Journal of Global Research in Electronics and Communication
Volume 1, No. 4, April 2025
Available Online at: https://jgrec.info/index.php/jgrec/index
ISSN: 2321-3175
RESEARCH PAPER

Survey on IOT Security Vulnerability Risk Mitigation and Emerging Trends

Dr. Mohammad Sabir,
Associate Professor,
Electronics and Communication Engineering,
Geetanjali Institute of Technology and Management,
md.sabir@gits.ac.in

***Abstract*—The latest technological advancement, known as the Internet of Things (IoT), functions as a crucial force that links billions of intelligent devices throughout the healthcare industry sectors, as well as transportation systems and agricultural production, together with industrial operations. The extensive implementation of IoT systems brings important efficiencies and automation as well as data-powered decision processes, despite creating multiple security and privacy challenges for widespread implementation. IoT devices exist in resource-limited environments where their security features are insufficient, making them susceptible to data leakage attacks in addition to distributed denial-of-service (DDoS) attacks and unauthorized intrusions. The research analysis examines existing IoT security challenges along with their protective measures, which involve key management systems and machine learning detectors, and blockchain authentication protocols as examples. The survey tracks current security advancements that include AI monitoring for anomalies and implementations of zero-trust frameworks and TPMs, and PUFs hardware security elements. This paper explores recent evidence from literature and actual events to show that IoT systems need adapted security solutions that scale effectively and operate with minimal weight. Research gaps and future strategies for IoT network resilience as well as trustworthiness, appear in this survey for promoting improvements in an interconnected digital environment.**

Keywords*—*Internet of Things (IoT), IoT Security, Vulnerability Assessment, Risk Mitigation, Cybersecurity, Threat Detection, Machine Learning (ML), IoT Risk Management, Emerging Security Trends.

I. INTRODUCTION

The IoT stands as a vital digital infrastructure component that current technology serves to modernize different sectors and adjust human-technological interactions. IoT represents a system that unites various devices such as RFID tags, heart rate monitors, sensors, and intelligent meters to obtain, transfer and examine data with embedded systems and network connectivity [1][2]. Users can employ various sectors to install these things for intelligent decision-making in conjunction with real-time automation and monitoring.

The worldwide implementation of IoT devices shows a remarkable speed of growth. The quantity of connected devices rose from 8.4 billion in 2020 to 20.4 billion in 2022, based on recent data. The rapid rise of IoT directly corresponds to significant economic value growth because the industry is expected to generate over 4 trillion USD in revenue by 2025, while starting at 892 billion USD in 2018. Digital economy expansion is the main factor driving this rise in revenue [3]. The extensive growth of IoT has led to revolutionary applications in smart homes, distant patient observation and industrial automation and city management effectiveness [4], enhancing customer convenience, operational efficiency, and service personalization [5].

The IoT ecosystem continues to face many cybersecurity threats because of its limited resources and multiple device structure types. The lack of enough security mechanisms during deployment leaves numerous IoT devices vulnerable to attacks. The attack of a Jeep during highway travel in St. Louis by ethical hackers exemplifies how devices can be hijacked remotely to gain access to vehicle controls, including braking and engine operations, and entertainment functions [6]. Large-scale attacks from Distributed Denial of Service (DDoS) methods using Mirai malware-based botnets disrupt major US and French Internet service providers through thousands of hijacked IoT devices [7].

Standard security architectures find it difficult to adjust their methods to constraints present in IoT devices since they use limited computational power and draw limited power. Insufficient infrastructure capabilities block the proper deployment of cryptographic protocols, which results in poor functionality of essential protection services and secure connection maintenance. Developers now prioritize the creation of optimized key management plans that support the particular IoT ecosystem needs. The entire process consists of key creation along with distribution systems and protection frameworks, utilization elements, and revocation functionalities. The implementation of a secure scheme requires trusted entities to assign cryptographic keys, followed by protected distribution protocols based on cluster-based logical network architecture [8].

