Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.057877

REVIEW

Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity

Ali Hassan[1], **N. Nizam-Uddin**[2], **Asim Quddus**[3], **Syed Rizwan Hassan**[4], **Ateeq Ur Rehman**[5,*] **and Salil Bharany**[6]

[1]Department of Electrical Engineering, HITEC University, Taxila, 47080, Pakistan

[2]Department of Biomedical Engineering, HITEC University, Taxila, 47080, Pakistan

[3]Department of Electronics Engineering, University of Chakwal, Chakwal, 48800, Pakistan

[4]Department of Computer Science, NFC Institute of Engineering and Fertilizer Research, Faisalabad, 38000, Pakistan

[5]School of Computing, Gachon University, Seongnam-si, 13120, Republic of Korea

[6]Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, 140401, Punjab, India

*Corresponding Author: Ateeq Ur Rehman. Email: 202411144@gachon.ac.kr

Received: 29 August 2024 Accepted: 11 November 2024 Published: 19 December 2024

ABSTRACT

Enhancing the interconnection of devices and systems, the Internet of Things (IoT) is a paradigm-shifting technology. IoT security concerns are still a substantial concern despite its extraordinary advantages. This paper offers an extensive review of IoT security, emphasizing the technology's architecture, important security elements, and common attacks. It highlights how important artificial intelligence (AI) is to bolstering IoT security, especially when it comes to addressing risks at different IoT architecture layers. We systematically examined current mitigation strategies and their effectiveness, highlighting contemporary challenges with practical solutions and case studies from a range of industries, such as healthcare, smart homes, and industrial IoT. Our results highlight the importance of AI methods that are lightweight and improve security without compromising the limited resources of devices and computational capability. IoT networks can ensure operational efficiency and resilience by proactively identifying and countering security risks by utilizing machine learning capabilities. This study provides a comprehensive guide for practitioners and researchers aiming to understand the intricate connection between IoT, security challenges, and AI-driven solutions.

KEYWORDS

Internet of Things (IoT); artificial intelligence (AI); IoT architecture; security; attacks in IoT

1 Introduction

In recent years, the concept of the internet has been progressively expanding its influence across all facets of life [1]. Researchers face the intricate challenge of uncovering the optimal extent of internet utilization. Over time, the term "Internet" has evolved to encompass "things," giving rise to the concept of the Internet of Things (IoT) [2]. As the name implies, objects are interconnected through various technologies, such as wireless sensor networks (WSNs), radio-frequency identification (RFID), Bluetooth, near-field communication (NFC), long-term evolution (LTE), 5G, and other sophisticated communication methods [3]. Therefore, the IoT can be defined as the interconnection of things via the internet, facilitating the transfer of information collected from diverse devices to specific destinations online. Despite its current status as a significant technological term, the IoT has yet to fully realize its inherent potential.

IoT applications encompass smart cities, connected devices, automobiles, healthcare solutions, residences, agriculture, education, industry and entertainment setups, etc., [4]. According to Cisco's research, approximately 500 billion devices are projected to utilize sensors and establish internet connectivity by the year 2030 [5]. The IoT serves as the network that facilitates data communication among these devices. The extensive interconnection of devices to the internet and the significant volume of accompanying data give rise to a plethora of issues within the IoT domain [6]. These issues encompass interoperability, standardization, scalability, infrastructure constraints, complexity, analytics and data management, and security [7–9]. However, this paper specifically focuses on addressing the IoT security aspect. Table 1 presents the literature that highlights the challenges associated with the IoT.

Security, inherently, is a methodology aimed at ensuring protection to the extent that it aligns with user advancements and implementation levels, constituting a pivotal objective. This underscores the inquiry into the manner in which safety considerations are often integrated into the later stages of development and debugging in numerous contemporary IoT device implementations and design instances [10]. Security requisites might ultimately emerge through the identification of access provisions to production environments and, conceivably, other developmental necessities.

IoT security pertains to the level of safeguarding or resilience exhibited by IoT applications and their underlying infrastructure. These devices have emerged as susceptible targets owing to their heavy reliance on external resources, often leading to situations where they are left unattended. Once the network layer is compromised, cyber attackers and hackers find it considerably difficult to gain unauthorized access and control over a device [11]. This compromised device can then be utilized to launch attacks on neighbouring devices via the compromised network node. A recent study conducted by the Hewlett-Packard revealed that 70% of all internet-connected devices are alarmingly vulnerable to potential attacks.

