Global Trends in Science and Technology

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

Emerging Trends in Information Technology and Cybersecurity: A Comprehensive Review

Muhammad Talal Qaisar[1*], Syed Muhammad Aale Muhammad[2]

[1, 2] Washington University of Science and Technology, Alexandria, Virginia

[1]mqaisar.student@wust.edu, [2]aamuhammad.student@wust.edu

open access

Corresponding Author
Muhammad Talal Qaisar
mqaisar.student@wust.edu

Article History:
Submitted: 07-08-2026
Accepted: 11-09-2026
Published: 16-09-2026

Keywords

Artificial Intelligence, Cybersecurity, Cloud Computing, Block chain, Machine Learning, Information Technology.

ABSTRACT

Digital systems have undergone a dramatic change thanks to the fast pace of evolution of Information Technology (IT) and are currently facing new challenges in terms of cybersecurity. This review covers some of the emerging trends in IT and cyber security including AI/ML, Cloud and Edge Computing, Internet of Things (IoT), Zero Trust Architecture, Block chain, Quantum Computing and Advanced Cyber Threats. The study points to the potential of these technologies to be used to facilitate automation, connectivity, efficiency and enhanced security. It also addresses the threats of ransom ware, data breaches, privacy intrusion, advanced cyber-attacks and vulnerabilities in connected systems. Last, future research avenues focusing on secure innovation, proactive defense, privacy, resilience and post-quantum security are discussed.

INTRODUCTION

Information Technology (IT) and cyber security are integral parts of today's society and impact virtually every aspect of personal, organizational, industrial and governmental activity. Digital technologies have dramatically changed traditional systems into "digital environments" that enable information to be generated, processed, stored and shared, at unprecedented speeds [1]. The IT landscape is constantly evolving with the emergence of technologies like cloud computing, artificial intelligence (AI), machine learning (ML), Internet of Things (IoT), block chain, edge computing, and big data analytics. These technologies offer great promise for enhancing efficiency, automation, communications, and decision-making, but also pose fresh security risks and challenges. In this way, cybersecurity has turned into a strategic issue for companies and countries [2].

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

As people have grown increasingly reliant on digital infrastructure, so too have cyber threats. The methods used by cybercriminals to exploit information systems are growing increasingly complex, with ransomware, phishing, malware, social engineering, identity theft, distributed denial-of-service (DDoS) attacks and advanced persistent threats (APTs) playing an important role [3]. The proliferation of remote working, Cloud based applications, mobile devices and connected IoT systems has added to the attack surface that could be exploited by attackers. Further, the application of AI by attackers has opened up novel avenues for automated and highly targeted attacks, with traditional security strategies proving ineffective in certain scenarios [4].

New trends in IT are then closely related to new developments in cyber security. To enhance their security posture, organizations are turning to technologies like Zero Trust Architecture, security automation, behavioral analytics, threat intelligence, and AI-powered detection systems. Meanwhile, new technologies like quantum computing can present opportunities and new threats, especially to existing methods of encryption [5]. As IT becomes increasingly innovative, cybersecurity must also evolve, necessitating ongoing research, investment, and adaptation to ensure the protection of data confidentiality, integrity, and availability.

This review article investigates key trends in the field of information technology and cybersecurity that are currently emerging and assesses their implications on individuals, organizations, and society. It emphasizes the connection between technological progress and the changing nature of cyber threats and security methods, and also introduces new research directions. This study examines the latest advancements in AI and ML, cloud and edge computing, IoT, Zero Trust, block chain, quantum computing, and other advanced cyber threats, giving a broader view of the changing IT and cybersecurity landscape. Overall, the review highlights the critical role of proactive security measures, ongoing innovation, cybersecurity practitioners, and robust policies in creating resilient digital ecosystems.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN INFORMATION TECHNOLOGY AND CYBER SECURITY

Artificial Intelligence (AI) and Machine Learning (ML) are among the two most impactful technologies of the era that will define the future of Information Technology (IT) and cybersecurity. AI is the design of systems that can do things that typically need human intelligence: think, decide, understand languages, and solve problems [6]. One of the most significant areas of AI—Machine Learning—allows computer systems to identify patterns in data and enhance their capabilities through learning without being specifically programmed for each task. AI and ML are becoming increasingly significant tools in the realm of cybersecurity, playing a crucial role in complex IT environments and

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

solving today's security challenges [7].