Several new security patterns are currently being developed for IoT security as global threats evolve. Artificial intelligence (AI), together with machine learning (ML) systems, is used for real-time anomaly detection followed by automated threat mitigation processes [9][10][11]. Blockchain technology provides decentralized authentication while it offers an unalterable database storage solution. Zero-trust security models are now gaining popularity through continuous least-privilege access security policies that span across all networks. The security features of Through hardware mechanisms, Trusted Platform Modules (TPMs) and Physically Unclonable Functions (PUFs) provide fundamental device protection. These new security innovations combine to create an adaptive intelligent safety

solution set that protects the continuous growth of IoT systems.

A. Structure of the Paper

This review paper includes Section II on IoT security vulnerabilities, Section III discusses risk mitigation strategies, Section IV covers challenges and future directions, Section V presents the LOR, and Section VI concludes with findings and future research suggestions.

II. Security Vulnerabilities In IoT

The security of IoT devices must be paramount because they directly connect to the physical infrastructure. The open-source security flaws discovered in these devices create direct dangers to operational safety, particularly in industrial applications and critical infrastructure [12][13]. Attackers are unable to alter device settings in a manner that might endanger workers or equipment when proper security safeguards are in place. As more businesses integrate IoT devices into their physical infrastructure, this is very helpful.

A. Common threats and attack vectors

Three categories may be used to classify security concerns. dangers in the form of hardware assaults (using IC applications). The second concern is the use of malicious software to take over devices completely. Lastly, dangers that intercept and alter data while it's in transit [14][15].

B. Case studies of IoT security breaches

Several notable case studies highlight the consequences of IoT security flaws in the real world:

- **Miraa Botnet:** The Miraa botnet launched huge DDoS assaults in 2016 by taking advantage of IoT devices' default passwords, resulting in widespread internet disruptions [16]
- **Smart Home Intrusions:** Researchers have shown how flaws in smart home appliances may be used to monitor activity, get unauthorized access, and even take control of home automation systems.
- **Industrial IoT:** Industrial IoT device security lapses may cause serious interruptions, monetary losses, and even physical injury. For instance, Iran's nuclear program suffered significant harm when the Stuxnet virus attacked industrial control systems [17][18].

C. Impact on industries and users

There are several challenges for industrial IoT networks. Having fast and dependable WIFI connectivity is essential. Manufacturing on a manufacturing line, surgical equipment, and tracking are among the applications that need connections with low latency and high dependability. A piece of hardware with a sensor that can send data to a remote place over the internet is called an Internet of Things device [19][20][21]. Due to the large number of sensors involved in its functioning, a complex system has to be built with the least amount of money, time, and work possible. Because patient data is sensitive and important, data security is essential in sectors like healthcare. Many IoT applications need to make smart choices in real time according to user expectations.

III. Risk Mitigation Strategies

Risk mitigation is the process of identifying, assessing, and mitigating the risks to which your business may be subject. Numerous possible dangers, including natural disasters, unstable economies, strategic mistakes, and more, might give rise to these hazards. Several techniques that may be used for various hazards are necessary for effective risk mitigation.[22]. The main goal is to reduce the possible effects on your project or organization, not to completely remove them.

A. Encryption and secure communication

The user may decide to secure personal information by encrypting the image text and sending the encrypted copy of the data to the cloud server for storage. However, after users upload the image text to the cloud server, several common tasks in the plaintext sector, such as searching for a certain file, become difficult [23][24][25]. Once the user has downloaded, searching the file is the simplest way to recover all encrypted files from the cloud server locally and convert them back to plaintext. However, the massive amount of duplicated data would result in needless network and storage expenses throughout the deployment phase. Large-scale data encryption and decryption will result in a significant computing strain in the meantime. Furthermore, its viability is further diminished by the restriction of objective constraints like network capacity.