As the landscape of the IoT continues to evolve, security remains a persistent concern, and new challenges continue to emerge. Despite this, this era is poised to introduce fresh opportunities for the development of novel techniques aimed at enhancing the security of IoT devices [12]. Existing methods for securing the IoT often fail to address the novel security risks that the evolving IoT infrastructure may confront [13]. Consequently, these techniques struggle to identify vulnerabilities or pre-empt attacks originating from within the IoT ecosystem. Furthermore, only a limited number of studies have explored the comprehensive layers of the IoT infrastructure as unified entities. Table 1 summarizes the key findings from the state-of-the-art and pinpoints the precise knowledge gaps that still exist in the field. Through a critical analysis of these works, we can identify the need for improved security measures that are specific to the various architectures of IoT systems. Every item emphasizes the important findings gained from earlier studies as well as the unaddressed gaps that demand more research. Our study intends to close these gaps by offering a thorough analysis of IoT security, investigating critical security characteristics, architectural weaknesses, and the application of artificial intelligence in creating robust security solutions.

Table 1: Issues related to the security of the IoT as discussed in the literature

Ref.	Year	Key points	Evolution trend	Research gaps identified	Research gaps unaddressed	Link to current study
[14]	2024	This study investigated the security challenges associated with IoT systems and explored various AI techniques for improving their protection. By categorizing challenges into device-level security, network security, data security, privacy, and ethical considerations, it underscored the complex nature of IoT security in the realm of AI.	Transition to IoT security with an AI focus, addressing complex problems at all security levels.	AI's limited real-world applications in IoT environments.	There is no empirical validation for AI frameworks on various IoT devices.	Our study highlights the potential of AI in IoT security, particularly in Sections 7 and 8, offering examples of its practical implementation.
[15]	2024	Examines the effects of IoT on daily life, emphasizing major security issues and the application of Machine Learning (ML) and Deep Learning (DL) techniques.	A focus on incorporating ML/DL into IoT security to improve threat detection and real-time data processing.	Inadequate incorporation of ML/DL techniques into current IoT architectures.	Need for clarity on operationalization of ML/DL methods in practical settings.	Our study integrates AI-driven solutions in Section 8, detailing methods like supervised and unsupervised learning.
[16]	2024	Inspects the effects of Distributed Denial of Service (DDoS) attacks on IoT and suggests methods for mitigation and detection.	Research on IoT-focused DDoS mitigation using AI-based threat detection is being expanded.	Less attention paid to preventive actions before attacks happen.	IoT-specific gaps in predictive threat assessment techniques.	In Section 5, our study looks at current attacks to provide context for preventative IoT security solutions.
[17]	2024	This study examines IoT security research through the lenses of firmware security, access control, blockchain technology, AI, communication protocols, and privacy protection laws.	Expanded IoT security, using blockchain and AI to improve privacy and trust.	Insufficiently thorough mitigation approaches in various IoT environments.	Lack of a unified architecture that addresses vulnerabilities on all kinds of devices.	In Section 2, we provide an overview of IoT architecture; in Section 3, we address important security characteristics, highlighting particular vulnerabilities and their fixes.

(Continued)

Table 1 (continued)

