI models that can be used for more effective cybersecurity, and creation of ethical standards in the digital defense of the resources of the nation to do it more robustly and responsibly.*

Keywords: *information security, Cyberattacks, Intrusion detection system, SIEM, SOAR, Security system, security awareness*

Received: April 28, 2025; Received in revised form: July 3, 2025; Accepted: August 10, 2025

1. INTRODUCTION

Over the recent explosion of digital landscapes, unprecedented levels of cyber threats have threatened individual, corporate, and governmental lifelines. With the increasing interconnectedness of systems, the attack surface that threatens cybercriminals has more than expanded, allowing for greater sophistication in exploiting vulnerabilities [1]. The aftermath of cyber attacks tends to be multifarious; therefore, it may lead to financial damage, data breaches [2] [3]. The new world of cybersecurity also includes the challenge of growing threats. In addition to this, attacks such as Advanced Persistent Threats are well-financed adversaries that conduct sustained, targeted attacks on networks. APTs aim to breach into organizations' networks; often, these go unnoticed for long durations by exploiting zero-day vulnerabilities, thereby putting sensitive data and critical systems at a considerable risk [4], [5]. These attacks require defense systems not only to block the intrusion but to identify it and respond promptly.

Artificial Intelligence (AI) and Machine Learning (ML) now stand as weapons in this cyber battle. They can process huge amounts of real-time data for detecting malicious behavior which may be missed by traditional techniques [6]. AI-based solutions can be used to automatically identify threats, thus allowing cybersecurity teams to react more quickly to incoming threats [7]. Yet while AI offers new opportunities for improving cybersecurity, it also represents new challenges because attackers might try to defeat or trick AI models to avoid security controls [8]. IoT has further confused matters in its attempts to create an increasingly sophisticated Internet of Things, but on this count, the expanding global complexity does nothing but add to the challenge of cybersecurity. There are billions of IoT devices in operation today, many with weak or no security, which attackers have identified as routes to mount large-scale attacks, for instance, DDoS [9], [10]. Last is hard to secure because diversity makes it challenging to patch in the field found after deployment. Integration of IoT into critical infrastructure increases the demand for stronger security protocols in safeguarding such devices against cyberattacks [11]. In addition, blockchain technology is gaining attention for its potential application for cyber security. The decentralized nature of blockchain and its cryptographic foundations would make such a framework immune to tampering, hence providing a safe place for the storage and transmission of data [12]. Blockchain has been researched in applications involving secure communication, digital identity verification, and transaction monitoring. However, despite all this promise, it has numerous challenges facing it, with major ones having to do with scalability and high energy consumption. These aspects limit its higher adoption into cybersecurity frameworks [13].

The other tool part of the application in modern cybersecurity efforts is the Security Information and Event Management (SIEM) systems which facilitate the monitoring of data from different sources in support of real-time threat visibility [6]. With SOAR, SIEM platforms can provide faster and more effective incident responses and therefore potentially contain situations before significant damages are incurred [14]. Such systems are critical to guiding organizations to better manage the thousands of alerts thrown off by modern cybersecurity tools [7].

In the future, therefore, it is going to be one of the most significant challenges for cybersecurity. Once achieved, and fully realized, quantum computers may break most encryption algorithms that today are used to secure data [12]. This puts direct endangerment to confidentiality related to sensitive information because quantum algorithms can be used to decrypt data that currently is considered secure [15]. As an answer, researchers are developing quantum-resistant cryptographic algorithms, which will be obligatory to maintain data security post-quantum [13], [14].

While there are many review studies in the field of cybersecurity, the majority concentrate on either individual technologies, for instance, machine learning for intrusion detection, or individual fields like cloud or IoT security. Even fewer works offer a broad understanding across technical, architectural, and ethical aspects. This paper tries to bridge the gap by providing a systematic, multi-domain overview that categorizes and contrasts current threats and defenses and highlights their interdependencies and real-world implications. In contrast to descriptive only surveys, this overview focuses on comparative analysis through summarizing recent empirical literature, reviewing defense methods with performance-based assessments, and signaling new issues like AI-enabled attacks, quantum-age vulnerabilities, and the ethical need for governing cybersecurity systems.

Through synthesizing existing literature using a domain-based perspective and analysing strengths and weaknesses of dominating methodologies, this paper intends to act as an encompassing guide for researchers, professionals, and policymakers. Not only does it scan available work, but it also critically outlines areas of research gaps and suggests avenues for future investigation—especially in adaptive AI frameworks, quantum-resilient cryptographic protocols, and cross-disciplinary security paradigms.

2. CYBER THREATS AND ATTACK VECTORS

Cyber threats are diverse, employing various tactics to exploit vulnerabilities in systems and networks. The most common attack are as given below.

2.1. MALWARE

A malicious software whose forms include viruses, worms, ransomware, and spyware; they are primarily targeted at harming or stealing data from systems. It mainly spreads through phishing emails or com- promised websites or malicious downloads on personal as well as corporate devices [16]. A very destructive form of malware is ransomware that encrypts data and demands ransom payments for recovery. It has also shown a drastic surge in its attacks lately targeting sectors such as healthcare and finance that resulted in losses not only to the financial implications but also to the operational shutdowns [17]. The polymorphic malware does pose other kinds of challenges due to the constant changing of code so as not to be detected by the traditional antivirus solutions [18]. Mobile malware has gained and risen where attackers exploit flaws in mobile applications and utilize this to gain access to sensitive information on the smartphone [19].

2.2. PHISHING

Phishing remains one of the very successful attack vectors, operating on deception to steal sensitive information or install malware. While initially email-centric, phishing now encompasses various modes like social media and SMS, commonly known as smishing [20]. Phishing attacks typically capture login credentials, financial information, or personal details. One type of targeted phishing attack such as Spear phishing targets a specific individual, usually with a high position or handling sensitive and critical systems [21]. Most attacks use phishing as the entry point to launch a large-scale attack, for example, a business email compromise, wherein attackers impersonate executives to approve fraudulent financial transactions [22].

2.3. SOCIAL ENGINEERING AND INSIDER THREATS

They exploit psychological vulnerabilities rather than technical ones. In any case, their means is always the psychological manipulation that forces users to divulge confidential information. Other attacks with phishing or impersonation attempts are usually found along with these attacks. The insider threat is another major one-person threat. Insider refers to those who gain authorized access and accidentally or intentionally compromise security. A disgruntled employee or one who has mal-intentions may misuse this access to steal sensitive data or sabotage operations [23]. Even unintentional acts, for instance, clicking an email phishing, or sharing one's credentials, can potentially cause large breaches in security [24].

2.4. APT ADVANCED PERSISTENT THREATS

Advanced Persistent Threats, also known as APTs, are long-lasting attacks that are usually performed by nation-state actors or well-funded criminal enterprises. They usually employ a combination of social engineering, phishing, and zero-day exploits to gain a presence in the target's network and can evade detection for years. The purpose of such an attack is to steal sensitive data or disrupt operations in critical infrastructure sectors, such as energy, finance, or defense [25]. This is why APTs, with persistence and stealth attributes, are highly dangerous as they most of the time evade the traditional security measures implemented, and when caught late in the day, it might lead to catastrophic damage.

2.5. EMERGING THREATS

Cyber threats are numerous, using various tactics they are exploiting weaknesses in the network. Of the many attack vectors, malware, phishing, insider threats, and APTs are the most common. Each is constantly evolving, becoming more complicated and destructive with time.