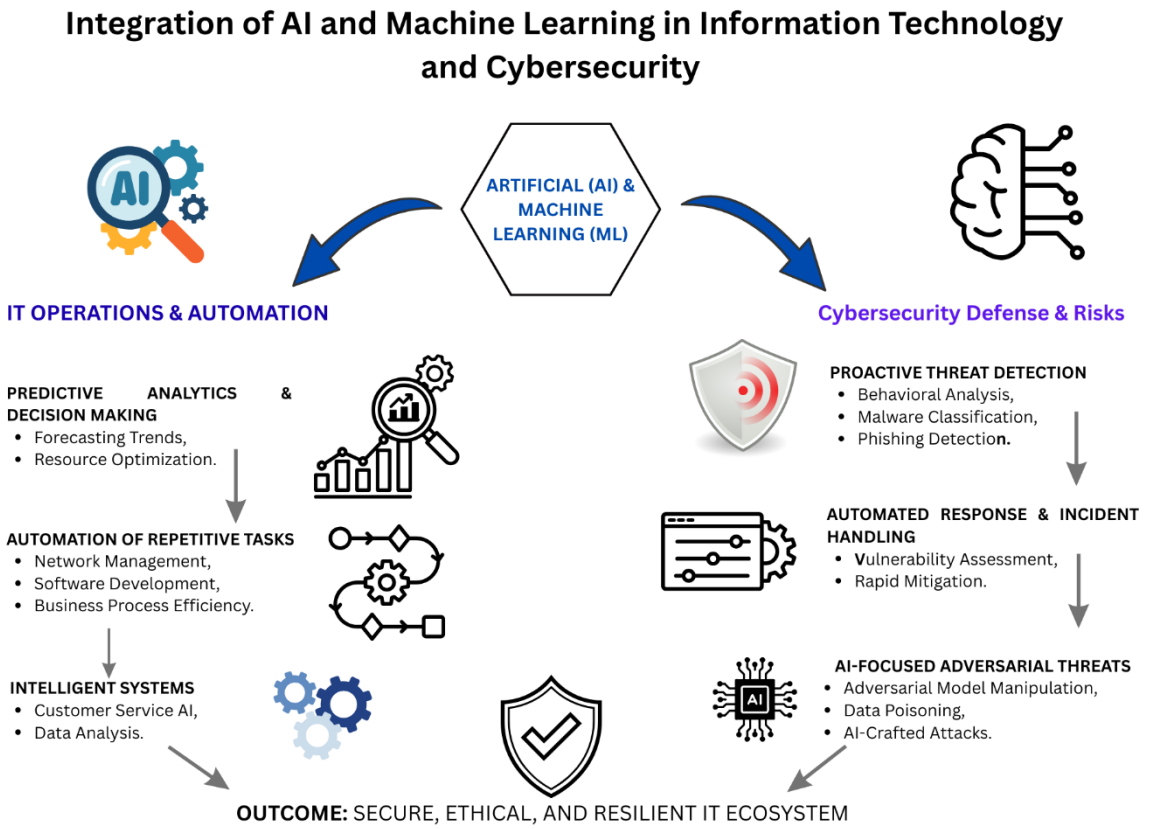

Figure 1. Integration of AI and Machine Learning in Information Technology and Cybersecurity

In the field of Information Technology, AI and ML are being used to automate repetitive tasks, improve system performance, analyze massive amounts of data, and aid in intelligent decision-making. AI-driven systems are utilized in customer service, predictive analytics, recommendation systems, network management, software development, and business intelligence for organizations [8]. By analyzing past trends and patterns, ML algorithms can forecast future trends, enabling organizations to make informed decisions. Moreover, AI-driven automation can decrease man hours and improve business efficiency by automating repetitive and time-consuming tasks [9].

AI and ML offer a range of robust tools in cybersecurity to detect and respond to threats. Traditional security systems are often based on known patterns and signatures, and are not able to identify new or evolving attacks [10]. ML-based security systems can, on the other hand, por through huge information about network traffic, user behavior, system logs, and more to discover unusual patterns. For instance, behavioral analysis can identify unusual access patterns, data transfers or login attempts, which could signify a security breach. Automated threat detection, malware classification, phishing detection, vulnerability assessment, and incident response are other areas where AI can be helpful [11].

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

But the adoption of AI also brings novel cybersecurity challenges. AI can be used to craft more convincing phishing emails, enable automated attacks, develop malicious code, and uncover vulnerabilities more effectively – and this is where cybercriminals come in [12]. Another category of adversarial attacks is targeting the AI systems themselves, via data poisoning, adversarial model manipulation, and unauthorized access. As a result, it is essential that AI technologies are created and utilized in a secure, private, transparent, and ethical manner [13].

AI and ML are reshaping the landscape of cybersecurity by shifting the focus from being reactive to proactive and predictive. They can handle vast quantities of information and identify intricate patterns, making them valuable assets in today's security operations. The integration of AI into security monitoring, automated response, and risk management is likely to see further enhancements in the future [14]. However, ongoing research and appropriate implementation are crucial to ensure the advantages of AI and ML do not outpace the risks of misuses and the vulnerabilities.

CLOUD COMPUTING, EDGE COMPUTING, AND CLOUD SECURITY

Cloud Computing and Edge Computing are two primary trends in the contemporary world of Information Technology and are reshaping the methods and approaches by which digital resources are stored, processed and accessed by organizations. Cloud computing is a way to access computing technology like servers, storage, databases, and applications and networking services on the Internet, on-demand [15]. Organizations can leverage cloud platforms to scale resources as per the business requirements, instead of maintaining extensive physical infrastructure. This approach has a number of benefits, such as cost savings on infrastructure, flexibility in resource allocation, ease of access, quick deployment, and remote working capabilities [16]. Cloud computing is thus now an integral part of the digital transformation.

Cloud services can be broken down into Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models enable businesses to choose computing resources based on their business needs [17]. Furthermore, there are varying degrees of control, scalability, and security for the different types of cloud environments - public, private, and hybrid. But, as the use of cloud services has grown, so too has cybersecurity issues. Sensitive organizational data can be exposed to unauthorized access, data breaches, insider threats, and weak authentication, insecure application interfaces, misconfigured cloud storage, and inadequate access controls [18]. So, the most important aspects of cloud security include robust IAM, encryption, MFA, constant monitoring, secure configuration and periodic vulnerability checks [19].

Edge computing is an addition to cloud computing that brings processing and analytics nearer to the sources of data. Edge devices can process some data at local computing nodes or locally, rather than

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

sending all information to centralized cloud data centers or centers with the computing power [20]. This solution can be used in applications that demand low latency and quick decision making, such as autonomous systems, smart cities, industrial automation, healthcare monitoring, and IoT environments [21]. While edge computing can cut network congestion and enhance response times, it can also lead to new security challenges since computing power might be spread throughout various devices and locations [22].

SECURING THE INTERNET OF THINGS: A COMPREHENSIVE REVIEW OF APPLICATIONS, VULNERABILITIES, AND DEFENSE MECHANISMS

The Internet of Things (IoT) is an emerging technology in IT which aims to put physical devices into the internet and enable them to collect, share and work with data. Examples of the devices include smart home appliances, wearable devices, industrial sensors, medical equipment, surveillance, smart vehicles, and environmental monitoring devices [23]. They can communicate with one another and with centralized platforms or cloud servers, allowing organizations and individuals to gain a comprehensive view of their systems and execute tasks more efficiently. With the proliferation of IoT, automation, intelligent decision making and real-time data analysis opportunities have emerged in numerous industries [24].

In the industrial setting, IoT technologies are being used more and more to monitor machines, control production processes, predict machine failures, and optimize operations. Connected medical devices can be used in healthcare to assist in patient monitoring and to provide real-time data to healthcare professionals [25]. Smart cities rely on a network of sensors to monitor traffic, energy, waste, public transportation and the environment. Likewise, smart homes are home to devices that can control household appliances, lighting, security systems and heating [26]. The applications highlighted here showcase the vast possibilities of IoT in enhancing convenience, productivity, and resource management [27].

But the proliferation of connected devices has created significant cybersecurity problems. There are also constraints on the computing power, memory and energy of many IoT devices, making it challenging to implement more complex security mechanisms [28]. Weak passwords, communications protocols that are not secure, outdated software, or under-designed authentication processes are also used by some devices [29]. Once the attacker has compromised an IoT device, it could be exploited to gain access to other devices, to steal valuable data, to disrupt services, or even to be part of a larger network of devices compromised by the attacker [30].