Ref.	Year	Key points	Evolution trend	Research gaps identified	Research gaps unaddressed	Link to current study
[18]	2023	Explores the problems with IoT authentication and data integrity.	Initially, inter-disciplinary IoT security frameworks are discussed to solve data integrity issues.	Inadequate multidisciplinary methods for IoT security.	Research gaps in combining IoT security with more comprehensive cybersecurity frameworks. The author has not explored AI methods.	In Section 3, we go over important security elements from our analysis. Also, in Section 8 we revealed the potential of AI in IoT security.
[19]	2023	Examines IoT security measures including intrusion detection and encryption.	Transition to IoT security measures that are centred on usability.	Insufficient attention to usability when designing security measures.	User experience and security measures must be balanced.	In Section 7, we examine real-world case studies that assess usability in addition to security aspects.
[20]	2023	Examines security flaws in all IoT architecture layers.	Focus on vulnerabilities in IoT architecture that are specific to a layer.	In-depth knowledge of vulnerabilities particular to each layer is required.	Not enough case studies demonstrating weaknesses in different architectures.	In Section 2, our analysis maps vulnerabilities to specific layers and offers comprehensive insights into IoT design.
[21]	2023	Examines a model for user authentication for cloud-based IoT scenarios.	Dynamic trust model development for IoT of Things scenarios.	Restricted models of trust in dynamic situations.	Requirement for strong trust models that can change with IoT scenarios.	In Section 3, we address authentication in the IoT offering improved solutions for changing circumstances.
[22]	2023	Emphasizes that the most important security precaution for IoT is authentication.	Enhanced focus on thorough authentication across various IoT architectures.	Insufficiently comprehensive authentication remedies a range of architectures.	Not enough information about how to integrate authentication methods on different IoT platforms.	Section 3 of our study highlights the significance of authentication mechanisms.

(Continued)

Table 1 (continued)

Ref.	Year	Key points	Evolution trend	Research gaps identified	Research gaps unaddressed	Link to current study
[23]	2023	Examines IoT security issues while highlighting AI's contribution to improved communication protocols.	Growing interest in using AI to improve protocols.	Empirical research proving AI's usefulness in practical settings is necessary.	In practical IoT security scenarios, limited validation of AI solutions is conducted.	In Section 8, our study provides example case studies that highlight AI's usefulness and highlight its significance for IoT security.
[12]	2022	The growth of IoT has brought with it serious security flaws, as connected objects can be targets of cyberattacks that harm people's physical, financial, and health conditions.	Initial investigation of unified security frameworks that combine feasible countermeasures.	IoT device security is still a challenge for IoT makers, which results in serious flaws in a variety of application areas.	Unified frameworks that combine practical countermeasures with security objectives are required for a variety of IoT systems.	This study closes this gap by looking at IoT design, spotting vulnerabilities at different IoT layer levels in Section 2, and suggesting AI-powered fixes to protect IoT applications in the future in Section 8.
[24]	2021	Reveals the security issues related to the layers and protocols of the IoT architecture.	A thorough understanding of the necessity of protocol-specific security measures.	Inadequate investigation of customized security measures for particular protocols.	Insufficient thorough analyses of security measures.	In Sections 2 and 6, we go into detail on the architecture of IoT, offering customized security solutions.

1.1 Motivation

The world of the IoT is in its evolutionary phase, fitting itself into every domain and part of our lives but bothering everyone that these interconnected devices are safe enough. The sheer growth of the IoT, which has permeated everything from smart homes and healthcare to industrial automation and critical infrastructure, presents a limitless surface area for attack that might have far-reaching outcomes. IoT devices are increasingly vulnerable to cyberattacks, data breaches, and malicious exploits since they manage enormous volumes of sensitive data and regulate essential systems. Many IoT systems are dangerously vulnerable due to poor encryption, weak security measures, and inconsistent updating policies. The challenge of protecting IoT networks against refined, dynamic threats is made more difficult by the intricacy and diversity of these ecosystems.

The motivation of this study is to dive deep into the core of IoT security. The fundamental architecture, crucial security features, common attack vectors, and revolutionary potential of AI-driven solutions are examined. We aim to highlight novel research directions and highlight important vulnerabilities by offering a thorough analysis.

1.2 Methodology

This section outlines the process we employed to conduct cutting-edge research. The main purpose of this study is to address the following research questions:

- **RQ1:** What are the fundamental architectural components of IoT systems, and how do they influence the overall design and effectiveness of key security features?
- **RQ2:** What are the various prevalent and recent attacks that target IoT systems, and how can these attacks be effectively countered by existing and emerging security measures?
- **RQ3:** What are current challenges in IoT security, and how do practical case studies elaborate the effectiveness of various solutions?
- **RQ4:** What emerging trends of AI in IoT security shape the future of connectivity?