2.5.1. IoT Vulnerabilities

IoT devices have drastically increased the attack surface for cybercriminals with their sheer growth. IoT devices are mostly not very secure with minimum encryption and authentication in place. As a result, these devices have now become the most sought-after by hackers [26]. They are increasingly connected to critical systems, including healthcare and industrial controls and their compromise will have very disastrous impacts. Botnet attacks, including the Mirai botnet, have proved the power of hacking unsecured IoT devices in massive Distributed Denial of Service (DDoS) attacks [27].

2.5.2. AI-driven Attacks

Cyber-criminals are now arming themselves with Artificial Intelligence to carry out more efficient and evasive attacks. It has been referenced that AI-based attacks use the algorithm in machine learning to auto-scanner vulnerabilities, craft sophisticated phishing campaigns, and avoid discovery while in the learning phase about defensive patterns of targeted systems [28]. For instance, AI can prepare customized phishing messages that may most probably fool their recipient, thus raising the success percentage of these assaults as seen in [29].

2.5.3. Ransomware Evolution

The trend with ransomware attacks has become even more aggressive in terms of methods, one of which is double extortion. In such an approach, unless a ransom is paid, attackers encrypt the data and they jeopardize divulging sensitive information. Indeed, this method has been widely proven to be highly effective at forcing organizations to pay ransoms due to reputational damage and legal consequences [30]. Critical infrastructure targeting, including hospitals and energy sectors, is also one of the types of attacks that made ransomware one of the significant cybersecurity threats of today [27].

3. CYBER DEFENSE TECHNIQUES

Cyber defense techniques have various techniques aimed at proactively identifying and mitigating cyber threats as well as preventing them. Based on the combination of detection, response, and adaptive security measures to ensure defense against evolving attack vectors that might otherwise compromise the systems, cyber defense techniques protect critical systems from evolving attack vectors and reduce potential risks.

3.1. INTRUSION DETECTION SYSTEM

IDS is a subelement within the cybersecurity, monitoring network and system activities for suspicious behavior. Intrusion detection means obtaining information regarding unauthorized access, violations of system policy, or malicious activity that may put the integrity, confidentiality, or availability of the system in danger. IDS operates through network packets as well as system logs, which are patterns indicating that an attack or policy violation is underway or has already been set in motion [31, 32]. Contemporary IDS solutions offer immediate alerts to their administrators regarding the occurrence of an intrusion, meaning that response time and damage are being achieved in a rather shorter period [33]. There are several types of IDS based on the detection methodology adopted:

3.1.1. Signature-based Intrusion Detection Systems (SIDS)

SIDS rely on the comparison of network traffic with a pre-established database containing a set of known attack signatures. These work well on the detection of known attacks because they match a specific pattern, for instance, a byte sequence, packet headers, or known malware footprints. However, SIDS, by their nature, cannot identify new, zero-day attacks because they rely solely on signatures that yet do not exist for threats [32, 34]. For example, if malware has assumed a new version that adopts a payload structure that is not known to any signature, then the SIDS will miss it until there has been an update in the signature database [35].

3.1.2. Rule-based IDS

Also known as policy-based IDS, these systems identify intrusions by comparing and checking net- work activity against predefined rules. Such systems are very highly adaptable because an administrator can define specific behaviors that should be flagged. For example, a rule may mark traffic coming from a particular IP address or volumes of traffic over a certain threshold within a timeframe [36, 37]. Although rule-based IDS are flexible, they need continuous tuning and maintenance to stay effective, especially as network configurations change and various new attack techniques appear [33].

3.1.3. Anomaly-Based Intrusion Detection Systems (AIDS)

AIDS use an altogether different approach: instead of trying to match specific signatures or rules, it identifies deviations from the norm. In these systems, ML is employed to baseline normal network behavior and detect intrusions based on recognizing activities that significantly deviate from this baseline [31, 36]. The strength of AIDS is its ability to identify zero-day attacks, since it does not depend on a database of known signatures [38]. However, when there's a higher false positive rate, benign anomalies are often mislabeled as a threat [35, 37].

3.1.4. Hybrid Intrusion Detection Systems

The hybrid IDS takes the best from the signature-based and anomaly-based approaches. They try to of- fer better defense from threats for which signatures exist and anomaly detection for emerging unknown threats. Hybrid systems are very efficient in all high-traffic production environments where a significant number of known and emerging threats is expected in place - this could be the case for enterprises or critical infrastructure [39, 40].

3.1.5. Host-based vs. Network-based IDS

IDS can also be classified based on what environment they monitor. The host-based IDS (HIDS) keeps an eye on each device, focusing on system logs, file integrity, and user activity to discover the malicious behavior at host level. This is as opposed to the NIDS which monitors in real-time network traffic for signs of attacks anywhere in the network. NIDS is more appropriate to detect high-level attacks that contain DDoS attacks, while HIDS is more appropriate to detect malware or insider threats at the endpoint [32, 41].

3.2. ANOMALY DETECTION

Anomaly detection techniques are critical to identify that there is some kind of deviation from normal behavior in a network, which might be raising signals towards probable cyber threats. Traditional, old school, rule-based systems have matured into more complex forms, namely graph-based methods as well as unsuper- vised learning, especially in such environments as the Internet of Battlefield Things (IoBT), where adversarial attacks prevail [38, 42]. Machine learning models combined with adversarial training, therefore, promise to resist such attacks by dynamically updating according to changing threat landscapes [39, 42]. In addition, ensemble learning is a proven method to improve the performances of anomaly detection systems in terms of precision and resistance within adversarial environments [38, 39].

3.3. ML AND DEEP LEARNING

ML and deep learning also bring new innovations in cybersecurity, specially in multi-stage complex attacks detection. Recent advances in the field involve state-of-art techniques, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), which are useful in malware classification and network intrusion detection [43]. As they are able to recognize patterns in huge amounts of data, it can be used in actual time to detect advanced threats, including ransomware and insider attacks [43, 44]. Also, unsupervised learning methods, often used for anomaly detection with unlabeled data, thus make them handy for discovering unknown patterns of attacks [45].

3.4. THREAT RESPONSE TECHNIQUES

Other than detection, strong incident response skills are required that can rapidly respond in appropri- ate and timely manners to incidents. Responding to the threat relates to what may be done in order to contain, to mitigate or remediative losses with security breaches that eventually will minimize its impacts against an organization's operations and assets.

3.4.1. Security Information and Event Management (SIEM)

The SIEM systems collect, aggregate, and analyze varied sources of information such as firewalls and endpoint logs, and even network devices, in real time to detect security-related incidents. With the advancement of recent machine learning algorithm integration, SIEM solutions are more equipped to detect mature advanced threats with much fewer false positives. SIEM use in a critical infrastructure environment has proven to be very efficient in managing large and multi-layered security operations [46, 47].

3.4.2. Security Orchestration, Automation, and Response (SOAR)

Security operations are automated by SOAR to facilitate fast and effective incident response. The SOAR platforms interface with the SIEM systems and other tools for seamless threat response across the total infrastructure while ensuring standard processes in managing incidents [48, 49]. A new version of SOAR technology also offers automation through artificial intelligence for threat hunting and remediation work, thereby saving much manual effort for the security analyst. On top of that, SOAR provides advanced case management and incident analysis capabilities with minimal complexity in post-incident reviews and increases the overall security posture [48].

3.4.3. Endpoint Detection and Response

The EDR tool is concentrated on continuous monitoring and response at the endpoint level, as it provides deep insights into the behavior of the individual devices. EDR systems build on the strengths of behavioral analysis and ML algorithms, to identify APTs which would otherwise avoid detection by traditional antivirus solutions [50]. EDR also includes forensics and threat hunting capabilities that allow security teams the ability to unpack incidents in full detail and neutralize threats before they can spread throughout a network [50],[51].