Global Trends in Science and Technology

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

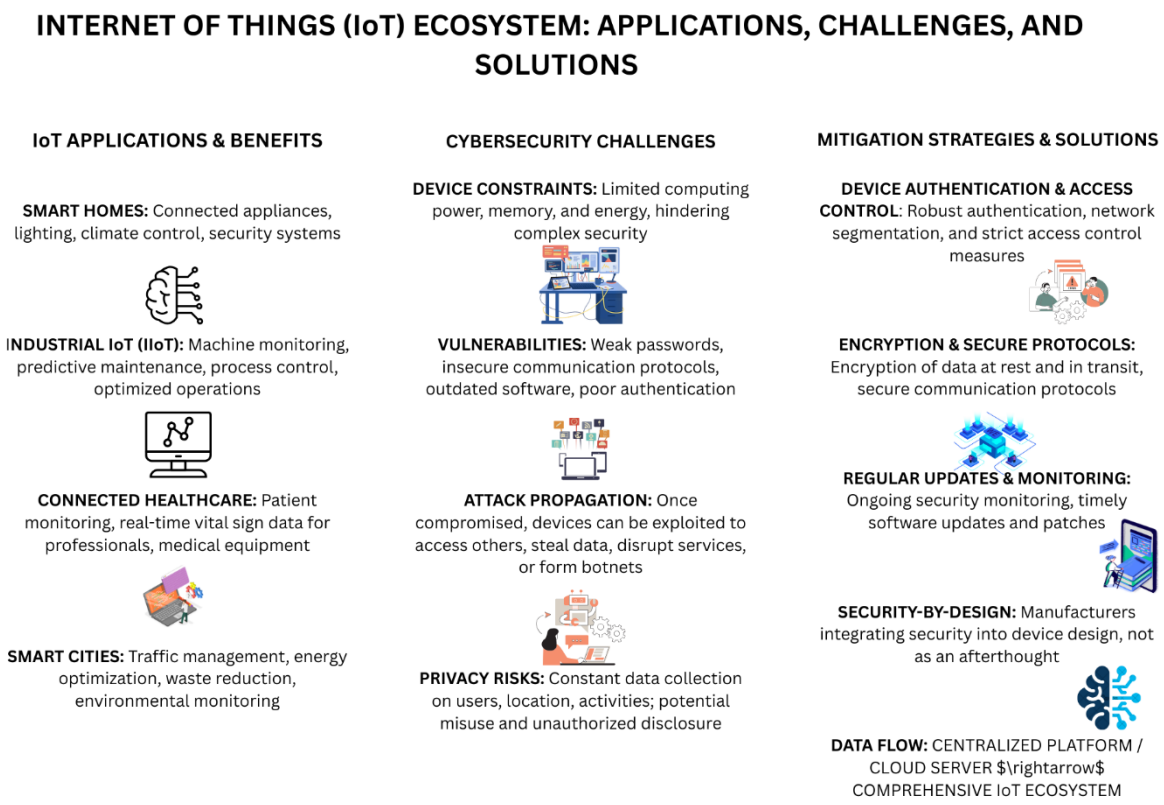

Figure 2. Internet of Things Ecosystem: Applications, Challenges, and Solutions

Another significant challenge related to the IoT is privacy. Tons of information is gathered from connected devices constantly about users, location, activities, and environments. Misuse of this information could result in its disclosure to unauthorized parties or entities [31]. Moreover, the devices used for IoT devices are typically located in sensitive areas such as homes, hospitals, factories, etc., and a successful attack may lead to more than just loss of information being the result. For instance, if there is a compromise in industrial or healthcare devices, it may impact physical processes and affect human safety [32].

Organizations can face these challenges by adopting robust device authentication, encryption, secure communication protocols, regular software updates, network segmentation, access control measures, and ongoing security monitoring [33]. Additionally, manufacturers must take a security-by-design approach to ensure that cybersecurity becomes part of the device design rather than an afterthought [34].

ZERO TRUST ARCHITECTURE AND MODERN CYBERSECURITY FRAMEWORKS

In today's digital landscape, Zero Trust Architecture (ZTA) has become a crucial cybersecurity strategy due to the complexity of digital environments. Because traditional security models are based on the concept that users and devices inside an organization's network can be trusted and that external users are untrusted [35]. But as cloud computing, remote work, mobile devices, Internet of Things

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

(IoT) devices and distributed networks continue to grow, the old perimeter-based approach is not as effective. With Zero Trust, the principle “never trust, always verify” applies to solve this issue [36]. With this one, there's no default trust placed on any user, device, application or network connection, whether it's within the organization's network or not.

Continuous verification is a key tenet of Zero Trust. Organizations require users to be identified and devices be secure before they are able to access their resources. Authentication can be through passwords, multi-factor authentication, biometrics, security tokens or any other means of identity verification [37]. Then access is granted based on the user's role, device conditions, place, etc. and depending on the security considerations. Importantly, access rights are typically restricted to just the resources needed to complete a particular task [38]. This is called "least-privilege access" and helps minimize the affect of compromised accounts.

Continuous monitoring and analysis is also a key aspect of Zero Trust. The activities of users, their network connections, their applications and devices can be tracked to detect suspicious activity. Artificial Intelligence (AI), machine learning, security analytics, and threat intelligence can be used by security teams to identify abnormal behavior and react to threats [39]. In cases of an authenticated user suddenly trying to access sensitive data from an unknown location or device, for instance, the system could call for further verification or deny access to the data. It allows organizations to get a head start on threats and minimize the chances of unauthorized access [40].

Modern cybersecurity frameworks are essential to complement Zero Trust and offer structured methods of handling cybersecurity threats. The NIST Cybersecurity Framework (CSF) is a framework that can be used to identify, protect, detect, respond, and recover from cybersecurity incidents. Other security frameworks and standards can be used as guidance for risk assessment; identity management, data protection, incident response, and organizational governance [41]. The frameworks are especially useful since cyber security extends beyond technology to policies, procedures, employee awareness, risk management, and organizational planning.