The RQ1 covers Sections 2 and 3, RQ2 covers Sections 4 and 5, RQ3 addresses Sections 6 and 7 while RQ4 spans Section 8. The aforementioned research questions are addressed via the extraction of crucial evidence from several databases, such as Google Scholar, IEEE, Wiley, Springer, MDPI, Elsevier, and Research Gate, etc. On the basis of keywords such as "IoT security, IoT and AI, IoT architecture, attacks on the IoT, features of the IoT, and the future of AI in the IoT", the most pertinent and excellent papers were chosen from a wide body of literature that was available in multiple databases. A number of the papers were eliminated from the analysis due to methodologies or applications that were duplicated, not expanded upon, or already applied in other contexts. The abbreviations used in this review can be found in Table 2.

Table 2: List of abbreviations

Description	Abbreviation	Description	Abbreviation
Internet of Things	IoT	Local Area Network	LAN
Artificial Intelligence	AI	Wide Area Network	WAN
Wireless Sensor Networks	WSN	Low Power Wide Area Networks	LP-WANs
Universal Mobile Telecommunications Service	UMTS	Zonal Intercommunication Global-standard	ZigBee
Wireless Fidelity	WIFI	Long Term Evolution	LTE
Near-Field Communication	NFC	Service Oriented Architecture	SOA
Long Term Evolution	LTE	Quality of Service	QoS
Radio-Frequency Identification	RFID	Machine-to-Machine	M2M
Global Positioning System	GPS	Personal Digital Assistants	PDAs
Quick Response	QR	Electromagnetic Interference	EMI
Intrusion Detection Systems	IDS	Hardware Security Modules	HSMs
Intrusion Prevention Systems	IPS	Denial of Service	DoS
Electromagnetic Compatibility	EMC	Distributed Denial of Service	DDoS
Man-in-the-Middle	MitM	Security Aware Routing	SAR
Secure Socket Layer	SSL	Transport Layer Security	TLS
Topology Graph Based Anomaly detection	TOGBAD	Optimized Link State Routing	OLSR
Ad Hoc On-Demand Distance Vector Security Extension	AODVSEC	Synchronize	SYN
User Datagram Protocol	UDP	Structured Query Language	SQL
Cross-Site Scripting	XSS	Structured Query Language Injection	SQLi

(Continued)

Table 2 (continued)

Description	Abbreviation	Description	Abbreviation
Extensible Markup Language	XML	Web Application Firewall	WAF
Simple Object Access Protocol	SOAP	Hypertext Mark-up Language	HTML
Content Delivery Networks	CDNs	Role-Based Access Control	RBAC
Multi-Factor Authentication	MFA	Address Space Layout Randomization	ASLR
Access Control List	ACLs	Digital Video Recorders	DVRs
Data Breach Investigations Report	DBIR	Vertrieb, Aufladung, Reparatur Transportabler Akkumulatoren	VARTA
United Kingdom	UK	Asia–Pacific	APAC
Federal Bureau of Investigation	FBI	Argonaut RISC Core	ARC
Information Commissioner’s Office	ICO	Network Video Recorders	NVRs
Asea Brown Boveri	ABB	Decentralized Identity Systems	DIS
Industrial IoT	IIoT	Post-Decision State	PDS
Machine Learning	ML	Deep Learning	DL
Deep Neural Networks	DNNs	Malicious Activities Recognition in Water-based IIoT	MARWIIoT
Deep Q-Network	DQN	Artificial Neural Network	ANN
Support Vector Machines	SVMs	K-Nearest Neighbours	KNN
Over-the-Air	OTA	Internet Engineering Task Force	IETF
Advanced Detection Technology	ADT	Health Insurance Portability and Accountability Act	HIPAA
Virtual Private Networks	VPNs	Transport Layer Security	TLS
Federated Learning	FL	Unmanned Aerial Vehicles	UAVs
Base Stations	BSs	Explainable AI	XAI
Generative AI	GenAI	Variational Autoencoders	VAEs
Trusted Execution Environments	TEEs	Generative Adversarial Networks	GANs

1.3 Contributions

To guide future research and stimulate innovation in protecting the interconnected IoT world, this study is an invaluable resource for researchers, experts, and decision-makers in the field of AI and IoT security. Several noteworthy additions to the field are made by this thorough survey:

- **Comprehensive Assessment of IoT Security Concerns:** This study assesses the security concerns prevalent in IoT devices and simultaneously evaluates the privacy challenges inherent in IoT applications.
- **In-Depth Analysis of IoT Architectures and Vulnerabilities:** It explores several IoT technologies and architectural frameworks, methodically locating security and privacy flaws in the IoT ecosystem. It provides a clear picture of how each layer is exposed to various threats by offering a thorough, classified breakdown of attacks studied via the perspective of the IoT’s layered architecture.
- **Examination of Recent Cyberattacks on IoT Systems:** It sheds light on a few recent attacks that have sparked concerns regarding the security of IoT technologies. These examples provide the vulnerability of this quickly developing technology and highlight the necessity for more robust defences.

- **Identification of Current Challenges and Real-World Solutions:** In addition to outlining the problems that IoT security is now experiencing, this study offers feasible, real-world solutions. It offers a practical method for resolving these problems and contains thorough examples and case studies that show how these solutions are being applied in diverse circumstances.
- **Exploration of AI-Driven Security Enhancements:** It provides a thorough analysis of the ways in which AI is now being used to protect IoT systems in a variety of industries, such as industrial IoT, smart grids, smart homes, smart cities, healthcare, and smart agriculture. With specific examples, it demonstrates how AI may be used to improve IoT security in real-world scenarios.
- **Projection of AI's Role in Future IoT Security:** The study examines how various AI strategies will increasingly influence IoT security in the future. It goes over how to create predictive models and adaptable security measures using supervised, unsupervised, and reinforcement learning techniques. The significance of Explainable AI (XAI) in guaranteeing transparency and trust in AI-powered security systems is also emphasized in the article. Moreover, it explores how Generative AI (GenAI) can be used to develop fresh approaches to security, which makes AI a vital instrument for addressing new IoT security issues. With the ongoing advancement of technology, these sophisticated AI techniques are expected to become indispensable for maintaining the security of IoT devices.

1.4 Organization

The rest of the paper is organized as follows: Section 2 discusses the IoT architecture, revealing its distinct layers. Section 3 underscores the crucial security features of the IoT. Section 4 explores various attacks targeting each IoT layer. In Section 5, recent attacks on IoT technology are examined. Section 6 presents the current challenges in IoT security and their possible solutions. Section 7 presents the practical case studies and examples, Section 8 emphasizes the power of AI in enhancing IoT security, and Section 9 provides the study's conclusions. The overall organization of the paper is presented in Fig. 1.

