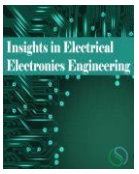
Lanash
Insights in Electrical Electronics Engineering
Research Paper
Volume 2 Issue 2
Published 09 December 2025




# Invigorating Internet of Things (IoT) Security within the Era of Artificial Intelligence (AI): Challenges, Innovations, and Future Pathways

**Z.B. Akhtar*[1] and A.T. Rawol[2]**

[1]Department of Computing, Institute of Electrical and Electronics Engineers (IEEE), USA
[2]Department of Computer Science, American International University-Bangladesh (AIUB), Bangladesh

Submitted on 09 June 2025
Accepted on 11 November 2025
Published on 09 December 2025

**To cite this article:** Z.B. Akhtar and A.T. Rawol, "Invigorating Internet of Things (IoT) Security within the Era of Artificial Intelligence (AI): Challenges, Innovations, and Future Pathways," *Insight. Electr. Electron. Eng.*, vol. 2, no. 2, pp. 1-14, 2025.



**Abstract**
As the accretion towards Internet of Things (IoT) expands and artificial intelligence (AI) becomes increasingly integrated into everyday technologies, safeguarding the security and privacy of IoT devices has become critical. This research exploration investigation presents a comprehensive analysis of the intersection between IoT, AI, and cybersecurity, identifying key challenges, proposing innovative strategies, and envisioning a secure future for IoT ecosystems. By exploring the intricate dynamics of IoT security within the realms of AI, cloud computing, and mobile internet, this research also highlights the evolving threats and emerging solutions. It offers a multidimensional perspective on the interplay between these technologies, providing valuable insights into building robust and secure IoT infrastructures in the age of AI.

**Keywords:** Artificial Intelligence; Blockchain; Cybersecurity; Deep Learning; Internet of Things; Machine Learning; Security; Privacy

**Abbreviations:** AI: Artificial Intelligence; DL: Deep Learning; IoT: Internet of Things; ML: Machine Learning; IoMT: Internet of Military Things

## 1. Introduction

In today's rapidly evolving digital ecosystem, the convergence of the Internet of Things (IoT) and Artificial Intelligence (AI) is ushering in a transformative era marked by unprecedented levels of innovation, connectivity, and automation [1,2,3]. IoT devices, ranging from smart home appliances to industrial sensors, have become integral components of this interconnected world. Meanwhile, AI technologies, fueled by machine learning and deep neural networks, are enhancing automation and decision-making processes across industries. However, with these advancements comes a critical challenge: ensuring the security and privacy of IoT devices in an increasingly complex environment.

The fusion of IoT and AI, hallmarked by the Fourth Industrial Revolution, represents a world where devices not only function autonomously but also communicate with each other. IoT devices now handle vital tasks, such as monitoring health metrics, managing energy consumption, and optimizing industrial operations. Simultaneously, AI systems process the data generated by these devices to make informed, real-time decisions, fundamentally reshaping industries, economies, and everyday life. Yet, this synergy also introduces significant security and privacy risks that require urgent attention and innovative solutions.

This research aims to thoroughly examine the intersection of IoT, AI, and security, focusing on the critical need for robust protection and privacy preservation in these interconnected systems. Taking a holistic approach, the study will explore not only the security of individual IoT devices but also the broader ecosystem in which they operate. Recognizing that IoT's evolution is intrinsically linked to advancements in Cloud Computing, Mobile Internet, Cryptography, Digital Forensics, and Information Hiding Technologies, this research will take an interdisciplinary approach to explore secure, privacy-respecting solutions for IoT. At the heart of this investigation lies a central question: How can we ensure the integrity, confidentiality, and availability of IoT data and services while leveraging the full potential of AI? To answer this question, we will analyze the unique security and privacy challenges posed by IoT, explore the dual role of AI as both a potential threat and safeguard, and investigate hardware and software security measures. Additionally, we will delve into the application of cryptography, digital forensics, and information hiding techniques, while examining the relationship between IoT, Cloud Computing, and Mobile Internet technologies in combating emerging cyber threats [4,5,6]. Through a comprehensive analysis of the state of IoT security and privacy, this research aims to inform both the academic community and industry stakeholders, empowering policymakers, innovators, and developers to shape a future where the promises of IoT and AI can be realized securely and responsibly [7,8,9]. As we navigate the ever-evolving landscape of IoT and AI, we embark on a journey that balances innovation with responsibility, ensuring that the future is both connected and secure.

## 2. Methods and Experimental Analysis

This research exploration adopts a wide range of mixed-methods approaches, integrating both qualitative and quantitative techniques to comprehensively investigate the security and privacy challenges of IoT devices in the context of AI integration. The qualitative methods have explored key challenges, assessed regulatory frameworks, and gathered expert opinions, while the quantitative methods focused on data analysis, simulations, and the evaluation of security measures and their effectiveness.

*Corresponding Author:
Z.B. Akhtar, Department of Computing, Institute of Electrical and Electronics Engineers (IEEE), USA

To begin, an extensive background research investigation analysis was conducted to identify existing research, frameworks, and case studies relevant to IoT security, AI integration, and related technologies. This will provide a foundational understanding of the current state of the field. In parallel, expert interviews were also conducted with professionals from diverse areas such as IoT, AI, cybersecurity, and digital privacy. These interviews will yield valuable insights into current challenges and emerging trends in securing IoT ecosystems. Additionally, surveys were also administered to a range of stakeholders, including IoT device manufacturers, AI developers, and end-users, to gather data on existing practices, concerns, and the adoption of security measures. Real-world data were also collected from different types of IoT devices, simulators, and controlled testbeds, which will play a crucial role in analyzing vulnerabilities, data flows, and communication patterns. This data will serve as the basis for both qualitative and quantitative analysis.

The analysis phase will be split into qualitative and quantitative segments. Qualitative analysis will utilize thematic analysis to extract key themes, challenges, and recommendations from expert interviews and background research. Thematic patterns will be identified, allowing for the development of a comprehensive understanding of the security and privacy concerns surrounding IoT devices and AI integration. For the quantitative analysis, statistical methods, machine learning algorithms, and simulation tools were mainly used to evaluate the effectiveness of security measures, AI-based threat detection techniques, and data encryption methods. These analytical approaches will provide insights into the real-world applicability and impact of various security strategies. In terms of experimental analysis, a controlled environment was also established to test a range of IoT devices, such as smart sensors, wearables, and home automation systems. AI integration will be a central component, with AI algorithms applied to tasks like anomaly detection, intrusion prevention, and predictive security. Simulations were used to assess cloud-based data storage and mobile internet connectivity scenarios, providing a comprehensive overview of how their security measures perform across different IoT environments.