Despite its benefits, implementing Zero Trust can be challenging. Organizations might need to upgrade old systems, combine a number of security technologies, maintain complicated access policies, and educate staff. Implementation may also take a lot of money and technological support. However, Zero Trust is a flexible security model that is appropriate for the digital world today [42]. Zero Trust Architecture is a departure from perimeter-centric security to identity-driven and constantly monitored security [43]. It can be used with existing cybersecurity standards to enhance organizational cyber resilience, minimize unauthorized access, and better manage the detection and response to escalating cyber threats.

Global Trends in Science and Technology
ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

BLOCKCHAIN, QUANTUM COMPUTING, AND NEXT-GENERATION TECHNOLOGIES

The emerging technologies that could have a huge impact on Information Technology (IT) and cybersecurity include block chain and quantum computing. They, while solving technological issues of different nature, are gaining more and more attention due to their possible use in the field of secure communication, data management, authentication, financial systems, and advanced computing [44]. The emergence of these technologies brings with them opportunities and challenges which organizations and cyber security practitioners need to grasp.

Block chain technology is a decentralized digital ledger that keeps track of transactions on a network of computers. Unlike the centralized system, block chain is a decentralized system, and transactions are processed and registered according to agreed mechanisms. The integrity of the information is protected by cryptographic methods and the linked structure of records makes it hard to alter them [45]. These attributes have enabled block chain to be leveraged in various domains, including digital currencies, supply-chain management, healthcare records, identity management, smart contracts, and secure data sharing. Block chain technologies and their application in cybersecurity are a promising way to enhance data integrity, authentication, transparency, and auditability [46]. For instance, decentralized identity systems can diminish reliance on centralized databases, which can be appealing targets for cybercriminals.

But, block chain isn't entirely secure. Block chain systems can be vulnerable to various factors such as smart contract vulnerabilities, implementation flaws, compromised private keys, and specific consensus-related attacks. Thus, robust development, efficient key management and ongoing auditing is crucial to trustworthy block chain applications [47]. Another technological development is quantum computing. Conventional computers process information in classical bits, but certain kinds of computation can be performed in fundamentally different ways with quantum bits, or qubits, in quantum computers [48].

While quantum computing (QC) on a large scale and capable of fault tolerance is still in the early stages of development, future quantum systems may be significant in the area of cyber security. In particular, sufficiently strong quantum computers could break some popular public-key cryptographic routines, by reducing the complexity of some mathematical problems [49]. As a result, there is an urgent need for organizations to plan for the shift towards post-quantum crypto, which involves finding cryptographic algorithms that are efficient enough to resist attacks by both classical and quantum computers [50].

Meanwhile, quantum technologies could offer even more possibilities for secure communication and

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

sophisticated computational functions. One of the areas of active research is quantum key distribution, which seeks ways to use the characteristics of quantum objects to create the keys that would establish a secure encryption system and detect certain forms of eavesdropping [51].

EMERGING CYBER THREATS, RANSOMWARE, AND ADVANCED ATTACK TECHNIQUES

As digital technologies have progressed, they've brought massive enhancements to communication, business processes and information handling. The rise in the use of digital systems, however, has also resulted in new opportunities for cybercriminals. New types of cyber threats are becoming more sophisticated, automated, and targeted and insidious [52]. Organizations need to constantly enhance their cybersecurity strategies to safeguard sensitive data, critical infrastructure, money, and digital services. Ransom ware, phishing, malware, social engineering, advanced persistent threats (APTs), supply-chain attacks, and attacks with the aid of artificial intelligence (AI) are emerging threats [53]. Ransom ware is among the most severe cybersecurity risks impacting organizations and people. During a typical ransom ware attack, malicious software is used to disrupt access to a user's files or systems, typically by encrypting the data. Attackers then ask for a ransom to restore access or to not release stolen information. Ransom ware attacks nowadays might implement a double extortion strategy: the attacker encrypts data and also threatens to leak sensitive information [54]. Hospitals, schools, government agencies, businesses and critical infrastructure can be especially appealing targets because the loss of their services can cause a financial and/or operational burden.

Phishing and social engineering are also a serious threat to security. Impersonation via email, text messages, or fake websites may be used to trick customers into disclosing passwords, credit card numbers, authentication codes, and other sensitive information [55]. Phishing attacks can be very sophisticated, using information that is available on the internet to make them appear very realistic. As AI becomes more prevalent, the quality of these fraudulent messages could further decrease the ability of users to tell the difference between legitimate messages and fraudulent ones [56].

The Advanced Persistent Threat (APT) is another significant threat. APT attacks are characterized by attackers' successful access to the target environment and holding on to it for an extended period of time. These attacks can target research institutions, government agencies, financial institutions and large corporations. Over time, attackers can work their way through networks, acquire sensitive data and try to evade detection [57]. Supply-chain attacks are also an emerging issue in cybersecurity. Rather than targeting a large organization, attackers can infiltrate a software vendor, service vendor, third party application or hardware component of an organization targeted. A successful compromise then has the potential to impact numerous organizations [58].

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

As AI becomes more prevalent, it also introduces new challenges and opportunities for cybersecurity. AI can be leveraged by attackers to automate vulnerability detection, create malicious content, enhance social engineering attacks, and more; defenders can use AI to detect anomalies, conduct threat intelligence, automate incident response, and analyze malware [59]. As a result, the tactics of cybersecurity professionals must continually evolve.

Protecting against emerging threats demands a multi-layered defense strategy that includes robust authentication, timely software updates, employee training, network segmentation, endpoint protection, secure backups, encryption, continuous monitoring and incident response planning. It is also important for organizations to periodically perform risk analyses and provide security awareness training [60]. In an era where cyber threats are constantly evolving, proactive risk management and timely detection will play a crucial role in ensuring secure and resilient cyber environments.