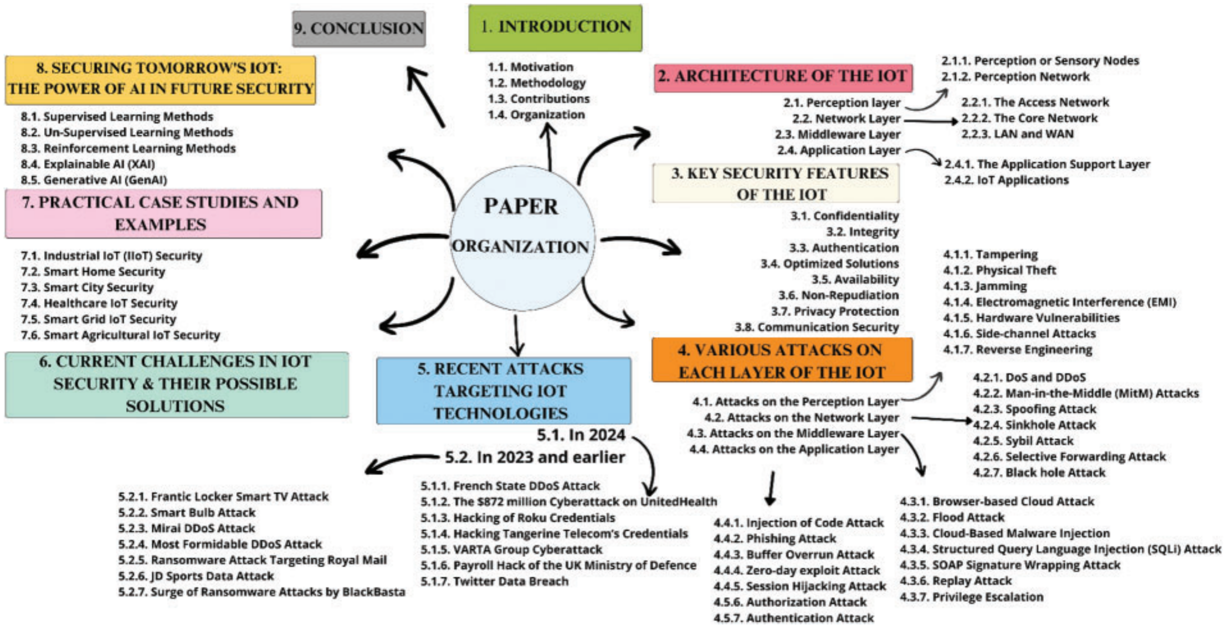

9. CONCLUSION
1. INTRODUCTION
1.1. Motivation
1.2. Methodology
1.3. Contributions
1.4. Organization
8. SECURING TOMORROW'S IOT: THE POWER OF AI IN FUTURE SECURITY
8.1. Supervised Learning Methods
8.2. Un-Supervised Learning Methods
8.3. Reinforcement Learning Methods
8.4. Explainable AI (XAI)
8.5. Generative AI (GenAI)
2. ARCHITECTURE OF THE IOT
2.1. Perception layer
2.2. Network Layer
2.3. Middleware Layer
2.4. Application Layer
2.1.1. Perception or Sensory Nodes
2.1.2. Perception Network
2.2.1. The Access Network
2.2.2. The Core Network
2.2.3. LAN and WAN
2.4.1. The Application Support Layer
2.4.2. IoT Applications
PAPER ORGANIZATION
7. PRACTICAL CASE STUDIES AND EXAMPLES
7.1. Industrial IoT (IIoT) Security
7.2. Smart Home Security
7.3. Smart City Security
7.4. Healthcare IoT Security
7.5. Smart Grid IoT Security
7.6. Smart Agricultural IoT Security
3. KEY SECURITY FEATURES OF THE IOT
3.1. Confidentiality
3.2. Integrity
3.3. Authentication
3.4. Optimized Solutions
3.5. Availability
3.6. Non-Repudiation
3.7. Privacy Protection
3.8. Communication Security
4.1.1. Tampering
4.1.2. Physical Theft
4.1.3. Jamming
4.1.4. Electromagnetic Interference (EMI)
4.1.5. Hardware Vulnerabilities
4.1.6. Side-channel Attacks
4.1.7. Reverse Engineering
6. CURRENT CHALLENGES IN IOT SECURITY & THEIR POSSIBLE SOLUTIONS
5. RECENT ATTACKS TARGETING IOT TECHNOLOGIES
5.1. In 2024
5.2. In 2023 and earlier
4. VARIOUS ATTACKS ON EACH LAYER OF THE IOT
4.1. Attacks on the Perception Layer
4.2. Attacks on the Network Layer
4.3. Attacks on the Middleware Layer
4.4. Attacks on the Application Layer
4.2.1. DoS and DDoS
4.2.2. Man-in-the-Middle (MitM) Attacks
4.2.3. Spoofing Attack
4.2.4. Sinkhole Attack
4.2.5. Sybil Attack
4.2.6. Selective Forwarding Attack
4.2.7. Black hole Attack
5.2.1. Frantic Locker Smart TV Attack
5.2.2. Smart Bulb Attack
5.2.3. Mirai DDoS Attack
5.2.4. Most Formidable DDoS Attack
5.2.5. Ransomware Attack Targeting Royal Mail
5.2.6. JD Sports Data Attack
5.2.7. Surge of Ransomware Attacks by BlackBasta
5.1.1. French State DDoS Attack
5.1.2. The $872 million Cyberattack on UnitedHealth
5.1.3. Hacking of Roku Credentials
5.1.4. Hacking Tangerine Telecom's Credentials
5.1.5. VARTA Group Cyberattack
5.1.6. Payroll Hack of the UK Ministry of Defence
5.1.7. Twitter Data Breach
4.4.1. Injection of Code Attack
4.4.2. Phishing Attack
4.4.3. Buffer Overrun Attack
4.4.4. Zero-day exploit Attack
4.4.5. Session Hijacking Attack
4.5.6. Authorization Attack
4.5.7. Authentication Attack
4.3.1. Browser-based Cloud Attack
4.3.2. Flood Attack
4.3.3. Cloud-Based Malware Injection
4.3.4. Structured Query Language Injection (SQLi) Attack
4.3.5. SOAP Signature Wrapping Attack
4.3.6. Replay Attack
4.3.7. Privilege Escalation