Security measures were rigorously evaluated throughout the research. The assessment encompasses hardware security, software/firmware security, cryptography, and digital forensics. Hardware security will focus on secure boot processes, tamper resistance, and hardware-based authentication mechanisms. Software and firmware security will examine processes such as firmware updates, software patching, and vulnerability assessments. Encryption protocols were assessed for their impact on ensuring data confidentiality, and digital forensics techniques which were developed to investigate IoT device security incidents. Ethical considerations were also a key priority in all aspects of the research process. Data collection, participant consent, and data handling followed ethical guidelines, especially in the case of sensitive personal or healthcare data. The research will comply with relevant data protection and privacy regulations, such as GDPR, HIPAA, or regional laws, ensuring the ethical integrity of the research. To illustrate the practical application of security measures and AI integration, real-world case studies were also included. These case studies highlighted how security measures can enhance the security and privacy of IoT devices and demonstrate the effectiveness of AI-based solutions in real-world settings. The research will culminate in the development of recommendations for securing IoT devices in the AI era, along with suggestions for future research directions. The findings will be validated through experimental simulations to ensure their credibility and relevance. In the final phase, the research findings, analysis results, case studies, and recommendations will be presented in a comprehensive research manuscript, which will conclude with a summary of the research outcomes and their implications for the future of IoT security.

## 3. Background Research and Investigative Exploration for Available Knowledge

The Internet of Things (IoT) represents a rapidly growing network of interconnected devices, each equipped with sensors, processing capabilities, and software that enable them to communicate and exchange data [1,2,3]. These devices, ranging from everyday household objects to industrial machinery, interact via the Internet or other communication networks [4,5,6]. Contrary to its name, IoT devices do not necessarily require a connection to the public internet; instead, they are often connected to private or local networks, with each device being individually addressable. This vast and ever-expanding network of devices, spanning diverse fields such as electronics, computer science, and communication engineering, is revolutionizing industries and reshaping everyday life [7,8,9]. The evolution of IoT has been fueled by the convergence of multiple technological advancements. In particular, the proliferation of ubiquitous computing, miniaturized sensors, powerful embedded systems, and sophisticated machine learning algorithms have paved the way for a new era of various intelligent, connected devices [1-11]. This technological synergy has enabled IoT applications to spread across a wide array of sectors, including consumer electronics, healthcare, industrial automation, and urban infrastructure. Among the most prominent applications are "smart home" systems, which allow users to manage various household devices such as lighting, heating, and security systems through smartphones or voice assistants. These systems, which embody the essence of convenience and energy efficiency, are at the forefront of IoT adoption in consumer markets.

However, as IoT technologies proliferate, they bring with them a series of challenges, particularly regarding security and privacy. Given that IoT devices are often involved in the collection and transmission of sensitive data, concerns about their vulnerability to cyberattacks and unauthorized data access have become paramount. To mitigate these risks [11-22], both industry players and government bodies have been actively working on establishing a set of international and local standards, guidelines, and regulatory frameworks. These efforts aim to ensure the responsible deployment of IoT technologies, protecting users' privacy while fostering the continued growth of the IoT ecosystem. The roots of IoT trace back to the early 1980s when the idea of a network of interconnected devices began to take shape. However, it was not until 1999 that the term "Internet of Things" was coined by Kevin Ashton, who envisioned a system in which devices embedded with radio-frequency identification (RFID) tags could communicate with each other and with humans [13-25]. This concept was the precursor to the modern-day IoT landscape, which is now populated with a wide variety of sensors, actuators, and interconnected devices. Over the years, IoT has continued to evolve, benefiting from advancements in wireless communication technologies, cloud computing, and data analytics. Today, IoT devices range from simple sensors that monitor environmental conditions to complex medical devices that remotely monitor patient health, contributing to a digital transformation in healthcare and other sectors.

IoT applications are vast and varied, impacting numerous industries and sectors. In consumer markets, IoT devices are widely used in connected vehicles, smart home devices, wearables, and healthcare applications. The healthcare sector, in particular, has seen significant transformations due to IoT, with devices such as wearable health monitors and remote patient monitoring systems enhancing patient care and streamlining medical workflows [16-26]. Within organizations, the concept of "Enterprise IoT" refers to IoT devices and systems deployed for business operations, such as asset tracking and supply chain management. In the medical domain, the Internet of Medical Things (IoMT) plays a crucial role in improving healthcare outcomes by enabling the real-time collection and analysis of health data. Devices in the IoMT range from simple health monitoring devices to more advanced implants, such as pacemakers, that actively monitor and manage patient health.

Transportation is another sector in which IoT is having a profound impact. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication are fundamental technologies for enabling autonomous driving and improving road safety. Beyond the automotive industry, IoT is being applied in agriculture, environmental monitoring, maritime operations, and infrastructure management, where it improves efficiency, safety, and resource optimization.

In the military, the Internet of Military Things (IoMT) incorporates IoT devices such as sensors, wearable biometrics, and unmanned systems for surveillance, reconnaissance, and combat operations. Additionally, IoT is transforming energy management systems, where connected devices optimize energy consumption, contribute to smart grid initiatives, and support sustainability efforts [22-30]. The application of IoT in environmental monitoring and urban management further exemplifies its wide-ranging impact, with IoT-based systems being used to monitor air quality, traffic conditions, and waste management in cities.

One of the most compelling trends in IoT is the integration of artificial intelligence (AI) and autonomous control. Traditionally, IoT devices were designed to gather and transmit data, but advancements in machine learning and deep reinforcement learning are enabling these devices to make intelligent decisions and act autonomously. Companies like Intel and others are working to combine IoT with AI capabilities, allowing IoT devices to adapt to dynamic environments, make real-time decisions, and optimize operations without human intervention [13-33]. This evolution marks a significant step toward creating truly "smart" IoT devices capable of performing complex tasks autonomously. As machine learning and AI technologies mature, they will continue to push the boundaries of what IoT devices can achieve, enabling new use cases across various sectors.

At the architectural level, IoT systems typically consist of three main layers: devices, edge gateways, and the cloud. Devices, which include sensors and actuators, collect data from the environment. Edge gateways serve as intermediaries, aggregating and pre-processing the data before transmitting it to the cloud. The cloud layer hosts IoT applications and databases that store sensor data, allowing for further analysis and decision-making. This multi-tiered architecture enables efficient operation and data processing, with each layer performing specialized tasks to optimize the overall system's performance. To manage the surge in IoT devices and their data traffic, network architectures must be highly scalable, leveraging technologies such as IPv6, 6LoWPAN, and MQTT protocols. Additionally, edge computing and fog computing are emerging solutions that help alleviate the strain on centralized cloud systems by processing data closer to the source, thus reducing latency and improving responsiveness for time-sensitive applications.

As IoT technology evolves, it faces numerous challenges, including platform fragmentation and the need for interoperability across diverse devices and protocols. The lack of standardized communication protocols and differing hardware architectures among IoT devices complicates the development of seamless applications. Security remains a critical concern, as vulnerabilities in IoT devices can lead to cyberattacks, data breaches, and physical safety risks.

Privacy issues also loom large, with the widespread collection of personal data raising concerns about surveillance and the potential misuse of sensitive information. Moreover, IoT devices generate massive amounts of data that need to be processed and stored, creating challenges related to data management and environmental sustainability. The need for secure, interoperable systems and robust data management solutions is critical to the widespread adoption of IoT technologies. Despite these challenges, the potential of IoT to revolutionize industries and improve lives remains immense. From smart cities to autonomous vehicles, healthcare advancements to environmental sustainability, IoT is opening up new possibilities for innovation and efficiency. As the technology continues to mature, it will undoubtedly lead to even greater integration of intelligent, connected systems that will redefine how we interact with the world around us.