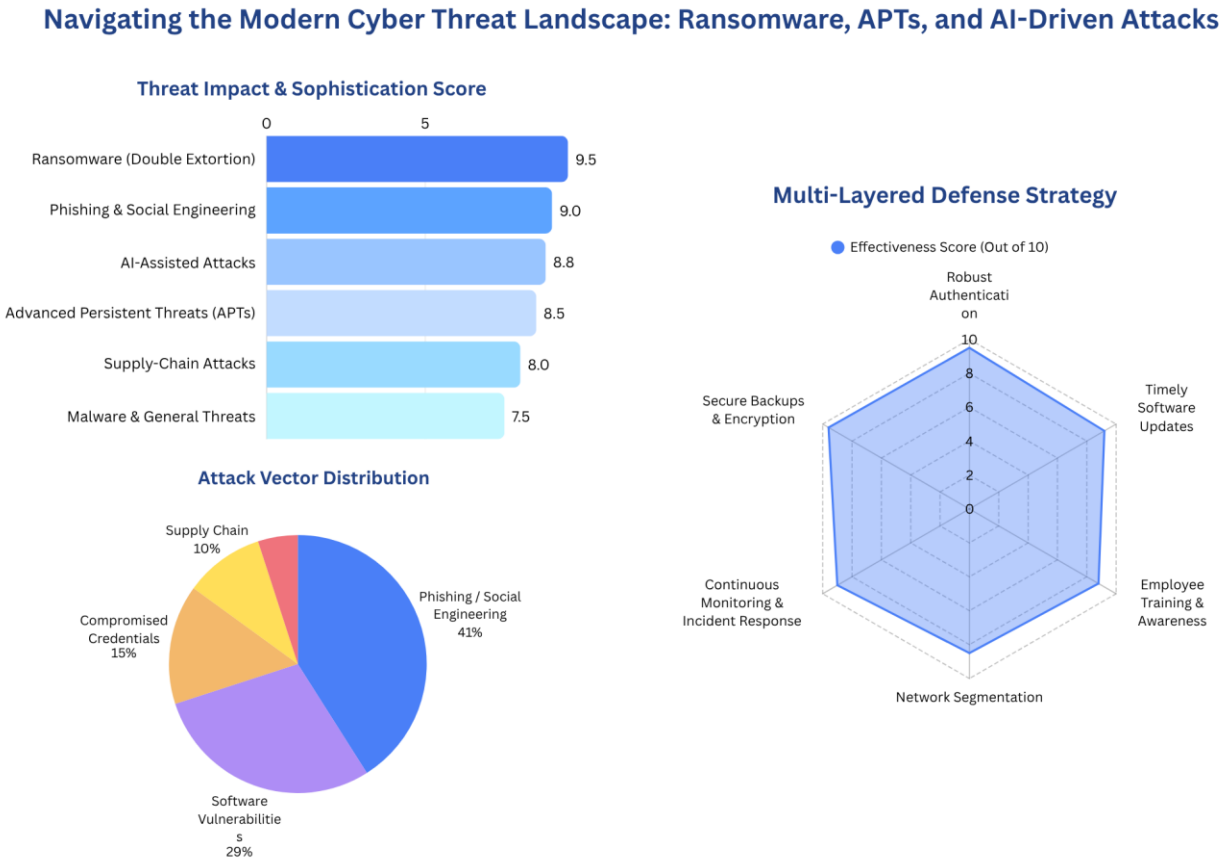

Figure 3. Navigating the Modern Cyber Threat Landscape: Ransomware, APTs, and AI-Driven Attacks

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

FUTURE DIRECTIONS AND FUTURE RESEARCH CHALLENGES

Technological advancements and digitization are likely to drive key trends in the future of Information Technology (IT) and cybersecurity, alongside the ongoing advancement of cyber threats. New technologies like Artificial Intelligence (AI), Machine Learning (ML), Quantum Computing, Cloud Computing, Edge Computing, Block chain and Internet of Things (IoT) will present new opportunities to organizations and new problems in security [61]. As such, future research needs should include more than just the advancement of new technologies, but the security, reliability, ethics and resilience of those technologies as well.

Artificial Intelligence and Machine Learning will become more prevalent tools in cybersecurity in the future. An AI-powered system is able to process vast amounts of security data and detect potential attacks, patterns, and support for automated incident response. There is a need for future studies to refine and clarify AI models to perform well in dynamic environments [62]. Researchers should also take steps to tackle specific threats to AI, such as adversarial attacks, data poisoning, model manipulation, and unauthorized use of AI for cybercrime. Creating trustworthy and secure AI systems will thus be a continuing research challenge [63].

Another important field for future research will be post-quantum cyber security. Some current cryptographic techniques will be potentially vulnerable to the advent of strong quantum computers. Organizations thus have to explore and adopt cryptographic methods that are resilient to quantum attacks. Post-quantum cryptographic algorithms need to be assessed in terms of performance, scale, and compatibility as well as long-term security [64]. The shift from current cryptographic systems to quantum resistant systems may also necessitate ample technical and organizational planning.

There are more research challenges in the continued growth of IoT and edge computing. Billions of interconnected devices will create and share a vast amount of data. Implementing strong security mechanisms is not easy due to the limited computational resources of many IoT devices. Lightweight encryption, secure authentication, privacy-preserving methods, automated device management, and AI-driven anomaly detection in resource-constrained settings are recommended areas for future research [65].

One major course to explore is the emergence of Zero Trust security architecture for increasingly distributed organisations. Traditional network boundaries are no longer relevant as applications, employees, devices and data are all working from disparate places. Adaptive authentication, ongoing risk assessment, an identity-based approach to access control, and automated policy enforcement are additional areas of research that could enhance Zero Trust environments [66]. Ethical issues and privacy will be additional major factors to consider. The ubiquity of data collection and analysis here

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

brings up some concerns with respect to surveillance, consent, data ownership, and responsible technology. Cybersecurity research should thus incorporate privacy protection and ethical considerations to system design for the future [67].

There should be a greater focus on human factors and cyber security education. A significant amount of security incidents are caused by human error, weak passwords, social engineering or by poor security practices. Creating successful awareness programs and cybersecurity skills will continue to be critical. Future research should be a multidisciplinary study, which integrates computer science, cybersecurity, artificial intelligence, law, ethics and human behavior [68]. Ongoing cooperation between researchers, governments, industry and educational institutions will be needed to achieve secure, resilient digital ecosystems that can adapt to the dynamic nature of technology and cybersecurity.

CONCLUSION

Information Technology and cybersecurity field are rapidly changing and shaping the way individuals, organizations, businesses and governments function in the digital environment. This review has explored some of the key emerging trends like Artificial Intelligence (AI) and Machine Learning (ML), cloud and edge computing, Internet of Things (IoT), Zero Trust Architecture, block chain, quantum computing, and advanced cyber threats. These technologies offer many potential benefits for increasing efficiency, automation, connections, data handling, and decision-making. Meanwhile, they have become ubiquitous, bringing in vulnerabilities and expanding the cybersecurity ecosystem, which is leading to ongoing changes in cybersecurity strategies.