4. CYBERSECURITY IN DIFFERENT DOMAINS

Cybersecurity in various domains demands specialized approaches to address distinct challenges unique to each environment.The following section highlights attack vectors and remediation techniques for different domains like cloud, mobile, iot, network security and the role of artificial intelligence in cybersecurity.

4.1. CLOUD SECURITY

Multi-tenant architectures present gigantic challenges in terms of cloud security due to vulnerabilities exploited by potential attacks, which may take advantage of shared resources and thus compromise the isolation between the tenants and perhaps data leakage [52]. Data privacy becomes challenging in cloud infrastructure because it is stored in distributed networks scattered all over, allowing for potential unauthorized access and some accidental breaches [53]. Furthermore, regulatory requirements such as tighter conditions like GDPR make cloud security more complex because the cloud service providers handle data storage in geographically remote locations which complicates issues of legal jurisdiction as well as data sovereignty [54]. The best cloud security solutions will balance protection for high levels of data integrity in conjunction with confidentiality but with performance optimizations. Encryption and other security measures heavily impact system efficiency so that large amounts of data often become too slow to process easily with security measures on [55]. Techniques such as homomorphic encryption have demonstrated promising early results in performing computations on encrypted data using secure protocols in a Cloud-based environment but are quite limited for commercial use due to the high computational costs that pervade the development of efficient scalable versions [56].

4.2. MOBILE SECURITY

The malicious phishing and malware attacks are highly targeted on mobile apps due to the wide permissions given to applications as well as third-party invoked libraries within an application, which may lead to leakage of private user information to malicious parties [57]. This has also given rise to new forms of risks, as the increased complexity of the infrastructures involved in 5G is vulnerable to attacks on the signaling plane and DDoS attacks, affecting layers of both application and network [58]. These threats require counter-measures from Mobile Device Management (MDM) solutions for organizations to monitor and control usage on devices. However, MDM systems themselves are also vulnerable to such advanced persistent threats (APTs) and mobile botnets that potentially bypass traditional detection mechanisms and breach enterprise security [59]. Recent works have come forward with blockchain-based MDM solutions as a promising advancement for securing mobile devices, proposing a decentralized manner of managing and securing communication channels, while persistent scalability challenges remain [60]. Adaptive security measures capable of real-time responses will be indispensable in protecting both networks and devices from evolved mobile threats [61].

4.3. IOT SECURITY

IoT security is a complex issue for the widespread deployment of these IoT gadgets in a variety of environments and the minimal adoption of general security standards that expose these devices to multiple attack vectors [62]. Most of the IoT devices are always constrained in their potential for computational and power capacity to provide traditional security protocols like intrusion detection systems and encryption in terms of feasibility [63]. Adding to this, the heterogeneity of IoT systems-ranging from industrial applications to consumer devices-made it even harder to implement uniform security standards. This made communication channels and privacy over data very vulnerable [64]. Moreover, the high volume of interconnecting IoT devices significantly expands the attack surface and leaves them open for large-scale attacks like DDoS and malware- based intrusions [65]. With regard to such security issues, lightweight encryption techniques and adaptive architectures are some researches being carried out to protect IoT networks with minimal resource usage over individual devices [66]. Despite this, persistent challenges persist, such as inconsistent implementation of authentication protocols and the difficulty in managing timely software updates that expose many potential IoT threats [67].

4.4. NETWORK SECURITY

Network security is under immense pressure because of the fast and continually advancing network architectures that require strong and adaptive protocols to defend against sophisticated attacks [68]. Sophisticated secure communication protocols have especially been advanced in 5G, and it is still found to be vulnerable towards attacks on control planes and signaling systems that disrupt critical network functions [69]. Real-time network monitoring is typically deployed using anomaly-based detection systems, which can be well-suited to catching suspicious activities but are not without the challenge of finding an appropriate balance between high detection rates and low false positives [70]. SDN promises to open up centralized security management capabilities that might otherwise be unmanageable but poses a risk in favoring single points of failure that at- tackers might enjoy exploiting [71]. Addressing such weaknesses of SDN, frameworks are now surfacing that automatically react to the threats once discovered for a more responsive defense to novel attacks [72]. However, managing extremely large software-defined networks is challenging, which is why research continues in secure and efficient protocols for when those demands are needed [73].

4.5. ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Artificial Intelligence (AI) has transformed the field of cybersecurity as it offers real-time response and detection capabilities with greater accuracy through advanced machine learning models [74]. In fact, these innovations are significant for using anomaly detection and predictive analytics in detecting zero-day vulnerabilities in a more proactive manner than traditional approaches to threat identification [75]. Neural networks have improved the reliability of IDS but these systems still face challenges like high false-positive rates and dependence on large data sets [76]. AI-based defenses are still vulnerable to attacks in the form of adversarial inputs that could mislead models into producing certain output, which would further create dangers to security [77]. To counter this, researchers are developing Explainable AI, or XAI, as an essential intervention to increase the transparency of decisions in AI, which may also reduce vulnerabilities to adversarial attacks [78]. Despite the above developments, integrating AI into cybersecurity still faces challenges with meeting the balance between security and efficiency when dealing with these very extensive and ever-increasing datasets that characterize modern networks [79].

5. CYBERSECURITY CHALLENGES

Cybersecurity is a dynamic field, and with newer advanced technologies and more profound attackers, security professionals face more challenges. The following section outlines some of the key challenges in cybersecurity including human factors and social engineering, privacy and ethical issues, and regulatory and legal challenges.

5.1. HUMAN FACTORS AND SOCIAL ENGINEERING

Human factor is the most significant challenge in cybersecurity. Humans often are the most vulnerable point in the security chain, as it is said, and attackers have exploited this more over time using social engineering. Social engineering attacks include phishing, baiting, and pretexting, where users are convinced to provide information or access to secure systems [101]. Phishing attacks are one of the most common forms of social engineering where attackers are taking advantage of users' trust in official-looking communications to steal credentials or spread malware [102]. Another very significant risk in the case of cybersecurity is insider threats. Insider threats refer to persons inside the organization that may misuse their access to adversely affect the organization on purpose, accidentally, or otherwise [80]. According to [80], insider threats are very difficult to detect because they emanate from trusted employees or contractors who already have legitimate access to the system. Insider incidents can result from malicious intent or negligence; in the latter case, the user unintentionally compromises sensitive information due to unawareness or unsafe practices [80, 101]. A poor understanding among users is one of the major human-related causes. In most cases, users do not know about the emerging threats, and there is not adequate education provided to identify or control potential dangers [103]. The organizations that do not spend their money on continuous security education for its employees are prone to being breached [80, 101].

5.2. PRIVACY AND ETHICAL ISSUES

Balancing security and user privacy is also another major challenge in cybersecurity. Although organizations institute more enhanced security measures like surveillance, logging, and monitoring, privacy issues begin to creep in [84]. For instance, organizations may collect vast amounts of user data for security purposes; however, sometimes this collection might infringe on the user privacy rights if mishandled [83]. For example, the GDPR in Europe demonstrates how privacy and data protection laws have evolved in this regard with a tendency to develop more user control and their information [6]. Nonetheless, enforcement of such regulations might likely prove challenging while adhering to robust security. According to research, integration of such privacy-enhancing technologies into security solutions must be achieved to establish a good balance between protection of users' information and compliance with regulations [83]. Ethical hacking, or penetration testing, is the practice that attempts to unveil vulnerabilities within systems before these malicious actors can access them [90]. Even though this process is necessary for strengthening security, ethical concerns emerge when considering the possible misuse of testing tools [91]. Ethical boundaries must restrain hackers in penetration testing roles so that their activities do not violate law or user privacy requirements [84]. Second, ethical hacking, if performed well, enables organizations to examine and analyze security vulnerabilities without breaking users' trust or neglecting the privacy of any individual, laws [84], [90].