B. Authentication mechanisms and access control

A vital precondition for IoT security is authorization. Participants must be authenticated by the receiving node to gain entry to any IoT apps or entities. Typically, IoT utilities, along with apps, concentrate on data exchanges across several networks [26][27]. After analysis, a decision-making process transfers the data gathered from IoT systems. The data flow in these applications may be comparable. However, these processes may vary depending on the IoT architecture. For instance, a user or an application needs certain data without compromising the generality of data from an IoT device. The transmitter node to the IoT network should then be authenticated by the IoT device. Access permissions to the necessary data or node should be ensured for the requester [28]. The request to access such data or node is denied in any other way. AAs are crucial in IoT networks because of their functions in regulating the network's degree of management of trust and stopping scammers from impersonating genuine IoT devices. Furthermore, all users' access to sensitive data via IoT apps or nodes must be terminated after a predetermined period of inactivity. Several authentication methods are covered in this section. they describe many types of AA from the literature before talking about ML-based AA systems [29].

C. Blockchain for IoT security

Blockchain is one of the main services that has the potential to transform IoT and help solve its problems [1, 2, 3]. Additionally, since biological phenomena and IoT share some functions, bio-inspired AI techniques have emerged as a viable paradigm for dynamic and adaptable IoT networks [30][31].

Intelligence of Things that depend on a single point of detection may be produced via AI-based models. They are based on a third-party auditor, which is a centralized server/client paradigm in charge of verifying all nodes [32], In contrast, one of the most widely used decentralization technologies is Blockchain in Figure 1. All network transactions are stored in this distributed database, which all network users share. Blockchain-based approaches provide a shared distributed ledger with a consensus process that may

ensure safe, unchangeable data sharing [33][34]. Issues with privacy and reliability may be resolved by the Blockchain.

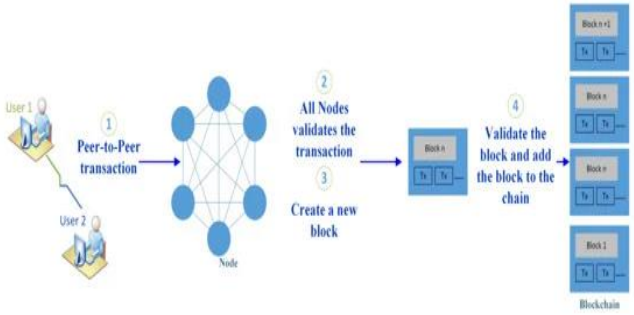

Fig. 1. Blockchain for IOT security

D. Emerging Trends in IoT Security

Figure 2 demonstrates some of the challenges and recent advancements in the field of IoT security research. IoT security challenges include device heterogeneity, scalability, privacy concerns, firmware/software defects, and networking safety. The primary focus is on safe coding practices, privacy-preserving tactics, and standardized security standards.[35][36]. Research is also addressing legal and regulatory issues and investigating how blockchain and DLT might be integrated for improved security. In the context of the IoT, AI and ML systems must be trusted in order to ensure their reliability and security [37].

Fig. 2. Trends in IOT security

1) AI and machine learning in threat detection

In the finals of 2021, danger recognition was improved with limitations on privacy and the use of AI and machine intelligence was prioritized. Strong security architectures and edge computing became the main priorities. with the adoption of Zero Trust concepts and automated security features [38][39][40]. A yearly visual representation of the effectiveness of IoT secure technologies can be seen throughout this time, Cooperation between regulatory agencies and stakeholders has been essential to bolstering IoT security requirements and effectiveness indicators. IoT security evolution.

2) Edge computing and decentralized security models

The primary objective of using Blockchain technology with edge computing is to improve security and efficiency in a distributed network [41][42][43]. Both of these technologies are also made to function well in huge systems. This makes it easy for the two systems to integrate. In We examine how blockchain technology may be integrated with edge computing in the next parts of this piece of content.

3) Role of quantum cryptography in future security paradigms

Comparing quantum cryptography to lightweight encryption, such as Ascon, which is designed for low-memory devices like IoT devices, reveals a distinct strategy. With its primary emphasis on quantum key distribution (QKD) and adherence to quantum mechanical principles, it provides security that is almost hard to breach [44][45][46].