## 4. IoT and its associated Security Challenges

The Internet of Things (IoT) represents an increasingly vast and diverse network of connected devices that go beyond just computers and smartphones. This ecosystem encompasses everything from home appliances to industrial machinery, all of which are susceptible to cyber threats. As the number of connected devices grows, so does the risk of cybercriminals exploiting vulnerabilities within this network, putting user data and system integrity at significant risk. Given the scale and complexity of IoT, securing it from cyberattacks is paramount.

Security breaches in IoT systems can have wide-ranging consequences, impacting both virtual and physical environments. For example, a smart car could be hacked, compromising essential safety features, or a device in a hospital could be manipulated, endangering patient care. In industries relying on the Industrial Internet of Things (IIoT), cyberattacks could disrupt critical infrastructure, causing catastrophic damage. Similarly, IoT devices in smart homes can be exploited to monitor private activities, raising serious privacy concerns. The interconnected nature of these systems makes them a prime target for malicious actors.

Several key challenges contribute to IoT security concerns:

1. Insufficient Testing and Development: Many manufacturers prioritize speed to market over security, resulting in devices with weak or overlooked security features. These devices often lack adequate security updates, leaving them vulnerable to exploitation. However, awareness around IoT security has prompted improvements in device safety over time.

2. Default Passwords and Brute-Forcing: Many IoT devices come with default, often weak passwords. Users frequently fail to change these, leaving the devices open to brute-force attacks and password hacking, which can give cybercriminals unauthorized access.

3. IoT Malware and Ransomware: The proliferation of IoT devices has led to an increase in malware and ransomware attacks. Malicious actors often use IoT botnets to carry out large-scale attacks, compromising devices and using them as part of distributed denial of service (DDoS) assaults.

4. Data Privacy Concerns: IoT devices collect vast amounts of data from users. Often, users do not fully understand the implications of agreeing to terms of service, which can result in their personal data being shared with third parties, raising significant privacy issues.

5. Escalated Cyberattacks: Infected IoT devices can be hijacked and used as part of DDoS attacks or to spread malware across networks, amplifying the scale and impact of cyberattacks on businesses and individuals alike.

6. Insecure Interfaces: Many IoT devices lack proper encryption and data authentication in their interfaces, making them vulnerable to exploitation. These security gaps can provide attackers with easy access to sensitive data or the ability to control devices remotely.

7. Remote Working Vulnerabilities: The rise of remote work during the COVID-19 pandemic has exposed new IoT security vulnerabilities. Home networks are often less secure than organizational networks, making them easier targets for cyberattacks, especially as more devices are connected to home Wi-Fi.

8. Complex Security Configurations: As homes and businesses adopt more connected devices, managing IoT security becomes increasingly complex. A single misconfiguration or overlooked vulnerability in one device can compromise the entire network, making it crucial to properly configure and monitor each device.

To ensure the safety and privacy of users, as well as the integrity of IoT systems across industries, addressing these security challenges is critical. Effective IoT security requires ongoing awareness, proactive measures, and continuous improvements in device development, user practices, and network protections.

## 5. Ensuring Security Practices for IoT Breaches

IoT security breaches have become more common, highlighting the vulnerabilities inherent in connected devices. Notable incidents include the 2016 Mirai botnet attack, which used compromised IoT devices to launch massive DDoS attacks, temporarily shutting down services like Spotify, Netflix, and PayPal. In 2018, the VPNFilter malware infected hundreds of thousands of routers, allowing attackers to gather sensitive information and steal passwords. The automotive industry faced a similar challenge when a cybersecurity expert hacked a Tesla Model X in less than two minutes using a Bluetooth vulnerability. Additionally, in 2021, hackers gained access to Verkada's security cameras, compromising 150,000 live feeds from public sector and corporate buildings.

To strengthen the security of IoT devices and networks, users should follow several key best practices:

1. Keep Firmware and Software Updated: Regularly updating your IoT devices' firmware and software is crucial for patching known vulnerabilities and enhancing device security.

2. Change Default Passwords: Many IoT devices come with default, often weak passwords. Changing these to strong, unique passwords for each device can help prevent unauthorized access.

3. Secure Your Wi-Fi Network: Use strong encryption protocols, like WPA2, to secure your Wi-Fi network. Consider creating a separate guest network for visitors to minimize the risk of unauthorized access.

4. Review Privacy Settings: Regularly examine and adjust privacy settings on your IoT devices to control the data they collect, share, and store. Disabling unused device features can also reduce potential attack surfaces.

5. Enable Multi-Factor Authentication (MFA): MFA adds an extra layer of protection to your devices. Enabling this feature where available is highly recommended to prevent unauthorized access.

6. Understand Your IoT Devices: Familiarize yourself with all the IoT devices on your network, and consider upgrading to newer models with enhanced security features when necessary.

7. Use VPNs for Remote Access: When managing IoT devices remotely over public Wi-Fi networks, use a Virtual Private Network (VPN) to encrypt your data and protect it from potential threats.

By implementing these best practices, users can significantly reduce the risks posed by IoT security breaches and better protect their privacy and sensitive data from cyberattacks.

## 6. 6G Solutions, Architecture Deployments for IoT

The growing presence of Internet of Things (IoT) devices, spanning from smartphones and smart cars to home appliances, has ushered in a new era of connectivity and innovation across industries such as transportation, healthcare, and smart cities. The upcoming sixth-generation (6G) networks are set to revolutionize IoT, enabling high-speed, high-capacity data exchange among billions of connected devices and applications. These advanced networks will overcome the limitations of current fifth-generation (5G) technologies, meeting the demands of an increasingly connected digital ecosystem. However, the rapid expansion of IoT devices raises significant security concerns.

Many of these devices store sensitive user data and are often remotely accessible, making them prime targets for cyberattacks. Among the many threats, botnets stand out as a particularly significant risk. In 2021, the emergence of BotenaGo, a new botnet designed to target millions of IoT devices, highlighted the growing severity of these attacks. Botnets serve as powerful tools for spamming, phishing, data theft, and launching distributed denial-of-service (DDoS) attacks, exacerbating security challenges. The traditional IoT architecture, which consists of the perception, network, and application layers, faces difficulties in delivering comprehensive security solutions. To address these challenges, innovative approaches powered by software-defined networking (SDN), network function virtualization (NFV), and infrastructure virtualization are critical. SDN, by decoupling the control and data planes, enhances network flexibility and programmability, allowing for more efficient and dynamic management of IoT networks. Meanwhile, NFV supports service-oriented, scalable IoT infrastructures, enabling flexible and efficient deployment of network functions. Together, these technologies can better manage the complexities of IoT networks, enabling robust security measures and improving the resilience of 6G-enabled IoT ecosystems.