5.3. REGULATORY AND LEGAL CHALLENGES

Yet another challenge in the domain of cybersecurity is a complexity in the legal and regulatory land- scape. Regulations involving GDPR in Europe and HIPAA in the U.S. put stringent standards of data protection on organizations to adhere to these standards [90, 93]. However, a borderless internet has made laws radically vary from country to country, thus creating a patchwork of regulations where multinational organizations need to navigate through a different kind of legislation in almost every country [87, 94]. The challenge for businesses would then be to reconcile the divergent demands of different regulatory bodies in frequently conflicting jurisdictions [88]. For example, some countries impose data localization policies that mandate the storage of data within country borders, but other countries require data to be accessible for international investigations [87, 94]. Hence, organizations would have to adopt flexible yet robust cybersecurity policies that cater to a wide range of legal standards [93-95]. Another issue, therefore, is the fact that cyber threats evolve in manners that no one can keep track of with the pace of cybersecurity legislation [93]. Even though regulators try to make sure their rule-making remains abreast of the latest in cybersecurity issues, the law is too slow and often plays catch-up in catching up with new emerging threats [94]. Indeed, there has been a stream of recommendations to implement more flexible legal systems that can rapidly respond to new cybersecurity advances [87, 93, 95].

6. FUTURE TRENDS IN CYBERSECURITY

Future cybersecurity has many challenges along with opportunities. This section identifies some ar- eas where we can expect potential impacts on the future landscape of cybersecurity in the age of quantum computing, 5G networks, AI-driven systems, and edge computing.

6.1 QUANTUM COMPUTING AND CYBERSECURITY

Quantum Computing threatens to undermine the underpinning of modern cryptography. Algorithms like RSA and ECC rely on issues that may be challenging to solve for computers, such as factoring large numbers. Quantum computers are able to answer those issues much more rapidly using Shor's algorithm [97, 99], breaking many widely-used encryption methods. Most of today's secure communications are thus at risk when large-scale quantum computers come along. Pre-emption of this is being done by post-quantum cryptog- raphy which is developing quantum-resistant encryption algorithms. Methods like lattice-based cryptography and multivariate polynomials are some of the promising solutions considered [98]. As these methods do not depend on mathematical problems which can readily be answered by a quantum computer, they cannot be used to perform quantum attacks on them. This has resulted in active development of cryptographic standards that withstand threats from quantum computing, as led by organizations like NIST [98]. Lastly, blockchain technology is also vulnerable to the threats of quantum computing. The fundamental foundation for securing a blockchain relies on cryptographic principles that quantum computers may breach, primarily at public key algorithms related to transaction verification [99]. Scientists are thus looking to develop post-quantum crypto- graphic algorithms to secure blockchain and distributed ledger systems to ensure that blockchain systems can still function securely into the quantum future [97].

6.2. 5G SECURITY CHALLENGES

Apart from being faster and more real-time, 5G networks pose new security challenges in communi- cation. Unlike previous generations, 5G systems are much more decentralized, based on virtualization, with their attack surface increased [92]. Due to decentralization, several attacks could occur on these 5G networks by targeting virtualized environments and SDN. Here the attacker exploits weak points in the control systems of the network [91, 92]. The most critical problem with the surge of IoT devices is the case with 5G. Amount of IoT gadgets which are expected to be using 5G networks is very high, yet these devices do not have inbuilt security protections. A hacker can attack the network through vulnerable devices, and such an attack will likely result in a DDoS [100]. This large number of connected devices, coupled with heterogeneous security stan- dards developed by manufacturers, means securing the network is a task that is quite complex [100]. Against this backdrop, security researchers are concentrating on developing enhanced encryption protocols, anomaly detection systems, and zero-trust architectures for securing 5G networks. Network slicing, one of the major features of 5G, will allow for personalized and customized virtual networks for each application, but a breach in one slice can have a ripple effect on others [91]. This means that continuous innovation in network security solutions is then required to fill these vulnerabilities, such as more advanced real-time monitoring systems and adaptive encryption techniques [92].

6.3. CYBERSECURITY IN AI-DRIVEN SYSTEMS

AI is being incorporated into the cybersecurity defenses more and more, from real-time threat de- tection to automated systems of response. However, AI systems may be prone to many exploits including adversarial inputs-subtle changes to input data can deceive AI models into making wrong predictions [89]. These have been demonstrated in many domains, such as both image detection, natural language processing, demonstrating that there is a high critical need for better defenses [89]. Another emerging concern is that AI is increasingly being adopted by cyber attackers to enhance their malicious capability. Attackers use AI automa- tion tools to build up automated phishing campaigns, to create more sophisticated malware types and even for retaliating against adaptive cybersecurity efforts [85]. In this ″arms race" between defenders and attackers in wits, each of them becomes increasingly smart at outpacing the other in this cyber battle of wits [85]. Because of this reality, ensuring AI systems is of extreme importance, especially since maliciously applied AI automa- tion can now be deployed to execute attacks [81]. Multi-level Approach towards the Integrity and Security of AI Models The strength of adversarial training techniques combined with secure deployment of models and encrypted datasets prevent tampering with AI models [75]. In addition, the data used in the training of AI systems needs to be carefully chosen in order not to fall victim to any bias or manipulation that would lead to compromised decision-making processes in important systems, such as medical care and vehicles 4. With continued pace of AI evolution, it would also be important that its security be ensured to continue the trust value in AI-related systems 8.

6.4. EDGE AND FOG COMPUTING SECURITY

Fog computing pushes the cloud closer to the network's edge, providing better mobility with low latency for the IoT devices; however, this shift of data introduces an important security challenge [103]. For example, there is a need to secure data as it moves from fog nodes to multiple nodes in the cloud [103]. Because of the geographical distribution of fog nodes, they will face physical and cyber attacks based on the isolated nodes with lesser degrees of protection [104]. Indeed, maintaining data confidentiality and integrity at the edge is critical in carrying out operations in a secure manner as resources are limited [105]. Heterogeneity of devices involved in a fog environment complicates the implementation of uniform security protocols, hence possible security gaps [104]. To address the issues identified, researchers have developed access control systems and mechanisms for resource management specifically designed for fog environments [103]. An adaptive resource management framework presented to improve the protection of the fog, with monitoring user behavior through issue risk-based access certificates [105]. It conducts trust evaluations in real-time such that assessment whether to allow or deny will be made instantaneously thereby reducing the latency of the process in the access control mechanism [105]. Lightweight encryption frameworks are also important to achieve data protection on scalable and flexible resource-constrained fog devices with growing demands [104]. Such solutions are significant for ensuring security without any trade-off in the performance of fog-based networks [103]. Besides the protection of data transfer, protecting the nodes at the fog itself is a priority because the fog nodes are very critical in a fog architecture [104]. The distributed nodes usually have very limited security oversight, making these nodes suitable for use by a cybercrook to deploy malicious applications and manipulate sensitive data [103]. To overcome this, advanced risk estimation and trust management models are developed to detect anomalies and prevent unauthorized access of the deployed fog services [105]. These models will allow the fog network to dynamically assess the threat level and undertake proactive measures toward protecting infrastructure [104]. With these security advancements, fog computing can provide the flexibility required for future IoT applications while ensuring robust security [105].