Ascon is the focus of NIST's efforts to safeguard data on tiny IoT devices with constrained processing power. However, quantum cryptography seeks to use the unique properties of quantum bits (qubits) for secure communication, independent of the computing capability of the device [47].

IV. Challenges And Future Directions

Several AI algorithms that are appropriate for smart cities and how they could affect urban life. There are some challenges discussed below.

A. Scalability and interoperability issues

The capacity of a system to manage varying loads so that it can react quickly to changes in applications and system processing demands is known as scalability. Scaling machine learning programs that can manage any volume of data and carry out many calculations economically and efficiently to immediately serve millions of users spread throughout the globe is known as machine learning scalability [48] [49]. Data mining, machine learning, and statistics are used to provide flexible, scalable, and often nonparametric methods that enable ML scalability. Increased productivity, improved automation, improved modularization, and cost-effectiveness are just a few of the many advantages it gives the company.

B. Future research opportunities

Machine Learning-based security solutions for IoT systems, incorporating [50]. To start the conversation, the authors described the layers of the IoT system and the varied security threats that these levels face, such as various types of cyberattacks. Many machine-learning approaches were included in the paper, along with how they may be used to counteract different types of IoT system threats. The authors provided a cutting-edge analysis of security solutions for IoT devices, with an emphasis on employing machine learning techniques in all three IoT system levels. Finally, the writers discussed the difficulties and restrictions associated with ML-based security solutions for IoT systems and suggested possible avenues for further study.

C. Scalability and interoperability issues

There are issues with the scalability of this incorporation as well; as the total amount of IoT devices rises, it becomes more difficult to manage and aggregate data compared to an increasing number of sensors. To enable efficient To enable comprehensive and coherent environmental analysis during AI model training and deployment, standardized data formats and consistent information meaning across various IoT devices and platforms must be established [51].

D. Ethical and legal considerations

The IoT is still expanding in the twenty-first century. The biggest drawbacks of these technologies often go unnoticed as

their attention switches to using more of them to make their lives more convenient. This paper's analysis of the security, privacy, ethical, and legal issues surrounding IoT has shown how these issues significantly affect their day-to-day lives and how, considering the rapid expansion of the industry, there is a dearth of studies on these negative aspects [52].

E. Future research opportunities

The difficulties of deploying data-driven artificial intelligence (AI) solutions in modern smart cities, focusing on the algorithms' security, safety, and interpretability while providing advice on their present drawbacks, restrictions, and possible future research areas M. H. Panahi Rizi and S. A. Hosseini Seno provide an organized literature map and acknowledge current security and privacy solutions, unsolved research challenges, and barriers. The study's objectives are to provide a provide a starting point for more study in the field and condense the results into a collection of previously intricate and diverse data.

V. LITERATURE REVIEW

The lor section summarizes key studies on IoT security and applications, outlining each paper's focus, findings, research gaps, and future directions across areas like sustainability, proxy systems, port risk management, vulnerability frameworks, cloud security, and supply chain optimization.

Valencia-Arias et al. (2024) In the framework of ecological sustainability, this essay explores how technological developments, particularly in the Internet of Things (IoT) space, can foster social, economic, and productive growth. Through a bibliometric analysis utilizing PRISMA, the study aims to pinpoint certain patterns in the usage of these systems for sustainable activities. An assessment of the productivity of science worldwide is given in the book, emphasizing the important contributions made by nations like the US and China. Additionally, it highlights how important India is to the effectiveness of the agri-food supply chain [53].

Canavese et al. (2024) in this research paper, the author demonstrates the flexible nature of the IoT Proxy system that enhances IoT security and resiliency primarily during resource-constrained deployments. The IoT Proxy achieves externalized security involves redirecting data from IoT devices via a secure network gateway that houses a number of Virtual Network Security Functions (VNSFs). The solution encompasses VPN terminators and IPS that rely on oblivious authentication to create device identification through machine learning for IP-based defense systems. Through externalized security implementation, the IoT Proxy establishes a robust and protected IoT environment that specifically protects resource-constrained IoT devices [54].