The integration of artificial intelligence (AI), particularly machine learning (ML), with SDN brings new possibilities for intelligent and adaptive network monitoring. By combining ML with SDN, networks can achieve enhanced reconfigurability, security, and intelligence, which strengthens IoT security. Deep learning (DL), a subset of ML, is particularly promising for IoT security due to its ability to identify unknown threats by uncovering hidden patterns and correlations in large datasets. However, current ML/DL-based intrusion detection systems (IDSs) face challenges in scaling effectively to handle the rapid growth of IoT devices, leading to high network load and latency issues. Emerging technologies like fog computing, mobile edge computing (MEC), and edge intelligence (EI) offer additional promise in securing massive IoT deployments in 6G environments. Edge computing, a foundational component of 6G networks, helps reduce latency and alleviate network congestion by processing data closer to the edge of the network, rather than relying solely on centralized cloud servers. When combined with EI, these technologies create a robust and flexible platform for intelligent security services, providing effective defense mechanisms against cyber threats while enhancing scalability and automation. As the design of 6G networks evolves, there is an increasing need for a flexible and adaptive security architecture that meets the unique requirements of massive IoT systems. This exploration aims to bridge the gap in existing knowledge by examining the integration of intelligent networking technologies and ML/DL-based solutions for attack detection and mitigation. By reviewing the key enablers, AI applications, and the challenges of scaling ML/DL-based IDSs, this research highlights the importance of securing massive IoT networks within the 6G ecosystem. This investigation also provides insight into future trends, emerging solutions, and the growing need for innovative technologies to safeguard the rapidly expanding world of IoT devices in the upcoming 6G era. To visualize these concepts, Figure 1 provides an overview of the integration of 6G solutions with IoT security architecture.

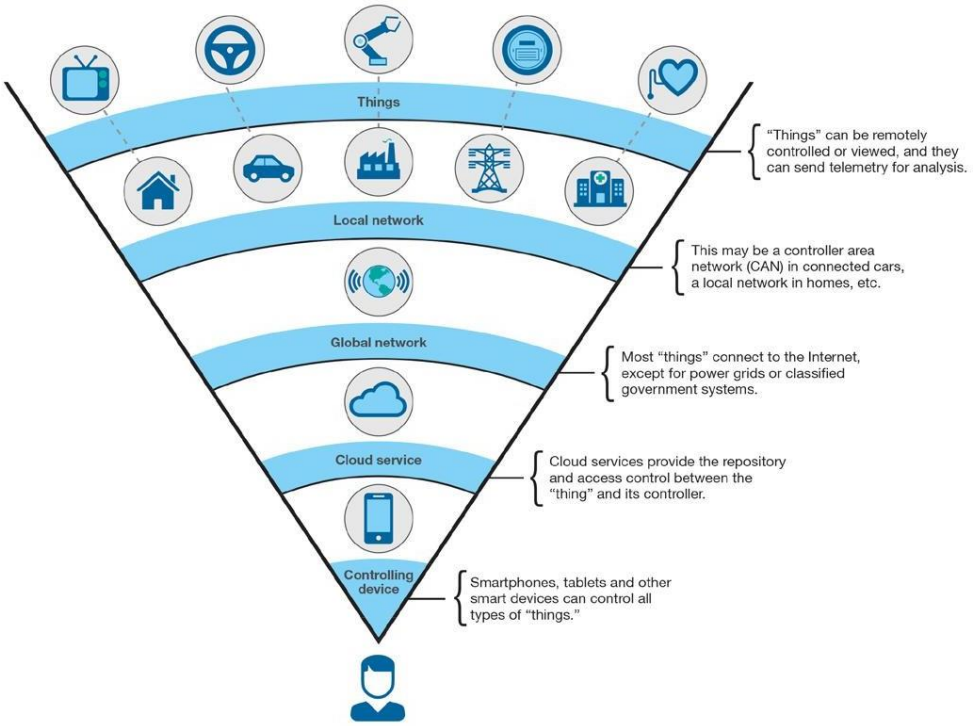



**FIGURE 1:** The Visual Representation of the IOT Architecture and its Deployable Solutions.

## 7. Case Studies Analysis: IoT Security, AI Integrations

The Internet of Things (IoT) is transforming various industries by enabling the seamless exchange of data between interconnected devices. Its ability to automate processes and facilitate real-time communication is revolutionizing sectors like healthcare, where IoT is playing a crucial role in enhancing patient care, improving health outcomes, and increasing access to healthcare services. However, the widespread adoption of IoT in healthcare also brings with it significant security, privacy, and safety concerns that affect both patients and healthcare professionals. As IoT devices become more integral to healthcare systems, protecting sensitive medical data and ensuring the integrity of these devices is of utmost importance. Despite ongoing research, the integration of secure IoT solutions in healthcare settings remains a critical area of focus.

One promising development in healthcare IoT is Narrowband IoT (N.B. IoT), which is recognized for its energy-efficient capabilities. N.B. IoT is especially valued in the healthcare sector for its ability to monitor and measure patient data over long distances, making it ideal for low-power, wide-area applications such as remote patient monitoring. However, challenges related to security and system performance must be addressed to ensure its effectiveness in healthcare environments. The protection of healthcare data, along with maintaining privacy, is paramount in this context. With IoT linking a vast array of medical devices and systems, safeguarding sensitive data from attacks such as spoofing, denial of service (DoS), jamming, and eavesdropping is a complex task that requires robust security frameworks.

Machine learning (ML) techniques, such as supervised learning, unsupervised learning, and reinforcement learning, are emerging as key tools to enhance the security of IoT networks. These AI-driven methods can be employed to authenticate devices, control access, ensure data integrity, and detect potential threats in real time. By leveraging machine learning algorithms, healthcare providers can monitor the security of IoT devices, identifying vulnerabilities and mitigating risks before they cause significant damage.

The economic impact of IoT applications by 2025 is expected to be transformative, particularly in sectors like healthcare, smart cities, and building management systems. These environments rely on IoT-enabled sensor data and intelligent systems to provide innovative services that significantly impact both business and the broader economy. Among these, the market for smart city services is poised for rapid growth, as IoT devices contribute to more efficient, sustainable, and connected urban environments. Nevertheless, challenges remain, particularly concerning communication, data management, scalability, security, and interoperability. A key hurdle in the widespread adoption of IoT is the lack of standardized protocols, which complicates interoperability between devices and systems. As IoT technologies continue to advance, addressing the need for unified standards and seamless communication between diverse devices will be essential. Additionally, the complexity of securing an IoT ecosystem, given its vast scale and variety, has made machine learning and deep learning (DL) techniques increasingly vital. These AI-based technologies are effective at detecting and responding to security threats, thus enhancing the reliability and user experience of IoT networks.

The integration of machine learning in securing IoT networks is particularly crucial for industries like healthcare, where data privacy and security are non-negotiable. By applying ML and DL techniques, healthcare organizations can not only improve the security of their IoT infrastructure but also drive greater innovation in patient care and service delivery. The continued development of these technologies will be essential to unlock the full potential of IoT while ensuring the safety and privacy of its users. To provide a clearer understanding of this dynamic, Figure 2 presents a visual representation of the integration of IoT security measures and AI applications in healthcare.