7. COMPARATIVE ANALYSIS OF EXISTING RESEARCH

AI and machine learning approaches have become increasingly important in cybersecurity research and the goal being improving both defensive and offensive capabilities. By automating threat detection and response processes, AI has the ability to provide real-time and adaptive solutions for a wide range of cyber threats.

7.1. CATEGORIZATION OF RESEARCH

Both offensive and defensive applications of AI draw attention to the various machine learning tech- niques for proactive threat modeling and intrusion detection [106]. Developing AI/ML models have a privacy focus which handle sophisticated cyberthreats and balance security with ethical considerations [107]. There are IoT-specific cyberthreats which exist. Machine learning approaches have the capacity to improve real-world security in IoT frameworks. [108]. Highlights of research on big data analytics applications in cybersecurity, specifically in identifying trends and patterns in massive datasets to reduce security breaches is another area of research [109].

7.2. CRITICAL ANALYSIS

Existing AI methods have shortcomings in responding to new cyberthreats, especially when it comes to managing changing attack strategies. There is an absence of frameworks which are capable of evolving with these threats. Additionally, limitations in dataset generalizability affect real-time application which reduces the effectiveness of AI in dynamic cybersecurity [110]. Offensive AI applications with short exploration focus on adversarial AI techniques and defense mechanisms while pointing out the gap in strategic policies for such attacks. [111]. Underlining ethical risks such as privacy invasion, human deskilling and AI-controlled cyber escalation is another major area of study. These topics highlight the need for comprehensive policies on AI's role in cybersecurity [112]. To provide a quick glance of comparative knowledge of cybersecurity issues across future technologies, Table 1 consolidates into a single view the challenges, implications, and directions of future research.

8. RECOMMENDATIONS FOR FUTURE RESEARCH

Future research should focus on developing adaptive AI models. These should be capable of evolving in response to emerging threats and shifting cyber landscapes. Interdisciplinary collaboration is necessary to address complex cybersecurity concerns, including domains such as ethics, law and data science.

8.1. EMERGING AREAS NEEDING ATTENTION

A thorough investigation into quantum-resistant algorithms is required. There is also a need to establish cybersecurity policies for dangers posed by quantum computing [107]. Ethical framework in cybersecurity is another area which needs attention. Issues such as privacy, autonomy and surveillance risks should be taken into account. Integrating ethical standards into AI model development in cybersecurity can help solve these issues [112].

Table 1. Quick overview of the future trends in Cybersecurity

Technology	Key Challenges	Security Implications	Emerging Solutions	Research Gaps
5G	Decentralized architecture, network slicing vulnerability	DDoS, signaling plane attacks, inter-slice leaks	Zero-trust architectures, secure network slicing	Standardization across slices, real-time anomaly detection
Quantum Computing	Ability to break RSA, ECC encryption	Cryptographic failure, data leakage	Post-quantum cryptography (e.g., lattice-based, code-based)	Scalability, migration to quantum-resistant protocols
AI in Security	Adversarial attacks, model poisoning	Misclassification, bypassing IDS/EDR	Explainable AI, adversarial training, federated learning	Real-world robustness, transparency, ethics integration
Edge Computing	Distributed trust, physical node exposure	Data interception, rogue edge nodes	Lightweight encryption, risk-aware access control	Standardized security frameworks for fog/edge nodes

8.2. IMPROVEMENT IN EXISTING STRATEGIES

Enhanced data processing methods for real-time threat detection within big data framework displayed the potential of robust data-driven analytics to identify and prevent complex attacks effectively [109]. There should also be advancements in DL and metaheuristic algorithms to improve response accuracy. Some models are also proposed which are capable of handling dynamic cyber threats and reducing false positives [110].

9. NOVELTY OF THE WORK

The paper presents a comprehensive consolidation of existing research in cybersecurity with a structured, cross-domain perspective that distinguishes it from generic surveys. The key novelty lies in the multi-layered comparative analysis of cybersecurity techniques across five critical domains: cloud, IoT, mobile, network, and AI-integrated systems. By organizing content not just thematically but also through tabular performance comparisons, the study offers accessible and evaluative insight into complex technical trends such as anomaly detection, EDR systems, SOAR platforms, and post-quantum cryptographic considerations. Moreover, the inclusion of emerging threat vectors like AI-driven cyberattacks, evolving ransomware tactics (e.g., double extortion), and 5G-induced vulnerabilities adds depth and relevance to the review, reflecting the shifting cybersecurity landscape. Unlike many generic reviews, this paper highlights defense-offense symmetry in AI usage, covering both adversarial inputs and defensive ML strategies, which is further contextualized through a categorization of research efforts (Section 7.1) and critical analysis of dataset generalizability (Section 7.2).

The survey also integrates regulatory, ethical, and human-factor dimensions, an often-overlooked aspect in purely technical reviews by synthesizing insights from cross-disciplinary studies (Table 4), thus presenting a more holistic view of cybersecurity challenges. The forward-looking research agenda (Section 8) not only outlines future trends like post-quantum cryptography and Explainable AI (XAI) but also advocates for adaptive and scalable cybersecurity solutions, filling gaps identified in current implementations. Overall, the novelty stems from the structured synthesis of current research, comparative tabulations with performance metrics, and cross-domain evaluation of threats and solutions, all while embedding future-forward and ethical dimensions within the cybersecurity discourse.

10. NOVELTY IN THE DOMAIN OF CYBERSECURITY

Cybersecurity is no longer confined to firewalls and antivirus software; it is rapidly transforming into a dynamic, intelligent, and deeply integrated defense ecosystem. As highlighted in this paper, the domain is undergoing a paradigm shift, driven by the infusion of cutting-edge technologies and the ever-evolving nature of threats.

At the forefront of this transformation is the adoption of Artificial Intelligence (AI) and Machine Learning (ML), which are revolutionizing threat detection and response. These technologies enable cybersecurity systems to go beyond static defenses, learning from network behavior to detect zero-day attacks, uncover anomalies, and even automate responses in real time. The field is also witnessing a new breed of AI-powered threats, where adversaries use machine learning to craft evasive malware and hyper-personalized phishing campaigns marking the rise of an AI-versus-AI security battlefield.

The novelty further extends to the emergence of post-quantum cryptography, as the threat of quantum computing looms over conventional encryption algorithms. This has sparked a race to develop quantum-resistant protocols that can withstand the computational power of future quantum systems, an innovation critical to safeguarding national infrastructure and sensitive data. Cybersecurity is also being redefined by its expansion into complex, heterogeneous environments like 5G, IoT, cloud, and edge computing. Each of these domains introduces novel challenges ranging from securing billions of low-power IoT devices to protecting decentralized fog nodes against tampering. As a result, there is a surge in lightweight cryptography, real-time threat intelligence, and decentralized defense strategies. Meanwhile, advanced platforms such as SOAR and EDR are reshaping security operations through automation, orchestration, and behavioral analytics offering rapid containment of threats that would otherwise evade traditional controls. These systems embody the shift toward intelligent, scalable, and responsive cybersecurity frameworks. Equally groundbreaking is the integration of ethical, legal, and human-centric dimensions into the cybersecurity conversation. The focus is shifting from purely technical safeguards to responsible AI, privacy-aware design, and resilience against insider threats ensuring that future solutions are not just powerful, but also accountable and trustworthy. The domain of cybersecurity is evolving from reactive defense into a proactive, predictive, and adaptive discipline ready to meet the challenges of a hyperconnected and increasingly intelligent digital world.