Argyriou and Tsoutsos (2024) in this research, the paper evaluates vital aspects at port areas connected to IoT devices prior to developing a risk-management structure designed for these environments. This report examines risk mitigation strategies together with best practices that will be described alongside recommendations for reducing these risks. Research developers created a risk-management framework by establishing its foundation with ORM principles and its utilization of avoidance and reduction, and techniques for retention and sharing. This study's primary accomplishment is the creation of a comprehensive risk-management framework based on Operational Risk-Management (ORM) methodology that is tailored for port IoT devices [55].

Baho and Abawajy (2023) the research evaluates and analyzes both the prevailing IoT vulnerability assessment frameworks and their corresponding challenges with an extensive and deep assessment approach. Research findings serve to better understand modern approaches for IoT vulnerability assessment thus enabling better risk characterization strategies during IoT vulnerability management initiatives. Multiple groups of readers from both IoT research fields and cybersecurity research, together with risk and vulnerability management professionals, will find this content interesting [56].

Gayathri et al. (2023) this paper a solution that develops strategies to protect cloud-based IoT devices from fake data injection and distributed denial-of-service (DDoS) assaults. The suggested security system combines moving target defense (MTD) techniques with access control rules (ACL), Kullback-Leibler distance (KLD), and simple network management protocol (SNMP) [57].

Mashayekhy et al. (2022) This paper intends to draw attention to the ways that Iot technologies affect supply chain inventory management and carries out an extensive investigation to determine the research gaps in this area. Through examination of the literature, the pattern and the potential of using IoT in industry 4.0 inventory management are investigated. Result their results indicate that more industries are doing studies on this subject [58].

Table I presents a summary of key literature on IoT security vulnerability and risk mitigation, highlighting each study’s focus, findings, deficiencies, and future directions, emphasizing the need for scalable, secure, and adaptable IoT solutions across various application domains

TABLE I. **SUMMARY ON** IOT SECURITY VULNERABILITY RISK MITIGATION

Reference	Focus	Findings	Deficiencies	Future Work
Valencia-Arias et al. (2024).	Role of IoT in sustainable development via bibliometric analysis using PRISMA	IoT contributes significantly to economic, productive, and social development; China, the USA, and India are leading contributors	Lack of technical focus on security and risk management	Suggest future exploration of security aspects in sustainable IoT adoption
(Canavese et al. (2024),	IoT Proxy for secure and resilient IoT communication via externalized security	Introduced IoT Proxy with VPN terminator and ML-based IPS; ensures secure communication for resource-limited devices	Limited scalability testing; no real-world deployment validation	Extend implementation in real-world settings; test with diverse IoT ecosystems
Argyriou and Tsoutsos (2024),	Framework for IoT risk management in port contexts	Developed ORM-based risk mitigation strategies tailored to port-based IoT infrastructure	Sector-specific; lacks adaptability to other critical sectors	Expand framework for broader application in transport and logistics
Baho and Abawajy (2023),	Systematic review of IoT vulnerability assessment frameworks	Highlights current tools and methods for vulnerability assessment; identifies key gaps	Does not propose a new framework; limited to a survey of the literature	Develop comprehensive models combining AI and real-time detection

Gayathri et al. (2023),	IoT cloud security using SNMP, KLD, ACL, and MTD	Proposed a multi-technique security model against DDoS and false data injection	High complexity; may not be feasible for constrained devices	Optimize the framework for lightweight environments; test performance on edge devices
Mashayekhy et al. (2022),	IoT implementation in supply chains and inventory management	Shows growing interest in using IoT for inventory monitoring; identifies research gaps	Focuses on industry trends, not technical vulnerabilities	Study IoT security issues in inventory management; explore secure data integration

VI. Conclusion And Future Work

The IoT continues to transform industries, offering unparalleled connectivity and automation; however, these advancements come with increasing security vulnerabilities. This survey has explored the situation of IoT security today, emphasizing the main obstacles such as weak encryption, poor key management, and inadequate protection for resource-constrained devices. Various risk mitigation strategies have been identified, including ML-based intrusion detection systems, blockchain for decentralized authentication, and the adoption of zero-trust security models. While these techniques show promise, the fast-evolving threat landscape demands continuous innovation. The growing integration of AI and ML into IoT ecosystems provides adaptive reactions and real-time threat detection, however, these technologies themselves must be hardened against adversarial attacks.