AI and ML show promise to enhance cybersecurity by automating threat detection, behavioral analysis, anomaly identification, and quick incident response. But attackers can also create more advanced and automated attacks with the help of AI. In the same way, cloud and edge computing offer flexible and scalable computing resources, but with challenges such as security concerns, data privacy, access control, misconfiguration, and distributed infrastructure. With the proliferation of IoT, the attack surface has been further widened as billions of connected devices can have vulnerabilities and can also be sources for the collection of sensitive information. The developments are all evidence that technological innovation and cyber security must go hand in hand.

In a modern digital landscape where the number of devices accessing corporate networks is growing rapidly and many are positioned in remote locations, Zero Trust Architecture offers a critical strategy for securing identity, user, device, and access to sensitive information, while simultaneously challenging the traditional network perimeter as the initial line of defense.As the number of devices accessing corporate networks explodes and many of these devices are situated in remote locations,

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

Zero Trust Architecture offers a new way to secure identity, users, devices, and access to sensitive information, and to distrust the network perimeter as the first line of defense. While block chain can help to ensure data integrity, transparency, authentication, and decentralized security, quantum computing could revolutionize the way data is processed and pose a threat to current cryptographic systems. The advancements underline the necessity to anticipate upcoming security needs, including in-depth studies of post-quantum cryptography and developing secure design for technology.

Additionally, the review focuses on the increasing complexity of cyber threats such as ransomware, phishing, Advanced Persistent Threats, supply-chain attacks, malware and identity-based attacks. One security technology or perimeter defense is not enough for effective cybersecurity. But that's not the only solution; layers of different security measures are needed, including robust authentication, encryption, constant surveillance, network segmentation, vulnerability management, secure backups, employee education, threat intelligence, and thorough incident response planning.

Looking forward, cybersecurity research needs to be directed towards creating secure, privacy-preserving, reliable, and resilient technologies. There is a need to pay more attention to issues of AI security, quantum resistant cryptography, IoT protection, cloud security, Zero Trust implementation and automated threat detection. Human factors should also continue to be a primary concern, as the awareness and professional skills in cybersecurity, along with user's behaviors, play a crucial role in minimizing risks.

Finally, these new IT technologies have vast potential to drive economic growth, innovation and digital transformation, but also increasingly complex IT security challenges. Web security must become a fundamental part of the design of technology, because if it is not integrated from the start, it will never become sustainable. Securing and resilient digital ecosystems will require ongoing research, intergovernmental cooperation, industry-academic and cybersecurity collaboration, and good policies and user awareness. Thus, balancing technological innovation, security, privacy and responsible use will be crucial for the future of IT and cybersecurity.

REFERENCES

[1]. Areghan E. Emerging Frontiers in Cybersecurity: Navigating AI-Powered Threats, Quantum Risks, and the Rise of Zero-Trust Architectures. International Journal of Advanced Trends in Computer Science and Engineering 14 (3). 120. 2025 May;136.

[2]. Lilhore UK, Kumar S, Alroobaea R, Alsafyani M, Baqasah AM, Algarni S, Tekeste LG. A unified post-quantum zero-trust architecture with AI-driven orchestration for secure healthcare fog networks. Scientific Reports. 2026 Jul 1;16(1):20144.

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

[3]. Ţălu M. Security in internet of things and cloud computing convergence: Current trends, challenges, and perspectives. Annals of the Faculty of Engineering Hunedoara. 2025 Nov 1;23(4):39-52.

[4]. Gael N. Cybersecurity risk management in smart IoT ecosystems using artificial intelligence. International Journal of Business Integrity and Technology Advancements. 2026 Feb 3;2(01):01-12.

[5]. Eren H, Karaduman Ö, Gençoğlu MT. Security and privacy in the Internet of Everything (IoE): A review on block chain, edge computing, AI, and quantum-resilient solutions. Applied Sciences. 2025 Aug 6;15(15):8704.

[6]. Hafez NH. Toward Intelligent IoT Security: Integrating AI, Block chain, and Quantum-Adaptive Frameworks. Nile Journal of Communication and Computer Science. 2026 Jun 1;11(1).

[7]. Adeniji SA, Oke F, Okolo J, Dopamu O. Cybersecurity in the Age of Cloud Computing and IoT: Emerging Threats and Advanced Protective Technologies.

[8]. Cherbal S, Zier A, Hebal S, Louail L, Annane B. Security in internet of things: a review on approaches based on block chain, machine learning, cryptography, and quantum computing. The Journal of Supercomputing. 2024 Feb;80(3):3738-816.

[9]. Terli S, Banisetti JS, Dokala VS. Quantum computing and machine learning for cybersecurity: Technologies, challenges, and future perspectives. International Journal of Applied Resilience and Sustainability. 2026 Jul 28;2(3):324-54.

[10]. Ali G, Aziku S, Kabiito SP, Morish Z, Adebo T, Wamusi R, Asiku D, Sallam M, Mijwil MM, Ayad J, Salau AO. Integration of artificial intelligence, block chain, and quantum cryptography for securing the industrial internet of things (IIoT): Recent advancements and future trends.

[11]. Saranya D. Next-Generation Cybersecurity Architecture for Medical Imaging Ecosystems: Quantum-Resistant Zero-Trust Framework with Predictive Threat Intelligence. Journal of Intelligent Decision Making and Information Science. 2026 Aug 21;3(8s):1225-47.

[12]. Khan IU, Khan FM, Haider ZA, Alturise F. Integrating AI, Block chain, and Edge Computing for Zero-Trust IoT Security: A comprehensive review of advanced cybersecurity framework. Computers, Materials & Continua. 2025 Oct 23;85(3):4307-44.

[13]. Gupta S. Secure Artificial Intelligence Powered Cloud Computing Model for Enterprise Cyber Intelligence and Digital Transformation. Journal of Cyber-Physical Security and Robotics. 2026 Jul 29;2(03):23-32.

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

[14]. Laghari AA, Khan AA, Ksibi A, Hajjej F, Kryvinska N, Almadhor A, Mohamed MA, Alsubai S. A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture. Scientific Reports. 2025 Jul 23;15(1):26843.

[15]. Chang HC, Lund BD, Beuerlein E, Mote C. Investigating the symbiotic relationship between artificial intelligence and block chain to promote zero-trust cybersecurity in an evolving information ecosystem. Information Discovery and Delivery. 2025 Aug 15.