11.CONCLUSION

This landscape of cybersecurity requires robust, adaptable, and forward-thinking defense mechanisms. This research has thrown light on how modern cyber threats, from traditional malware to AI-enhanced attacks, pose new challenges across different sectors of IoT, cloud, and network security. These are the defensive technologies that would fight these threats: IDS, SIEM, SOAR, and even solutions based on machine learning. But all of these have their limitations, especially as the evasion techniques become more sophisticated in the hands of cybercriminals. The newest entrants into the technologies - quantum computing and 5G - open new avenues of vulnerability and thus a call for quantum-resistant encryption and advanced network protocols. Moreover, ethical considerations need to be incorporated into the development of AI for cybersecurity as its role continues to expand so that there is no misuse and it gains trustworthiness. The paper underlines the fact that cybersecurity requires continuous research and adaptation, with innovative, data-driven, and ethically grounded solutions. The future directions remain in the development of tailored AI models for threat detection, resilient cryptographic frameworks for the quantum era, and regulatory challenges to establish a secure digital environment for all users.

REFERENCES

[1] M. N. Al-Suqri, M. Gillani, “A comparative analysis of information and artificial intelligence toward national security”, IEEE Access, Vol. 10, 2022, pp. 64420-64434.

[2] H. James, M. Sabir, “AI-Driven Cybersecurity for Sustainable Healthcare Data: Protecting Patient Privacy and Environmental Impact”, 2024.

[3] L. Ayala, “Cybersecurity for hospitals and Healthcare Facilities, A Guide to Detection and Prevention”, Apress Berkeley, 2016.

[4] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, M. Xu, “A survey on machine learning techniques for cyber security in the last decade”, IEEE Access, Vol. 8, 2020, pp. 222310-222354.

[5] D. Schlette, M. Caselli, G. Pernul, “A comparative study on Cyber Threat Intelligence: The security incident response perspective”, IEEE Communications Surveys & Tutorials, Vol. 23, No. 4, 2021, pp. 2525-2556.

[6] M. Ahsan et al. “Cybersecurity threats and their mitigation approaches using Machine Learning—A Review”, Journal of Cybersecurity and Privacy, Vol. 2, No. 3, 2022, pp. 527-555.

[7] S. Zong, A. Ritter, G. Mueller, E. Wright, “Analyzing the perceived severity of cybersecurity threats reported on social media”, arXiv:1902.10680, 2019.

[8] US GAO - US Government Accountability Office, “Cybersecurity: Threats Impacting the Nation”, 2012, https://www.gao.gov/products/gao-12-666t (accessed: 2025)

[9] E. Tyugu, “Artificial intelligence in cyber defense”, Proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 2011, pp. 1-11.

[10] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, R. Ahmad”, Machine Learning and Deep Learning Approaches for CyberSecurity: A Review”, IEEE Access, Vol. 10, 2022, pp. 19572-19585.

[11] F. R. Alzaabi, A. Mehmood, “A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods”, IEEE Access, Vol. 12, 2024, pp. 30907-30927.

[12] Z. Zulkifl et al. “FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs”, IEEE Access, Vol. 10, 2022, pp. 15644-15656.

[13] B. Guembe et al. “The emerging threat of AI-Driven Cyber Attacks: A Review”, Applied Artificial Intelligence, Vol. 36, No. 1, 2022.

[14] R. Bace, P. Mell, “Intrusion Detection Systems”, NIST, https://www.nist.gov/publications/intrusion-detection-systems (accessed: 2024)

[15] A. Chidukwani, S. Zander, P. Koutsakis, “A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations”, IEEE Access, Vol. 10, 2022, pp. 85701-85719.

[16] O. Aslan, R. Samet, “A comprehensive review on malware detection approaches”, IEEE Access, Vol. 8, 2020, pp. 6249-6271.

[17] D.-O. Won, Y.-N. Jang, S.-W. Lee, “Plausmal-Gan: Plausible malware training based on generative adversarial networks for analogous zero-day malware detection”, IEEE Transactions on Emerging Topics in Computing, Vol. 11, No. 1, 2023, pp. 82-94.

[18] E. Gandotra, D. Bansal, S. Sofat, “Malware analysis and classification: A survey”, Journal of Information Security, Vol. 05, No. 02, 2014, pp. 56-64.

[19] I. Gulatas, H. H. Kilinc, A. H. Zaim, M. A. Aydin, “Malware Threat on Edge/Fog Computing Environments from Internet of Things Devices Perspective”, IEEE Access, Vol. 11, 2023, pp. 33584-33606.

[20] H. Abroshan, J. Devos, G. Poels, E. Laermans, “Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process”, IEEE Access, Vol. 9, 2021, pp. 44928-44949.

[21] F. Castano, E. F. Fernandez, R. Alaiz-Rodrıguez, E. Alegre, “PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification”, IEEE Access, Vol. 11, 2023, pp. 40779-40789.

[22] H. Abroshan, J. Devos, G. Poels, E. Laermans, “COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic”, IEEE Access, Vol. 9, 2021, pp. 121916-121929.

[23] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, M. A. Ibrahim, “Social Engineering Attacks Prevention: A Systematic Literature Review”, IEEE Access, Vol. 10, 2022, pp. 39325-39343.

[24] F. R. Alzaabi, A. Mehmood”, A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods”, IEEE Access, Vol. 12, 2024, pp. 30907-30927.

[25] P. Lavanya, H. Anila Glory, V. S. Shankar Sriram, “Mitigating insider threat: A Neural Network approach for enhanced security”, IEEE Access, Vol. 12, 2024, pp. 73752-73768.

[26] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, S. Karuppayah, “MQTT vulnerabilities, attack vectors and solutions in the internet of things (IoT)”, IETE Journal of Research, Vol. 69, No. 6, 2021, pp. 3368-3397.

[27] K. Fahad Ali, G. Li, A. N. Khan, Q. W. Khan, My. Hadjouni, H. Elmannai. ”AI-Driven CounterTerrorism: Enhancing Global Security Through Advanced Predictive Analytics.” IEEE Access, Vol. 11, 2023, pp. 135864-135879.

[28] N. Kaloudi, J. Li, “The AI-Based Cyber Threat Landscape”, ACM Computing Surveys, Vol. 53, No. 1, 2020, pp. 1-34.

[29] S. Sharma, R. Kumar, C. R. Krishna, “Ransom Analysis: The Evolution and Investigation of Android Ransomware”, Proceedings of the International Conference on IoT Inclusive Life, Chandigarh, India, 19-20 December 2019, pp. 33-41.

[30] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, V. Pospelova, “The Emerging Threat of Ai-driven Cyber Attacks: A Review”, Applied Artificial Intelligence, Vol. 36, No. 1, 2022, pp. 1-34.

[31] K. Ansam, I. Gondal, P. Vamplew, J. Kamruzzaman, “Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges”, Cybersecurity, Vol. 2, No. 20, 2019, pp. 1-22.

[32] A. H. Almutairi, N. T. Abdelmajeed, “Innovative signature-based intrusion detection system: Parallel processing and minimized database”, Proceedings of the International Conference on the Frontiers and Advances in Data Science, Xi'an, China, 23-25 October 2017, pp. 114-119.

[33] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches”, Transactions on Emerging Telecommunications Technologies, Vol. 32, No. 1, 2020, pp. 1-29.

[34] T. Saba, A. Rehman, T. Sadad, H. Kolivand, S. A. Bahaj, “Anomaly-based Intrusion Detection System for IoT Networks Through Deep Learning Model”, Computers and Electrical Engineering, Vol. 99, 2022, p. 107810.