Future work should focus on developing lightweight, scalable security solutions suitable for constrained environments and integrating cross-layer security frameworks that consider device, network, and application-level risks. Additionally, standardization of security protocols and regulatory frameworks will play a crucial role in achieving secure interoperability across diverse IoT platforms. More empirical research and large-scale real-world testing are needed to confirm if the suggested remedies are effective. As IoT adoption expands, a collaborative approach involving academia, industry, and policymakers will be necessary to create an IoT infrastructure that is reliable, safe, and secure.

References

[1] T. Mazhar *et al.*, "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," *Brain Sci.*, vol. 13, no. 4, 2023, doi: 10.3390/brainsci13040683.

[2] D. D. Rao, "Systematic Analysis of threats, Machine Learning solutions and Challenges for Securing IoT environment," *J. Cybersecurity Inf. Manag.*, vol. 14, no. 2, pp. 367–382, 2024.

[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEe Access*, vol. 7, pp. 82721–82743, 2019.

[4] B. Ślusarczyk, "Industry 4.0: Are we ready?," *Polish J. Manag. Stud.*, vol. 17, 2018.

[5] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, 2020, doi: 10.1186/s40537-020-00318-5.

[6] M. Wazid, A. K. Das, S. Shetty, J. JPC Rodrigues, and Y. Park, "LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment," *Sensors*, vol. 19, no. 24, p. 5539, 2019.

[7] M. Rana, Q. Mamun, and R. Islam, "Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers," *Sensors*, vol. 23, no. 18, 2023, doi: 10.3390/s23187678.

[8] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surv. \& Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[9] V. Pillai, "Anomaly Detection in Financial and Insurance Data-Systems," *J. AI-Assisted Sci. Discov.*, 2024.

[10] S. R. Thota, S. Arora, and S. Gupta, "Hybrid Machine Learning Models for Predictive Maintenance in Cloud-Based Infrastructure for SaaS Applications," in *2024 International Conference on Data Science and Network Security (ICDSNS)*, IEEE, Jul. 2024, pp. 1–6. doi: 10.1109/ICDSNS62112.2024.10691295.

[11] V. P. Shashikant Tank Kumar Mahendrabhai Shukla, Nimeshkumar Patel, "AI Based Cyber Security Data Analytic Device," pp. 414425–001, 2024.

[12] P. M. Rajendra Prasad Sola, Nihar Malali, "Cloud Database Security: Integrating Deep Learning and Machine Learning for Threat Detection and Prevention: 0," *Notion Press*, 2025.

[13] M. Gopalsamy and K. B. Dastageer, "The Role of Ethical Hacking and AI in Proactive Cyber Defense : Current Approaches and Future Perspectives," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 2, 2025, doi: 10.5281/zenodo.14916984.

[14] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, Aug. 2022, doi: 10.1016/j.iot.2022.100564.

[15] M. Gopalswamy, "Building Scalable Anomaly IdentificationSystems toIoT Threat Mitigation usingMachine learning Techniques," *ournal Glob. Res. Math. Arch.*, vol. 12, no. 1, 2025.

[16] S. Arora and S. R. Thota, "Automated Data Quality Assessment And Enhancement For Saas Based Data Applications," *J. Emerg. Technol. Innov. Res.*, vol. 11, pp. i207–i218, 2024, doi: 10.6084/m9.jetir.JETIR2406822.

[17] P. P. B Yadav, DD Rao, Y Mandiga, NS Gill, P Gulia, "Systematic Analysis of threats," *Mach. Learn. Solut. Challenges Secur. IoT Environ. J. Cybersecurity Inf. Manag.*, vol. 14, no. 2, 2024.

[18] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 2, 2021, doi: DOI: 10.48175/IJARSCT-6268B.