[16]. Jaleeli YA, Zainlabuddin M. Secure And Privacy Preserving IoT Cybersecurity With A Block chain Based Zero Trust Model. International Journal of Artificial Intelligence and Communication Networks. 2026 Aug 19;2(3):86-98.

[17]. Machado J. Block chain-Enabled Secure Data Management System for Intelligent Computing Networks. Journal of Smart Computing and Data Intelligence. 2026 Mar 27;2(1):17-24.

[18]. Mohamed N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems. 2025 Aug;67(8):6969-7055.

[19]. Narimane SA. A Review of Future Trends in Cybersecurity, Emerging Technologies, and Challenges. Cybersecurity of Information Systems: Artificial Intelligence and Machine Learning Solutions. 2026 Jun 1:393.

[20]. Sundhar S. Next-Generation Cloud Computing Architecture for Secure, Sustainable, and Intelligent Digital Services. Bishop International Journal of Mathematics and Computer Science. 2025 Mar 10;1(1):27-39.

[21]. Adere K, Hailu S, Abebe M, Kemal A, Silassie SW, Tseghai A, Haile G, Tamirat B, Bitew W, Regassa D, Gizachew Z. A systematic review of artificial intelligence applications in Internet of Things, block chain, and quantum cryptography. Discover Artificial Intelligence. 2026 Feb 22;6(1):270.

[22]. Yu J. Research on zero-trust cloud security protection system integrating quantum encryption and AI analysis. Computer Science. 2025 Dec;4(4).

[23]. Radanliev P. Integrated cybersecurity for metaverse systems operating with artificial intelligence, block chains, and cloud computing. Frontiers in Block chain. 2024 Apr 16;7:1359130.

[24]. Doyle JC. The Integration of Cybersecurity, Artificial Intelligence, and Data Privacy in Next-Generation Digital Systems. AJAMRI-American Journal of Advanced Multidisciplinary Research and Innovation. 2021 Apr 20;3(2).

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

[25]. Misra R, Sharma N. Emerging Cybersecurity Threats and Advanced Defense Technologies: Challenges, Risks and Future Security Solutions.

[26]. Farhan M, Latif RM, Ullah F, Naeem MR. Future trends and emerging technologies in IoT security. Edge Intelligence. 2026 Jan 1:209-39.

[27]. Agarwal A, Jena A, Mohanty P. Resolving Cyber Security Issues in 6G Networks Using Block chain Technology and Quantum Computing. In2025 OITS International Conference on Information Technology (OCIT) 2025 Dec 18 (pp. 1-6). IEEE.

[28]. Sen S. Artificial Intelligence and Cryptography in Data Security. In2026 IEEE World AI IoT Congress (AIIoT) 2026 May 20 (pp. 0877-0886). IEEE.

[29]. Ameen AH, Mohammed MA, Rashid AN. Dimensions of artificial intelligence techniques, block chain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions. Journal of Intelligent Systems. 2023 Apr 10;32(1):20220267.

[30]. Asiku D, Adebo T, Wamusi R, Aziku S, Kabiito SP, Zaward M, Sallam M, Ali G, Mijwil MM. A survey on artificial intelligence and block chain applications in cybersecurity for smart cities.

[31]. Abimbola O, Idris OO. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Path of Science. 2025 Mar 31;11(3):4009-20.

[32]. Jha MK. From IoT to critical infrastructure battling next-gen cyber threats. International Journal of Engineering Trends and Applications. 2025;12(5):48-57.

[33]. Rani S, Babbar H, editors. Intelligent Cybersecurity in the AI-IoT Era: Architectures, Threats, and Directions. CRC Press; 2026 Sep 22.

[34]. Gokila D. Artificial Intelligence-Driven Zero Trust Architecture for Next-Generation Cybersecurity: Challenges, Opportunities, and a Proposed Adaptive Security Framework: Page No.: 1-9. International Journal of Mathematical Computing and Systems Management. 2026 Aug 19;1(1).

[35]. Pramod JP, Kushika G, Manaswi G. Emerging technologies in the digital era: A future perspective. Anveshana's International Journal of Research in Engineering and Applied Sciences. 2025;10(4).

[36]. Vasumathi MT, Sadasivan M, Kamarasan M, Manikandan G. Integrating AI and Machine Learning to Enhance Data Security in Intelligent IoT Systems. Quantum Machine Learning: Artificial Intelligence for Smart Internet of Things Applications. 2026 Jun 11:75-111.

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

[37]. Khule M, Motwani D, Chauhan D. A layered and integrative framework for Advance Persistent Threat detection and mitigation: combining AI, Zero-Trust, and Advanced Threat Intelligence. Cluster Computing. 2025 Oct;28(11):740.

[38]. De Macêdo AR, Jagatheesaperumal SK, Da Costa KA, Acharya K, Song H, Guizani M, De Albuquerque VH. Quantum ai-enhanced iot-fog communication: A survey from cybersecurity and data privacy perspective. IEEE Communications Surveys & Tutorials. 2025 Oct 20.

[39]. Selvaperumal P, Sahoo LK, Tomar A, Ingale K, Radha N, Patel DJ, Verma S. Artificial Intelligence Enabled Zero-Trust Cyber Security Framework for Smart Healthcare Infrastructure. International Journal of Artificial Intelligence and Machine Learning. 2026 May 12;6(2s):204-17.

[40]. Goyal NK. Security and privacy in IoT, fog, and block chain networks. InEnergy-efficient deep learning approaches in IoT, fog, and green block chain revolution 2025 (pp. 371-398). IGI Global Scientific Publishing.

[41]. Tyagi AK. Block chain and artificial intelligence for cyber security in the era of internet of things and industrial internet of things applications. InAI and block chain applications in industrial robotics 2024 (pp. 171-199). IGI Global Scientific Publishing.

[42]. Chaubey NK, Chaubey N, editors. Advanced cyber security techniques for data, block chain, IoT, and network protection. IGI Global; 2024 Nov 29.

[43]. Bodkhe SG. Cryptographic Algorithms and the Future of Data Security. Scriptora International Journal of Research and Innovation (SIJRI). 2026 May 2:97-105.

[44]. Omotade AL, Ghimire A, Sultan M. Cybersecurity, Data Privacy, and Information Security Management. In2025 3rd International Conference on Artificial Intelligence and Automation Control (AIAC) 2025 Oct 15 (pp. 27-33). IEEE.