**FIGURE 2:** An Illustration of IoT Security in terms of AI Perspectives.

## 8. Framework Models: Experimental Developments

Blockchain technology is becoming increasingly integral to improving the security, data sharing, and efficiency of Internet of Things (IoT) services. As the number of terminal devices in IoT networks continues to rise, concerns regarding the vulnerability of individual devices have emerged. Blockchain technology offers a promising solution to these concerns by enhancing security through robust access control and authentication mechanisms. Rather than requiring individual authentication for each device, users can authenticate once via the blockchain and then utilize smart contract tokens for subsequent access to the system. This approach not only simplifies authentication but also strengthens security, while enabling additional features such as fingerprint verification.

In the IoT context, confidentiality and data reliability are particularly critical, especially in sensitive fields like healthcare, where safeguarding personal data is essential. Blockchain technology is being utilized to provide distributed storage and tamper resistance for IoT data, ensuring that the integrity and confidentiality of data are preserved. This includes innovative data storage methods and consensus algorithms that further enhance the security and reliability of IoT data.

Another significant area where blockchain is making an impact is IoT data sharing. IoT devices generate vast amounts of heterogeneous data from various sensors across different sectors, which creates a need for secure and efficient data sharing. Blockchain enables the development of decentralized platforms that allow for trustless data sharing, effectively eliminating the need for centralized intermediaries. This decentralization not only improves data sharing efficiency by reducing redundancy but also ensures the integrity and reliability of the shared data. To further improve the efficiency of IoT services, researchers are exploring strategies to balance the demand for computing resources with the available resources. Techniques such as cooperative computing, cache capacity optimization, and game theory-based resource allocation are being applied to optimize the use of computing resources in IoT networks. These approaches aim to maximize the efficiency of data processing, ensuring that IoT services remain responsive and scalable as networks grow.

Blockchain technology is reshaping the landscape of edge-enabled IoT services by addressing key security challenges, enabling secure and efficient data sharing, and optimizing resource allocation. These advancements contribute to the overall reliability and effectiveness of IoT networks, ensuring that they can operate securely and efficiently in an increasingly interconnected world. To provide a clearer understanding of this framework, Figure 3 presents a diagrammatic representation of the deployed model and its experimental developments, which involves multiple steps and algorithmic processes.

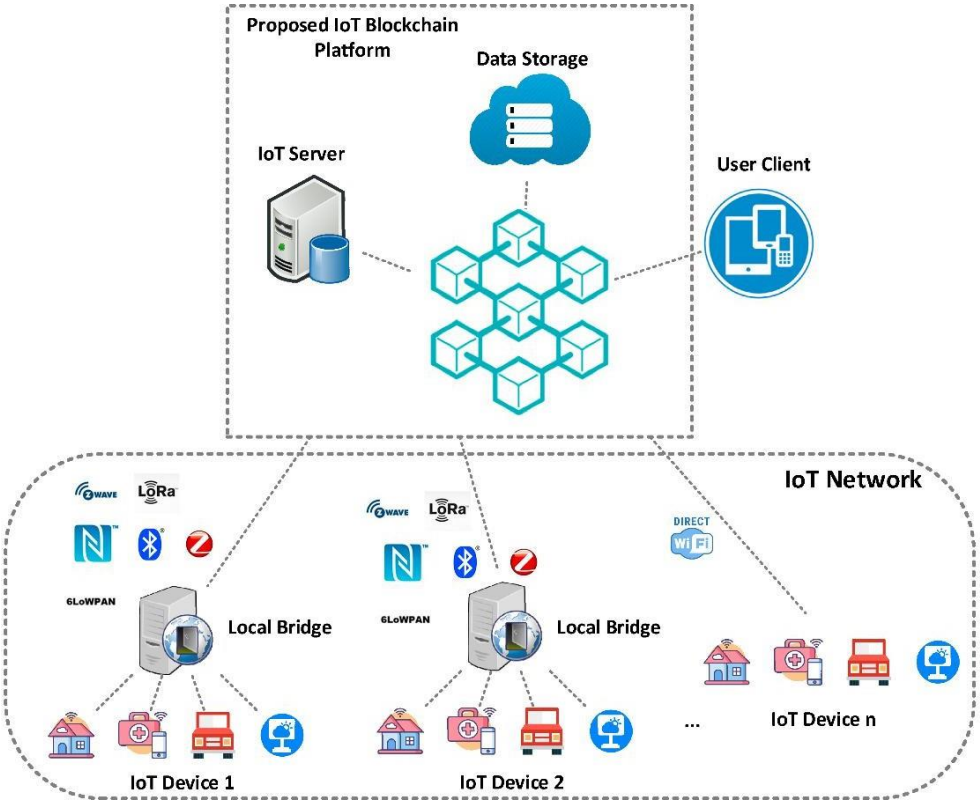



**FIGURE 3:** A Diagram of the Framework Model Experimentation.

## 9. Results and Findings

Securing Internet of Things (IoT) services with Artificial Intelligence (AI) offers immense potential, but it also presents significant challenges and unresolved issues that must be addressed. Machine Learning (ML)-based security frameworks have emerged as promising solutions for enhancing IoT security.

However, these frameworks face critical limitations, such as high computational and communication costs. Many ML-based schemes require large datasets and computationally intensive feature extraction, making them impractical for resource-constrained IoT environments. There is a clear and urgent need for more efficient ML-based security mechanisms that can operate effectively in such conditions. Subfields of ML, such as Deep Learning (DL) and Reinforcement Learning (RL), have demonstrated potential in improving IoT security. However, DL models are prone to overfitting and require extensive training data, while RL models struggle during the initial learning phases, especially when handling real-time attacks. To mitigate these limitations, the development of reliable backup security systems is essential to complement ML-based methods, ensuring robust and continuous protection even during system failures or learning delays.

Integrating ML with blockchain technology presents another avenue for strengthening IoT security. Blockchain's decentralized architecture addresses trust issues among IoT devices, enhancing overall security. However, this integration also introduces new challenges, such as double-spending and majority attacks. ML techniques can help detect and counter these threats, but further research is required to seamlessly and securely merge ML and blockchain in IoT applications.

Privacy concerns represent another significant challenge when employing blockchain in IoT systems. Private blockchains and encryption technologies are commonly used to address these concerns, but they often restrict the availability of training data for privacy-focused ML models. This restriction can reduce the effectiveness of these models in real-world implementations, highlighting the need to balance privacy protection with ML-based security efficacy. Developing strategies that maintain privacy while ensuring the performance of ML systems is critical for advancing IoT security.

From the experimental framework model and simulation, several key findings were identified. These findings provide insight into the effectiveness, limitations, and potential improvements of the proposed approaches. Different technologies have different roles in a protocol stack. The provided descriptions are the presentation of the roles of the several popular communication technologies within IoT applications. A comprehensive summary of these results and findings are presented in Tables 1, 2, 3 offering a clear and concise overview of the outcomes and their implications for the advancement of AI-driven IoT security solutions.