Figure 1: Overall paper organization

2 Architecture of the IoT

Architecture is the structured framework that delineates the physical elements of a network and its functional arrangement and setup, encompassing its operational principles, procedures, and data formats employed in its functioning [25]. In the context of the IoT, it serves as the foundational structure that empowers the comprehensive functionality of the IoT system as a whole. The IoT architecture encompasses an assemblage of physical entities, sensors, cloud services, developers, actuators, communication layers, users, business layers, and IoT protocols [26]. Owing to the extensive scope of the IoT, there is no universally accepted consensus on a single IoT architecture. Various researchers have proposed different architectural models to address the diverse facets of the IoT [27]. According to the majority of researchers, IoT architecture is commonly conceptualized as consisting of primary layers: perception, network, middleware, and application layers [20,22], as shown in Fig. 2.

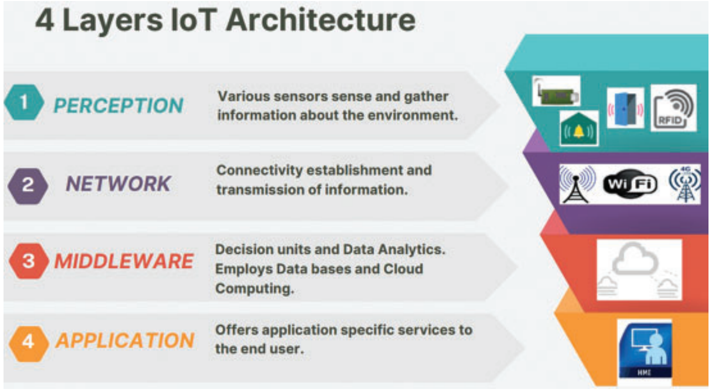

4 Layers IoT Architecture
1 PERCEPTION
Various sensors sense and gather information about the environment.
2 NETWORK
Connectivity establishment and transmission of information.
3 MIDDLEWARE
Decision units and Data Analytics. Employs Data bases and Cloud Computing.
4 APPLICATION
Offers application specific services to the end user.
RFID
Wi Fi
HMI

Figure 2: Layers of IoT architecture

2.1 *Perception Layer*

The perception layer, alternatively known as the recognition layer, sensory layer, or device layer, resides as the lowest tier in the IoT architecture. It encompasses technologies dedicated to several essential functions, including sensing (the collection of data from the surrounding environment and its transmission to databases, data warehouses, or the cloud), identification (discerning objects on the basis of their unique assigned identities), actuation (executing mechanical actions in response to the recognized data), and transmission (creating connections between diverse smart devices) with minimal human intervention [17]. This layer is distinguished primarily by its capacity to capture true information and represent it in digital form. The perception layer can be further split into two sublayers on the basis of its intended function: Perception nodes are also known as sensory nodes and perception networks.

2.1.1 Perception or Sensory Nodes

Physical devices, including controllers, actuators, sensors, and more, are included in this category of components. These devices have the ability to establish various types of networks, including *ad hoc* networks, mesh networks, or multihop environments, with the aim of increasing scalability and expediting deployment [28]. On the basis of the technology that drives them, such physical devices can take various forms, including global positioning system (GPS) devices, quick response (QR) codes or barcode readers, RFID readers, Bluetooth-enabled devices, and a range of sensors such as temperature, humidity, and light. Their primary function is to gather information from the environment, identify objects, manage data, and control objects. Depending on the type of device employed, the collected information can pertain to various object characteristics, such as their position, closeness, humidity, temperature, pollution concentrations, and other environmental factors. RFID readers, for instance, are employed to identify objects on the basis of data retrieved from associated tags. Object control is the process of controlling a device's operating settings to change its capabilities as needed. For example, it is possible to program a sensor device to remain in low-power doze mode until it detects an activity or an event, at which point it switches to an active mode to capture relevant information. Microchips embedded within objects that are not directly perceivable are programmed to intelligently sense their environment. This is where nanotechnology plays a crucial role, ensuring that the chip's design is sufficiently compact to be integrated within the body of these objects.