[19] I. S. Using, "brain sciences Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," 2025.

[20] A. G. Milavkumar Shah, "Distributed Query Optimization for Petabyte-Scale Databases," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 10, no. 10, pp. 223–231, 2022.

[21] Vashudhar Sai Thokala, "Scalable Cloud Deployment and Automation for ECommerce Platforms Using AWS, Heroku, and Ruby on Rails," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 2, pp. 349–362, Oct. 2023, doi: 10.48175/IJARSCT-13555A.

[22] V. Prajapati, "Cloud-Based Database Management: Architecture, Security, challenges and solutions," *J. Glob. Res. Electron. Commun.*, vol. 01, no. 1, pp. 07–13, 2025, doi: https://doi.org/10.5281/zenodo.14934833.

[23] L. Liu, M. Gao, Y. Zhang, and Y. Wang, "Application of machine learning in intelligent encryption for digital information of real-time image text under big data," *EURASIP J. Wirel. Commun. Netw.*, vol. 2022, no. 1, p. 21, 2022, doi: 10.1186/s13638-022-02111-9.

[24] S. Murri, "Data Security Environments Challenges and Solutions in Big Data," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 565–574, 2022.

[25] A. and P. Khare, "Cloud Security Challenges : Implementing Best Practices for Secure SaaS Application Development," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 669–676, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.11.

[26] K. Istiaque Ahmed, M. Tahir, M. Hadi Habaebi, S. Lun Lau, and A. Ahad, "Machine Learning for Authentication and Authorization

in IoT: Taxonomy, Challenges and Future Research Direction," *Sensors*, vol. 21, no. 15, 2021, doi: 10.3390/s21155122.

[27] S. Shah and M. Shah, "Deep Reinforcement Learning For Scalable Task Scheduling In Serverless Computing,"," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 3, no. 12, pp. 1845–1853, 2021.

[28] N. Malali, "Robustness and Adversarial Resilience of Actuarial AI/ML Models in the Face of Evolving Threats," *Int. J. Innov. Sci. Res. Technol.*, 2025.

[29] T. A. Murri Srinivas, Swetha Chinta, Souratn Jain, "Advancing Cloud Data Architectures: A Deep Dive into Scalability, Security, and Intelligent Data Management for Next-Generation Applications," *Well Test. J.*, vol. 33, 2024.

[30] V. Prajapati, "Blockchain-Based Decentralized Identity Systems : A Survey of Security , Privacy , and Interoperability," vol. 10, no. 3, 2025.

[31] A. K. Aftab Arif, Muhammad Ismaeel Khan, "An overview of cyber threats generated by AI," *Int. J. Multidiscip. Sci. Arts*, vol. 3, no. 4, pp. 67–76, 2024.

[32] M. S. Akaash Vishal Hazarika, "Serverless Architectures: Implications for Distributed System Design and Implementation," *Int. J. Sci. Res.*, vol. 13, no. 12, pp. 1250–1253, 2024.

[33] M. S. Akaash Vishal Hazarika, "Blockchain-based Distributed AI Models: Trust in AI model sharing," *Int. J. Sci. Res. Arch.*, vol. 13, no. 2, pp. 3493–3498, 2024.

[34] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *J. Glob. Res. Electron. Commun.*, vol. 2, no. 2, pp. 1–7, 2025, doi: https://jgrec.info/index.php/jgrec.

[35] S. R. Teja Krishna Kota1, "Implementing AI-Driven Secure Cloud Data Pipelines in Azure with Databricks," *Nanotechnol. Perceptions*, vol. 20, 2024, doi: https://doi.org/10.62441/nano-ntp.vi.4439.

[36] V. S. Thokala, "A Comparative Study of Data Integrity and Redundancy in Distributed Databases for Web Applications," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 383–389, 2021.

[37] S. S. S. Neeli, "Critical Cybersecurity Strategies for Database Protection against Cyber Attacks," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, p. 5, 2023.