**TABLE 1:** The challenges and proposed solutions/approaches in securing IoT services with AI, particularly ML-based security frameworks, and the integration with blockchain.

| Category | Challenge/Limitation | Proposed Solution/Approach | Notes/Further Research Needed |
|---|---|---|---|
| **ML-based IoT Security** | High computational and communication costs | Efficient ML-based security mechanisms | Need for mechanisms practical for resource-constrained IoT environments |
| **ML-based IoT Security** | Large datasets and computationally intensive feature extraction | Efficient ML-based security mechanisms | Many ML-based schemes are impractical for resource-constrained IoT |
| **Deep Learning (DL)** | Prone to overfitting | - | Requires extensive training data |
| **Reinforcement Learning (RL)** | Struggles during initial learning phases | - | Especially when handling real-time attacks |
| **General ML Limitations** | System failures or learning delays | Reliable backup security systems | Essential to complement ML-based methods for robust, continuous protection |
| **ML & Blockchain Integration** | Trust issues among IoT devices | Blockchain's decentralized architecture | Enhances overall security |
| **ML & Blockchain Integration** | Double spending attacks (in blockchain) | ML techniques to detect and counter | Further research required for seamless and secure merger |
| **ML & Blockchain Integration** | Majority attacks (in blockchain) | ML techniques to detect and counter | Further research required for seamless and secure merger |
| **Privacy in Blockchain IoT** | Restricting training data availability for privacy-focused ML models | Private blockchains and encryption technologies (common practice) | Reduces effectiveness of ML models in real-world implementations |
| **Privacy in Blockchain IoT** | Balancing privacy protection with ML-based security efficacy | Strategies to maintain privacy while ensuring ML system performance | Critical for advancing IoT security |

**TABLE 2:** Securing 6G-enabled massive IoT networks using AI and advanced networking enablers.

| Category | Technology | Role/Contribution to 6G IoT Security | Key Benefit/Mechanism |
|---|---|---|---|
| **AI Technologies** | Artificial Intelligence (AI) | Combats IoT security threats, identifies, analyzes, and mitigates attacks in real-time | Transformative force, forms comprehensive and robust framework |

| | | | |
|---|---|---|---|
| **AI Technologies** | Machine Learning (ML) | Detects anomalies, including previously unknown or zero-day attacks | Learns from diverse/complex datasets, identifies patterns and correlations in heterogeneous IoT data |
| **AI Technologies** | Deep Learning (DL) | Detects anomalies, including previously unknown or zero-day attacks | Learns from diverse/complex datasets, identifies patterns and correlations in heterogeneous IoT data |
| **Networking Enablers** | Software-Defined Networking (SDN) | Provides centralized network control for ML/DL algorithms | Enables ML/DL to monitor and respond to threats across the network |
| **Networking Enablers** | Edge Intelligence (EI) | Brings computational capabilities closer to the data source | Enables real-time analysis and faster threat mitigation |
| **Networking Enablers** | Network Function Virtualization (NFV) | Enhances security through increased adaptability, scalability, and precision | (Implicit in integration with AI) |
| **Networking Enablers** | Quantum Computing (QC) | Offers potential for unbreakable encryption and rapid threat analysis | Further strengthens IoT network security |
| **Networking Enablers** | Network Slicing (NS) | Ensures critical IoT applications operate in isolated and secure virtual networks | Provides secure environments for specific applications |
| **Networking Enablers** | Mobile Edge Computing (MEC) | Brings computational capabilities closer to the data source | Enables real-time analysis and faster threat mitigation |
| **Networking Enablers** | Fog Computing | Supports distributed security solutions | Facilitates broader security coverage |
| **Overall Approach** | Integration of AI with Cutting-Edge Networking Technologies | Addresses complex security challenges of 6G-enabled IoT | Provides a scalable, adaptive, and efficient approach for robust protection against evolving cyber threats |

There are various domains and data sources from which investigations are included and used for the conduction of the experimental framework model deployment. Table 4 provides details and clarification for further references.

**TABLE 3:** The Findings from the Framework Model.

| Protocol | Physical | Link / MAC | Network | Transport | Application |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| **Bluetooth LE** | Yes | Yes | Yes | Yes | Yes |
| **Z-Wave** | No | No | Yes | Yes | Yes |
| **ITU-T G.9959** | Yes | Yes | No | No | No |
| **Zigbee** | No | No | Yes | Yes | Yes |
| **Matter** | No | No | No | No | Yes |
| **TCP and UDP** | No | No | No | Yes | No |
| **Thread** | No | No | Yes | No | No |
| **IEEE 802.15.4** | Yes | Yes | No | No | No |
| **IPv6** | No | No | Yes | No | No |
| **Ethernet** | Yes | Yes | No | No | No |
| **Wi-Fi** | Yes | Yes | No | No | No |

**TABLE 4:** The Technical Standards in terms of IoT Security.

| Short name | Long name | Standards under development | Other notes |
|---|---|---|---|
| Auto-ID Labs | Auto Identification Center | Networked RFID (radiofrequency identification) and emerging sensing technologies | |

| | | | |
|---|---|---|---|
| Connected Home over IP | Project Connected Home over IP | Connected Home over IP (or Project Connected Home over IP) is an open-sourced, royalty-free home automation connectivity standard project which features compatibility among different smart home and Internet of things (IoT) products and software | The Connected Home over IP project group was launched and introduced by Amazon, Apple, Google,[R] Comcast and the Zigbee Alliance on December 18, 2019.[196] The project is backed by big companies and by being based on proven Internet design principles and protocols it aims to unify the currently fragmented systems.[R] |
| EPCglobal | Electronic Product code Technology | Standards for adoption of EPC (Electronic Product Code) technology | |
| FDA | U.S. Food and Drug Administration | UDI (Unique Device Identification) system for distinct identifiers for medical devices | |
| GS1 | Global Standards One | Standards for UIDs ("unique" identifiers) and RFID of fast-moving consumer goods (consumer packaged goods), health care supplies, and other things The GS1 digital link standard,[R] first released in August 2018, allows the use QR Codes, GS1 Datamatrix, RFID and NFC to enable various types of business-to-business, as well as business-to-consumers interactions. | Parent organization comprises member organizations such as GS1 US |
| IEEE | Institute of Electrical and Electronics Engineers | Underlying communication technology standards such as IEEE 802.15.4, IEEE P1451-99[R] (IoT Harmonization), and IEEE P1931.1 (ROOF Computing). | |
| IETF | Internet Engineering Task Force | Standards that comprise TCP/IP (the Internet protocol suite) | |
| MTConnect Institute | — | MTConnect is a manufacturing industry standard for data exchange with machine tools and related industrial equipment. It is important to the IIoT subset of the IoT. | |
| O-DF | Open Data Format | O-DF is a standard published by the Internet of Things Work Group of The Open Group in 2014, which specifies a generic information model structure that is meant to be applicable for describing any "Thing", as well as for publishing, updating and querying information when used together with O-MI (Open Messaging Interface). | |
| O-MI | Open Messaging Interface | O-MI is a standard published by the Internet of Things Work Group of The Open Group in 2014, which specifies a limited set of key operations needed in IoT systems, notably different kinds of subscription mechanisms based on the Observer pattern. | |
| OCF | Open Connectivity Foundation | Standards for simple devices using CoAP (Constrained Application Protocol) | OCF (Open Connectivity Foundation) supersedes OIC (Open Interconnect Consortium) |
| OMA | Open Mobile Alliance | OMA DM and OMA LWM2M for IoT device management, as well as GotAPI, which provides a secure framework for IoT applications | |
| XSF | XMPP Standards Foundation | Protocol extensions of XMPP (Extensible Messaging and Presence Protocol), the open standard of instant messaging | |

| | | | |
|---|---|---|---|
| W3C | World Wide Web Consortium | Standards for bringing interoperability between different IoT protocols and platforms such as Thing Description, Discovery, Scripting API and Architecture that explains how they work together. | |