[35] Ma lek, S. Zakiyabanu, B. Trivedi, A. Shah, “User behavior pattern-signature based intrusion detection”, Proceedings of the Fourth World Conference on Smart Trends in Systems, Security and Sustainability, London, UK, 27-28 July 2020, pp. 549-552.

[36] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, S. Venkatraman”, Deep Learning Approach for Intelligent Intrusion Detection System”, IEEE Access, Vol. 7, 2019, pp. 41525-41550.

[37] P. Ioulianou, V. Vassilakis, I. Moscholios, M. Logothetis, “A Signature-based Intrusion Detection System for the Internet of Things”, https://eprints.whiterose.ac.uk/133312/1/ictf2018IoT.pdf (accessed: 2025)

[38] D. A. Bierbrauer, A. Chang, W. Kritzer, N. D. Bastian, “Cybersecurity Anomaly Detection in Adversarial Environments”, arXiv:2105.06742, 2021.

[39] A. Yaseen, “The Role of Machine Learning in Network Anomaly Detection for Cybersecurity”, Sage Science Review of Applied Machine Learning, Vol. 6, No. 8, 2023, pp. 16-34.

[40] Q. Liu, V. Hagenmeyer, H. B. Keller, “A review of rule learning-based intrusion detection systems and their prospects in smart grids”, IEEE Access, Vol. 9, 2021, pp. 57542-57564.

[41] F. E. Ayo, S. O. Folorunso, A. A. Abayomi-Alli, A. O. Adekunle, J. B. Awotunde, “Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection”, Information Security Journal: A Global Perspective, Vol. 29, No. 6, 2020, pp. 267-283.

[42] M. Evangelou, N. M. Adams, “An anomaly detection framework for cyber-security data”, Computers & Security, Vol. 97, No. C, 2020.

[43] F. R. Alzaabi, A. Mehmood, “A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods”, IEEE Access Vol. 12, 2024, pp. 30907-30927.

[44] A. Nassar, M. Kamal, “Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies”, Journal of Artificial Intelligence and Machine Learning in Management, Vol. 5, No. 1, 2021, pp. 51-63.

[45] S. Yuan, X. Wu, "Deep Learning for Insider Threat Detection: Review, Challenges and Opportunities", Computers & Security, Vol. 104, 2021.

[46] G. G. Granadillo, S. G. Zarzosa, R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures", Sensors, Vol. 21, No. 14, 2021, pp. 1-28.

[47] M. A. Hussein, E. K. Hamza, "Secure Mechanism Applied to Big Data for IIoT by Using Security Event and Information Management System (SIEM)", International Journal of Intelligent Engineering and Systems, Vol. 15, No. 6, 2022, pp. 667-6681.

[48] U. Bartwal, S. Mukhopadhyay, R. Negi, S. Shukla. "Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots", Proceedings of the IEEE Conference on Dependable and Secure Computing, Edinburgh, Scotland, UK, 22-24 June 2022, pp. 1-8.

[49] J. Kinyua, L. Awuah, "AI/ML in Security Orchestration, Automation and Response: Future Research Directions", Intelligent Automation & Soft Computing, Vol. 28, No. 2, 2021, pp. 527-545.

[50] G. Karantzas, C. Patsakis, "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors", Journal of Cybersecurity and Privacy, Vol. 1, No. 3, 2021, pp. 387-421.

[51] W. U. Hassan, A. Bates, D. Marino, "Tactical Provenance Analysis for Endpoint Detection and Response Systems", Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 18-21 May 2020, pp. 1172-1189.

[52] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies", IEEE Access, Vol. 9, 2021, pp. 57792-57807.

[53] S. An, A. Leung, J. B. Hong, T. Eom, J. S. Park, "Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security", IEEE Access, Vol. 10, 2022, pp. 75117-75134.

[54] Q. Wang, Z. Wang, W. Wang, "Research on Secure Cloud Networking Plan Based on Industry-Specific Cloud Platform", IEEE Access, Vol. 11, 2023, pp. 51848-51860.

[55] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review", IEEE Access, Vol. 9, 2021, pp. 20717-20735.

[56] V. Chang, M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transactions on Services Computing, Vol. 9, No. 1, 2016, pp. 138-151.

[57] S. Mavoungou, G. Kaddoum, M. Taha, G. Matar, "Survey on Threats and Attacks on Mobile Networks", IEEE Access, Vol. 4, 2016, pp. 4543-4572.

[58] J. Cao et al. "A Survey on Security Aspects for 3GPP 5G Networks", IEEE Communications Surveys & Tutorials, Vol. 22, No. 1, 2020, pp. 170-195.

[59] I. Ahmad et al. "An Overview of the Security Landscape of Virtual Mobile Networks", IEEE Access, Vol. 9, 2021, pp. 169014-169030.

[60] R. Khellaf, S. Boudouda, "Enhancing Mobile Enterprise Security: A Blockchain and Agent Paradigm-Based Approach for Continuous Protection and Rapid Adaptation," IEEE Access, Vol. 12, 2024, pp. 108108-108120.

[61] M. Sajjad, A. Ahmad, A. W. Malik, A. B. Altamimi, I. Alseadoon, "Classification and Mapping of Adaptive Security for Mobile Computing," IEEE Transactions on Emerging Topics in Computing, Vol. 8, No. 3, 2020, pp. 814-832.

[62] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments", IEEE Access, Vol. 9, 2021, pp. 121975-121995.

[63] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security", IEEE Internet of Things Journal, Vol. 7, No. 10, 2020, pp. 10250-10276.

[64] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations", IEEE Communications Surveys & Tutorials, Vol. 21, No. 3, 2019, pp. 2702-2733.

[65] M. Adam, M. Hammoudeh, R. Alrawashdeh, B. Alsulaimy, “A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems”, IEEE Access, Vol. 12, 2024, pp. 57128-57149.

[66] M. Frustaci, P. Pace, G. Aloi, G. Fortino, “Evaluating Critical Security Issues of the IoT World: Present and Future Challenges”, IEEE Internet of Things Journal, Vol. 5, No. 4, 2018, pp. 2483-2495.

[67] W. Zhou, Y. Jia, A. Peng, Y. Zhang, P. Liu, “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved”, IEEE Internet of Things Journal, Vol. 6, No. 2, 2019, pp. 1606-1616.

[68] H. Wang, D. Zhao, X. Li, “Research on Network Security Situation Assessment and Forecasting Technology”, Journal of Web Engineering, Vol. 19, No. 7-8, 2020, pp. 1239-1266.

[69] V. P. Singh, M. P. Singh, S. Hegde, M. Gupta, “Security in 5G Network Slices: Concerns and Opportunities”, IEEE Access, Vol. 12, 2024, pp. 52727-52743.

[70] J.-Y. Yu, E. Lee, S.-R. Oh, Y.-D. Seo, Y.-G. Kim, “A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security”, IEEE Access, Vol. 8, 2020, pp. 45304-45324.

[71] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu, M. Liyanage, “A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions”, IEEE Communications Surveys & Tutorials, Vol. 26, No. 1, 2024, pp. 534-570.

[72] G. Arfaoui et al. “A Security Architecture for 5G Networks”, IEEE Access, Vol. 6, 2018, pp. 22466-22479.

[73] D. Fang, Y. Qian, R. Q. Hu, “Security for 5G Mobile Wireless Networks”, IEEE Access, Vol. 6, 2018, pp. 4850-4874.