[38] S. R. Siraparapu and S. M. A. K. Azad, "Securing the IoT Landscape: A Comprehensive Review of Secure Systems in the Digital Era," *e-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 10, p. 100798, 2024, doi: https://doi.org/10.1016/j.prime.2024.100798.

[39] Godavari Modalavalasa, "The Role of DevOps in Streamlining Software Delivery: Key Practices for Seamless CI/CD," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 1, no. 12, pp. 258–267, Jan. 2021, doi: 10.48175/IJARSCT-8978C.

[40] J. Thomas, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.

[41] M. Alrakhami, A. Gumaei, A. Alamri, and S. M. M. Rahman, "Decentralized Blockchain-based model for Edge Computing," 2021. doi: 10.48550/arXiv.2106.15050.

[42] S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. Paul Aderemi, "Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches," in *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICIPTM59628.2024.10563348.

[43] H. Chandu, "Advanced Methods for Verifying Memory Controllers in Modern Computing Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, pp. 377–388, 2024, doi: 10.48175/IJARSCT-19862.

[44] P. Radanliev, "Artificial intelligence and quantum cryptography," *J. Anal. Sci. Technol.*, vol. 15, no. 1, p. 4, 2024, doi: 10.1186/s40543-024-00416-6.

[45] S. S. S. Neeli, "Securing and Managing Cloud Databases for Business - Critical Applications," *J. Eng. Appl. Sci. Technol.*, vol. 7, no. 1, p. 6, 2025.

[46] A. Goyal, "Scaling Agile Practices with Quantum Computing for Multi-Vendor Engineering Solutions in Global Markets," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 557–564, 2022.

[47] N. Patel, "Quantum Cryptography In Healthcare Information Systems: Enhancing Security In Medical Data Storage And Communication," *J. Emerg. Technol. Innov. Res.*, vol. 9, no. 8, 2022.

[48] M. K. A Arif, A Khan, "Role of AI in Predicting and Mitigating Threats: A Comprehensive Review," *JURIHUM J. Inov. dan Hum.*, vol. 2, no. 3, pp. 297–311, 2024.

[49] Censius, "What is Scalability?," *censius.ai*, 2024.

[50] M. E. E. Alahi *et al.*, "Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends," *Sensors*, vol. 23, no. 11, 2023, doi: 10.3390/s23115206.

[51] D. M. Dave and B. Mittapally, "Data Integration and Interoperability in IOT: Challenges, Strategies and Future Direction," *Int. J. Comput. Eng. Technol.*, vol. 15, pp. 45–60, 2024.

[52] A. Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," *Internet of Things*, vol. 15, p. 100420, 2021, doi: https://doi.org/10.1016/j.iot.2021.100420.

[53] A. Valencia-Arias *et al.*, "Research Trends in the Use of the Internet of Things in Sustainability Practices: A Systematic Review," *Sustainability*, vol. 16, no. 7, 2024, doi: 10.3390/su16072663.

[54] D. Canavese, L. Mannella, L. Regano, and C. Basile, "Security at the Edge for Resource-Limited IoT Devices," *Sensors*, vol. 24, no. 2, 2024, doi: 10.3390/s24020590.

[55] I. Argyriou and T. Tsoutsos, "Assessing Critical Entities: Risk Management for IoT Devices in Ports," *J. Mar. Sci. Eng.*, vol. 12, no. 9, 2024, doi: 10.3390/jmse12091593.

[56] S. A. Baho and J. Abawajy, "Analysis of Consumer IoT Device Vulnerability Quantification Frameworks," *Electronics*, vol. 12, no. 5, 2023, doi: 10.3390/electronics12051176.

[57] R. Gayathri *et al.*, "Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques," *Sensors*, vol. 23, no. 3, 2023, doi: 10.3390/s23031708.

[58] Y. Mashayekhy, A. Babaei, X.-M. Yuan, and A. Xue, "Impact of Internet of Things (IoT) on Inventory Management: A Literature Survey," *Logistics*, vol. 6, p. 33, 2022, doi: 10.3390/logistics6020033.