## 10. Discussions

Securing networks against malicious cyberattacks in the context of 6G-enabled massive IoT presents a critical and complex challenge. Traditional network architectures and security measures often fall short in addressing the advanced and evolving security threats within this dynamic ecosystem. This necessitates the development of innovative solutions and architectural paradigms tailored to the unique demands of 6G-enabled IoT networks. Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), has emerged as a transformative force in combating IoT security threats. These technologies provide powerful tools for identifying, analyzing, and mitigating attacks in real time. When combined with advanced networking enablers such as Software-Defined Networking (SDN), Edge Intelligence (EI), Network Function Virtualization (NFV), Quantum Computing (QC), Network Slicing (NS), Mobile Edge Computing (MEC), and Fog Computing, AI technologies form a comprehensive and robust framework for securing 6G-enabled massive IoT environments.

ML and DL are especially valuable due to their ability to adapt and learn from diverse and complex datasets. These techniques excel in detecting anomalies, including previously unknown or zero-day attacks, by identifying patterns and correlations within heterogeneous data generated by IoT devices. Furthermore, their integration with networking enablers enhances security through increased adaptability, scalability, and precision in threat detection. For instance, SDN enables centralized network control, providing a platform for ML and DL algorithms to monitor and respond to threats across the network. Edge Intelligence (EI) and MEC bring computational capabilities closer to the data source, enabling real-time analysis and faster threat mitigation. Network Slicing ensures that critical IoT applications operate in isolated and secure virtual networks, while Fog Computing supports distributed security solutions. Quantum Computing offers the potential for unbreakable encryption and rapid threat analysis, further strengthening IoT network security. The integration of AI with cutting-edge networking technologies presents a paradigm shift in securing massive IoT networks in the 6G era. These advancements provide a scalable, adaptive, and efficient approach to addressing the complex security challenges of 6G-enabled IoT, ensuring robust protection against evolving cyber threats.

## 11. Conclusions

The integration of advanced technologies such as Artificial Intelligence (AI) and Edge Computing (EC) offers transformative potential in enhancing the security and performance of Internet of Things (IoT) services. By addressing the limitations of traditional cloud-based systems, EC introduces a novel computational paradigm that significantly enhances the IoT ecosystem, enabling faster, localized data processing and real-time threat detection. This research underscores the importance of privacy and security as critical enablers for high-quality IoT services and explores how cutting-edge technologies can address the evolving cybersecurity landscape in the 6G-enabled massive IoT era.

The study highlights the critical role of AI, particularly Machine Learning (ML) and Deep Learning (DL), in identifying and mitigating security threats through intelligent, adaptive systems capable of recognizing patterns and anomalies in complex datasets. Furthermore, the research emphasizes the synergy between AI and key networking technologies, including Software-Defined Networking (SDN), Network Function Virtualization (NFV), Quantum Computing (QC), Network Slicing (NS), Mobile Edge Computing (MEC), and Fog Computing. These technologies collectively empower IoT networks with enhanced flexibility, scalability, and efficiency in securing massive IoT deployments. In addition, blockchain technology emerges as a robust solution for ensuring data integrity, trustless interactions, and decentralized security in IoT environments.

The collaborative integration of blockchain and AI further strengthens IoT security by addressing challenges such as privacy protection, cryptographic resilience, and efficient data sharing. However, the investigation also reveals several open challenges and issues, such as the computational demands of AI-driven security mechanisms, the need for robust privacy-preserving frameworks, and the complexity of seamlessly integrating diverse technologies. Addressing these challenges is critical to unlocking the full potential of AI and EC in securing IoT services. This research establishes a foundation for leveraging AI and EC to revolutionize IoT security. The fusion of advanced computational paradigms, intelligent algorithms, and cutting-edge networking enablers provides a comprehensive approach to safeguarding IoT services in the dynamic and evolving landscape of 6G-enabled IoT networks. Continued innovation and interdisciplinary collaboration will be essential in addressing the remaining challenges and driving the next wave of advancements in IoT security.

### Supplementary information

The various original data sources, some of which are not all publicly available, because they contain various types of private information. The available platform provided data sources that support the exploration findings, and information of the research investigations is referenced where appropriate.

### Acknowledgments

The authors would like to acknowledge and thank GOOGLE DeepMind Research with its associated pre-print access platforms. This research exploration was investigated under the platform provided by GOOGLE DeepMind which is under the support of GOOGLE Research and GOOGLE Research Publications within the GOOGLE Gemini platform. Using their provided platform of datasets and database-associated files with digital software layouts consisting of free web access to a large collection of recorded models that are found within research access and its related open-source software distributions, which is the implementation for the proposed research exploration that was undergone and set in motion. There are many data sources, some of which are resourced and retrieved from a wide variety of GOOGLE service domains as well. All the data sources which have been included and retrieved for this research are identified, mentioned and referenced where appropriate.

**Funding**
No Funding was provided for the conduction concerning this research.

**Conflict of interest/Competing interests**
There are no Conflict of Interest or any type of Competing Interests for this research.

**Ethics approval**
The authors declare no competing interests for this research.

**Consent to participate**
The authors have read, approved the manuscript and have agreed to its publication.

**Consent for publication**
The authors have read, approved the manuscript and have agreed to its publication.

**Availability of data and materials**
The various original data sources some of which are not all publicly available, because they contain various types of private information. The available platform provided data sources that support the exploration findings and information of the research investigations are referenced where appropriate.

**Code availability**
Mentioned in detail within the Acknowledgements section.

**Authors' contributions**
Described in details within the Acknowledgements section.

**References**
[1] Ullah, I., Adhikari, D., Su, X., Palmieri, F., Wu, C., & Choi, C. (2025). Integration of data science with the intelligent IoT (IIoT): Current challenges and future perspectives. *Digital Communications and Networks*, *11*(2), 280-298.

[2] Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, *9*(1), 28-78.

[3] Hosny, K. M., El-Hady, W. M., & Samy, F. M. (2025). Technologies, Protocols, and applications of Internet of Things in greenhouse Farming: A survey of recent advances. *Information Processing in Agriculture*, *12*(1), 91-111.