[74] M. Gupta, C. Akiri, K. Aryal, E. Parker, L. Praharaj, “From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy”, IEEE Access, Vol. 11, 2023, pp. 80218-80245.

[75] L. Yee Por et al. “A Systematic Literature Review on AI-Based Methods and Challenges in Detecting Zero-Day Attacks”, IEEE Access, Vol. 12, 2024, pp. 144150-144163.

[76] R. Shevchuk, V. Martsenyuk, “Neural Networks Toward Cybersecurity: Domain Map Analysis of State-of-the-Art Challenges”, IEEE Access, Vol. 12, 2024, pp. 81265-81280.

[77] S. Zeadally, E. Adi, Z. Baig, I. A. Khan, “Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity”, IEEE Access, Vol. 8, 2020, pp. 23817-23837.

[78] N. Capuano, G. Fenza, V. Loia, C. Stanzione, “Explainable Artificial Intelligence in CyberSecurity: A Survey”, IEEE Access, Vol. 10, 2022, pp. 93575-93600.

[79] S. A. A. Bokhari, S. Myeong, “The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder’s Perspective”, IEEE Access, Vol. 11, 2023, pp. 69783-69797.

[80] J. Jeong, J. Mihelcic, G. Oliver, C. Rudolph, “Towards an Improved Understanding of Human Factors in Cybersecurity”, Proceedings of the IEEE 5th International Conference on Collaboration and Internet Computing, Los Angeles, CA, USA, 12-14 December 2019, pp. 338-345.

[81] S. Lee, S. Kim, “Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges”, IEEE Access, Vol. 10, 2022, pp. 2602-2618.

[82] M. A. Khatun, S. F. Memon, C. Eising, L. L. Dhirani, “Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation”, IEEE Access, Vol. 11, 2023, pp. 145869-145896.

[83] J. Pastor-Galindo, P. Nespoli, F. G. Marmol, G. M. Perez, “The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends”, IEEE Access, Vol. 8, 2020, pp. 10282-10304.

[84] T. Sauter, A. Treytl, “IoT-Enabled Sensors in Automation Systems and Their Security Challenges”, IEEE Sensors Letters, Vol. 7, No. 12, 2023, pp. 1-4.

[85] M. Aljabri et al. “Detecting Malicious URLs Using Machine Learning Techniques: Review and Research Directions”, IEEE Access, Vol. 10, 2022, pp. 121395-121417.

[86] R. Shevchuk, V. Martsenyuk, “Neural Networks Toward Cybersecurity: Domain Map Analysis of State-of-the-Art Challenges”, IEEE Access, Vol. 12, 2024, pp. 81265-81280.

[87] A. Khurshid, R. Alsaaidi, M. Aslam, S. Raza, “EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme”, IEEE Access, Vol. 10, 2022, pp. 129932-129948.

[88] A. Sundararajan, T. Khan, A. Moghadasi, A. I. Sarwat”, Survey on Synchrophasor Data Quality and Cybersecurity Challenges, And Evaluation of Their Interdependencies”, Journal of Modern Power Systems and Clean Energy, Vol. 7, No. 3, 2019, pp. 449-467.

[89] M. Gupta, C. Akiri, K. Aryal, E. Parker, L. Praharaj, “From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy”, IEEE Access, Vol. 11, 2023, pp. 80218-80245.

[90] A. W. Khan, S. Zaib, F. Khan, I. Tarimer, J. T. Seo, J. Shin, “Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach”, IEEE Access, Vol. 10, 2022, pp. 65044-65054.

[91] A. Dutta, E. Hammad, “5G Security Challenges and Opportunities: A System Approach”, Proceedings of the IEEE 3rd 5G World Forum, Bangalore, India, 10-12 September 2020, pp. 109-114.

[92] L. Shi, “Analysis of the Security of 5G Technology from the Network Level”, SHS Web of Conferences, Vol. 144, 2022.

[93] P. G. Chiara, “The Cyber Resilience Act: the EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements”, International Cybersecurity Law Review, Vol. 3, 2022, pp. 255-272.

[94] A. Joshi, “Study of Cybersecurity Laws and Regulations”, Indian Journal of Law, Vol. 2, No. 3, 2024, pp. 7-14.

[95] R. Ducato, "Data protection, scientific research, and the role of information," Computer Law & Security Review, Vol. 37, 2020, p. 105412.

[96] S. Patil, A. Jangra, M. Bhale, A. Raina, P. Kulkarni, “Ethical hacking: The need for cyber security”, Proceedings of the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, Chennai, India, 21-22 September 2017, pp. 1602-1606.

[97] M. Njorbuenwu, B. Swar, P. Zavarsky, “A Survey on the Impacts of Quantum Computers on Information Security”, Proceedings of the 2nd International Conference on Data Intelligence and Security, South Padre Island, TX, USA, 28-30 June 2019, pp. 212-218.

[98] K. Roy, “Quantum Computing and its Impact on Cryptography”, https://www.idsa.in/backgrounder/quantum-computing-and-its-impact-on-cryptographykroy190717 (accessed: 2025)

[99] H. Yalcin, T. Daim M. M. Moughari, A. Mermoud, “Supercomputers and quantum computing on the axis of cyber security”, Technology in Society, Vol. 77, 2024, p. 102556.

[100] G. Sahu, S. S. Pawar, “Security Challenges in 5G Network”, Software Defined Networking for Ad Hoc Networks, Springer, 2022, pp. 75-94.

[101] K. Chetioui, B. Bah, A. O. Alami, A. Bahnasse, “Overview of Social Engineering Attacks on Social Networks”, Procedia Computer Science, Vol. 198, 2022, pp. 656-661.

[102] J. Hunker, C. W. Probst, “Insiders and insider threats an overview of definitions and mitigation techniques”, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 2, No. 1, 2011, pp. 4-27.

[103] S. Parikh, D. Dave, R. Patel, N. Doshi, “Security and Privacy Issues in Cloud, Fog and Edge Computing”, Procedia Computer Science, Vol. 160, 2019, pp. 734-739.

[104] R. Rezapour, P. Asghari, H. H. S. Javadi, S. Ghanbari, “Security in fog computing: A systematic review on issues, challenges and solutions”, Computer Science Review, Vol. 41, 2021.

[105] W. B. Daoud, S. Othmen, M. Hamdi, R. Khdhir, H. Hamam, “Fog computing network security based on resources management”, EURASIP Journal on Wireless Communications and Networking, Vol. 50, 2023.

[106] I. D. Aiyanyo, H. Samuel, H. Lim, “A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning”, Applied Sciences, Vol. 10, No. 17, 2020.

[107] M. Roshanaei, M. R. Khan, N. N. Sylvester, “Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions”, Jour-

nal of Information Security, Vol. 15, No. 3, 2024, pp. 320-339.

[108] T. S. AlSalem, M. A. Almaiah, A. Lutfi, "Cybersecurity Risk Analysis in the IoT: A Systematic Review", Electronics, Vol. 12, No. 18, 2023.

[109] D. B. Rawat, R. Doku, M. Garuba, "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security", IEEE Transactions on Services Computing, Vol. 14, No. 6, 2021, pp. 2055-2072.

[110] A. H. Salem, S. M. Azzam, O. E. Emam, A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques", Journal of Big Data, Vol. 11, 2024, p. 105.

[111] M. Malatji, A. Tolah, "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI", AI and Ethics, Vol. 5, 2025, pp. 883-910.

[112] M. Taddeo, "Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity", Minds and Machines, Vol. 29, No. 2, 2019, pp. 187-191.