[45]. Sai S, Goyal I, Sharma S, Manuri SH, Chamola V, Buyya R. Quantum machine learning for cybersecurity: A taxonomy and future directions. Software: Practice and Experience. 2026.

[46]. PRIYADHARSHINI DS, KARIM SR, KHAN OU, CHOWDHURY SM, RAHAMAN KM, KHAN H. CYBERSECURITY IN THE AGE OF CLOUD COMPUTING: A REVIEW OF THREATS AND MITIGATION STRATEGIES. TPM–Testing, Psychometrics, Methodology in Applied Psychology. 2026 Feb 10;33(S2):67-76.

[47]. Davis P, Coffey S, Beshaj L, Bastian ND. Emerging technologies for data security in zero trust environments. The Cyber Defense Review. 2024 Jul 1;9(2):49-72.

[48]. Shaheen A. Cybersecurity in the modern era: An overview of recent trends. Journal of Engineering and Computational Intelligence Review. 2023 Dec 31;1(1):39-50.

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

[49]. Mujlid HM, Alshahrani R. Quantum-driven security evolution in IoT: AI-powered cryptography and anomaly detection. The Journal of Supercomputing. 2025 Jun 29;81(9):1087.

[50]. Rishiwal V, Agarwal U, Yadav M, Tanwar S, Garg D, Guizani M. A new alliance of machine learning and quantum computing: concepts, attacks, and challenges in iot networks. IEEE Internet of Things Journal. 2025 Jan 28;12(12):18865-86.

[51]. Čekerevac Z, Prigoda L, Cekerevac P. Leading technological innovations in digital security. InTechnological innovations in digital security 2025 (pp. 193-208).

[52]. Sharma S, Agrawal SS, Kumar SA. Unlocking cybersecurity horizons: exploring cutting-edge technologies, strategies, and trends in the dynamic cyber threat landscape. In2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC) 2024 Nov 23 (pp. 1-6). IEEE.

[53]. Silveira P. Integrating Artificial Intelligence with Cloud Computing for Enterprise Cybersecurity Data Intelligence and Intelligent Automation. International Journal of Engineering & Extended Technologies Research (IJEETR). 2026 Jul 15;8(3):5149-59.

[54]. Raghuveer Reddy Chandanaduru NM. Securing the Future of Connected Healthcare: AI, Block chain, and Emerging Technologies in Medical Device Cybersecurity. International Journal of Trend in Scientific Research and Development. 2025;9(5):8-16.

[55]. SathishKumar T, Kasi B, Kumarakrishnan S, Saravanan R, Tamilselvan T, Priyadharshini SD. Adversarial Artificial Intelligence in Cybersecurity: A Comprehensive Analysis. Cybersecurity of Information Systems: Artificial Intelligence and Machine Learning Solutions. 2026 Jun 1:281.

[56]. Ahmed W. Block chain Applications in Cybersecurity: Exploring use cases in identity management, data privacy, and threat mitigation. Prem. J. Sci.. 2025;7:100063.

[57]. Singh B, Chandra S, Kaunert C, Mishra S. Cruising artificial intelligence (AI) cutting-edge privacy protection and data security in metaverse and cloud computing. InNavigating AI and the metaverse in scientific research 2025 (pp. 305-320). IGI Global Scientific Publishing.

[58]. Singh R, Gehlot A, Akram SV, Sharma R, Malik PK. Next-generation cybersecurity system in integration with Artificial Intelligence and block chain. Smart Electronic Devices: Artificial Intelligence, Machine Learning, and the Future. 2025 Sep 16:293.

[59]. Uddin MS, Khan A, Alim I, Khan D. The Evolution of Cybersecurity in the Digital Age Contemporary Threats, Technologies, and Future Directions. Journal of Computational Systems & Engineering Insights. 2026 Jul 12;4(02):12-29.

ISSN : 3079-5761
Volume 2, Number 4, 2026
https://doi.org/10.70445/gtst.2.4.2026.45-63

[60]. Alsulami FN. Adaptive-AI-ZeroTrust-Chain: block chain-backed dynamic zero-trust enforcement via artificial intelligence. Journal of King Saud University Computer and Information Sciences. 2026 Jul;38(5):262.

[61]. Ashok G. AI-ASSISTED POST-QUANTUM CRYPTOGRAPHY FOR BLOCK CHAIN AND IOT SYSTEMS: EMERGING THREATS, INTELLIGENT DEFENSES, AND QUANTUM-SAFE ARCHITECTURES. Integrations in Engineering and Technology. 2026 May 11:21-.

[62]. Robert W, Denis A, Thomas A, Samuel A, Kabiito SP, Morish Z, Ali G. A comprehensive review on cryptographic techniques for securing internet of medical things: A state-of-the-art, applications, security attacks, mitigation measures, and future research direction. Mesopotamian Journal of Artificial Intelligence in Healthcare. 2024;2(1):135-69.

[63]. Iftikhar U, Rashid H, Attaullah HM. Future emerging challenges and innovations in next gen-cybersecurity and information systems security. InEmerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics 2025 Apr 18 (pp. 173-203). Cham: Springer Nature Switzerland.

[64]. Sola RP, Malali N, Madugula P. Cloud Database Security: Integrating Deep Learning and Machine Learning for Threat Detection and Prevention: 0. Notion Press; 2025 Feb 22.

[65]. Kalpana AV. Strengthening Enterprise Data Intelligence with Agentic AI Cloud Computing and Zero Trust Security Frameworks. Journal of Cyber-Physical Security and Robotics. 2025 Nov 30;1(02):116-25.

[66]. Ishtaiwi A, Al Khaldy MA, Al-Qerem A, Aldweesh A, Almomani A. Artificial intelligence in cryptographic evolution: Bridging the future of security. InInnovations in Modern Cryptography 2024 (pp. 31-54). IGI Global Scientific Publishing.

[67]. Joshan A. Analysis of Emerging Approaches in Cybersecurity for Internet of Things (IoT) Networks with an Emphasis on Smart Urban and Domestic Infrastructures. Journal of Data Analytics and Intelligent Decision-making. 2026 Mar 30;2(1):1-6.

[68]. AR S, Katiravan J. Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and block chain based cyber security. Scientific Reports. 2025 Jul 1;15(1):22369.