[4] Abu-Jassar, A. T., Attar, H., Amer, A., Lyashenko, V., Yevsieiev, V., & Solyman, A. (2025). Remote Monitoring System of Patient Status in Social IoT Environments Using Amazon Web Services Technologies and Smart Health Care. *International Journal of Crowd Science*, *9*(2), 110-125.

[5] Rahman, A., Islam, J., Kundu, D., Karim, R., Rahman, Z., Band, S. S., ... & Kumar, N. (2025). Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: Present perspectives and future directions. *International Journal of Communication Systems*, *38*(1), e5429.

[6] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 1-18.

[7] Kokila, M., & Reddy, S. (2025). Authentication, access control and scalability models in Internet of Things Security–A review. *Cyber Security and Applications*, *3*, 100057.

[8] Sun, P., Wan, Y., Wu, Z., Fang, Z., & Li, Q. (2025). A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions. *Computers & Security*, *148*, 104097.

[9] Nikpour, M., Yousefi, P. B., Jafarzadeh, H., Danesh, K., Shomali, R., Asadi, S., ... & Ahmadi, M. (2025). Intelligent energy management with iot framework in smart cities using intelligent analysis: An application of machine learning methods for complex networks and systems. *Journal of Network and Computer Applications*, *235*, 104089.

[10] Sinha, P., Sahu, D., Prakash, S., Yang, T., Rathore, R. S., & Pandey, V. K. (2025). A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning. *Scientific Reports*, *15*(1), 9684.

[11] Nguyen, H. P., Le, P. Q. H., Pham, V. V., Nguyen, X. P., Balasubramaniam, D., & Hoang, A. T. (2025). Application of the Internet of Things in 3E (efficiency, economy, and environment) factor-based energy management as smart and sustainable strategy. *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, *47*(1), 9586-9608.

[12] Rahmani, A. M., Haider, A., Moghaddasi, K., Gharehchopogh, F. S., Aurangzeb, K., Liu, Z., & Hosseinzadeh, M. (2025). Self-learning adaptive power management scheme for energy-efficient IoT-MEC systems using soft actor-critic algorithm. *Internet of Things*, *31*, 101587.

[13] Ficili, I., Giacobbe, M., Tricomi, G., & Puliafito, A. (2025). From sensors to data intelligence: Leveraging IoT, cloud, and edge computing with AI. *Sensors*, *25*(6), 1763.

[14] Wang, L., Zhang, C., Zhao, Q., Zou, H., Lasaulce, S., Valenzise, G., ... & Debbah, M. (2025). Generative ai for rf sensing in iot systems. *IEEE Internet of Things Magazine*, *8*(2), 112-120.

[15] Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and man-in-the-middle attacks. *Security and Privacy*, *8*(2), e70016.

[16] Kumar, P., Jolfaei, A., & Islam, A. N. (2025). An enhanced Deep-Learning empowered Threat-Hunting Framework for software-defined Internet of Things. *Computers & Security*, *148*, 104109.

[17] Najim, A. H., Al-sharhanee, K. A. M., Al-Joboury, I. M., Kanellopoulos, D., Sharma, V. K., Hassan, M. Y., ... & Abbas, A. H. (2025). An IoT healthcare system with deep learning functionality for patient monitoring. *International Journal of Communication Systems*, *38*(4), e6020.

[18] Kapoor, A. (2025). *Hands-On Artificial Intelligence for IoT: Expert machine learning and deep learning techniques for developing smarter IoT systems*. Packt Publishing Ltd.

[19] Lai, Q., & Hua, H. (2025). Secure medical image encryption scheme for Healthcare IoT using novel hyperchaotic map and DNA cubes. *Expert Systems with Applications*, *264*, 125854.

[20] Vankdothu, R., & Hameed, M. A. (2025). An Effective Congestion and Interference Secure Routing Protocol for Internet of Things Applications in Wireless Sensor Network. *Wireless Personal Communications*, *140*(1), 143-161.

[21] Sadhwani, S., Mathur, A., Muthalagu, R., & Pawar, P. M. (2025). 5G-SIID: an intelligent hybrid DDoS intrusion detector for 5G IoT networks. *International Journal of Machine Learning and Cybernetics*, *16*(2), 1243-1263.

[22] Dhumpati, R., Velpucharla, T. R., Bhagyalakshmi, L., & Anusha, P. V. (2025). Analyzing the Vulnerability of Consumer IoT Devices to Sophisticated Phishing Attacks and Ransomware Threats in Home Automation Systems. *Journal of Intelligent Systems & Internet of Things*, *15*(1).

[23] Dritsas, E., & Trigka, M. (2025). Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications. *Journal of Sensor and Actuator Networks*, *14*(1), 9.

[24] Saheed, Y. K., Omole, A. I., & Sabit, M. O. (2025). GA-mADAM-IIoT: A new lightweight threats detection in the industrial IoT via genetic algorithm with attention mechanism and LSTM on multivariate time series sensor data. *Sensors International*, *6*, 100297.

[25] Sizan, N. S., Dey, D., Layek, M. A., Uddin, M. A., & Huh, E. N. (2025). Evaluating Blockchain Platforms for IoT Applications in Industry 5.0: A Comprehensive Review. *Blockchain: Research and Applications*, 100276.

[26] Ntayagabiri, J. P., Bentaleb, Y., Ndikumagenge, J., & El Makhtoum, H. (2025). OMIC: A Bagging-Based Ensemble Learning Framework for Large-Scale IoT Intrusion Detection. *Journal of Future Artificial Intelligence and Technologies*, *1*(4), 401-416.

[27] Chai, X., Lee, B. G., Hu, C., Pike, M., Chieng, D., Wu, R., & Chung, W. Y. (2025). IoT-FAR: A multi-sensor fusion approach for IoT-based firefighting activity recognition. *Information Fusion*, *113*, 102650.

[28] Seifi, N., Keshavarz, M., Kalhor, H., Shahrakipour, S., & Adibifar, A. (2025). Ranking of criteria affecting the implementation readiness of Internet of Things in industries using TISM and fuzzy TOPSIS analysis. *Journal of Operations Intelligence*, *3*(1), 46-66.

[29] Jamshidi, S., Nikanjam, A., Nafi, K. W., Khomh, F., & Rasta, R. (2025). Application of deep reinforcement learning for intrusion detection in Internet of Things: A systematic review. *Internet of Things*, 101531.

[30] Qasim, M., & Sajid, M. (2025). An efficient IoT task scheduling algorithm in cloud environment using modified Firefly algorithm. *International Journal of Information Technology*, *17*(1), 179-188.

[31] *Sentinel Intelligence: Cybersecurity at the Intersection of AI and Innovation,* (2025). Elivapress.com. https://www.elivapress.com/en/book/book-6507392846/

[32] Z. Bin Akhtar, "Artificial Intelligence (AI) within the Realm of Cyber Security," *Insight. Electr. Electron. Eng.*, vol. 1, no. 1, pp. 1-11, 2024.

[33] Zarif Bin Akhtar. Securing the Future of Mobility: Understanding the Security Perspectives of Cybersecurity, Operating Systems (OS) Security, Mobile Computing. Open Access Journal of Computer Science and Engineering, 2024; 1(1): 51-66.