2.1.2 Perception Network

This network assumes the responsibility of communicating with the network layer, transportation layer, or transmission network. The information gathered by the perception nodes is safely sent to the gateways for further transmission. It also makes it easier for control signals to be transmitted to the controller devices, using both wireless and wired communication channels as necessary.

2.2 Network Layer

The network layer, which can also be referred to as the transportation layer or the transmission network, serves as an intermediary between the sensory perception network and the application layers. Its function is to serve as a hub for a variety of outdated networks, protocols, and technologies. Its primary goal is to make it easier for data gathered by perception nodes to be transmitted over wireless and wired communication channels to the data processing unit or advanced units that make decisions [29]. This transmission enables tasks such as data analysis, data mining, data aggregation, and data encoding. Additionally, it plays a crucial role in network management functionality. Depending on its specific functions, it can be categorized into three sublayers: the access network, the core network, and the local and wide area network [30].

2.2.1 The Access Network

The access network creates a widespread connection for the things used to sense and collect data. It is like a bridge between us, the users, and the services we rely on. This network sets up various ways for us to connect, such as mobile, satellite, and wireless communications, so we can stay connected and get things done. The IoT can use different types of access networks, such as *ad hoc* networks; GPRS networks; and 2G and 3G networks such as UMTS, Wi-Fi, ZigBee, and Bluetooth. Now, when we talk about the superfast internet for our mobile devices, we have 4G-LTE and 5G. These are the fancy new standards that ensure that we can browse and stream without any lag [31]. Access networks can be set up in different ways, depending on whether they have a central station or base station. Wi-Fi, for example, has a central setup where one main device connects everything, whereas an *ad hoc* network is more like a group of devices connecting directly to each other without a central hub.

2.2.2 The Core Network

The core network is similar to the big internet, and it forms the foundation of the IoT. Its main job is to send data to all of us who are using the internet through the access network, which is similar to the gateway to the Web. The core network is considered the central part of any communication system, similar to the backbone that holds everything together. It is where all the information and services flow through. One cool thing about the internet is that it allows us to connect all types of devices, even those with limited resources [17]. The internet can be used for all kinds of purposes, whether for the public, businesses, or the government. It can work over short distances or long distances, giving us the ability to keep an eye on and control physical objects from far away.

2.2.3 Local Area Network (LAN) and Wide Area Network (WAN)

A local area network (LAN) is similar to a network of devices in a small area. Devices in a LAN can talk directly to each other, and if they want to talk to devices in other places, they use gateways to help them. Think of it as a combination of infrastructure, such as roads, and access services, such as vehicles, that allow devices in a local area to connect and communicate.

On the other hand, wide area networks (WANs) are similar to networks that cover larger areas. They spread across larger geographical areas, such as highways connecting cities. Currently, low-power wide area networks (LP-WANs) are receiving much attention because they are good at connecting devices that do not use much power [32].

2.3 Middleware Layer

The primary objectives of the middleware layer encompass integrating services and application operations to establish a cost-effective platform. Additionally, it oversees service management, communication, data exchange, and storage management. The middleware layer also plays a crucial role in promoting service discovery to locate entities capable of offering the required services and information. Moreover, it determines the most suitable service to fulfil a given request and identifies trust mechanisms for carefully extracting, analysing, and utilizing data from services. This layer facilitates interactions between services, fostering a trustworthy framework. The cloud serves as an excellent example of this concept, providing hardware, software platforms, protocols, and applications and offering storage and analysis capabilities for IoT data.

Owing to the diversity and complexity of the IoT architecture, this layer encounters a multitude of security challenges. These challenges become even more pronounced in cloud computing, involving issues such as user authentication, security concerns, and privacy protection [33]. Moreover, ensuring the availability of cloud services is vital. Users also seek clarity about who manages their data and its storage location. Additionally, they want assurance that cloud service providers cannot misuse or unlawfully access their data.

2.4 Application Layer

The application layer is similar to the top floor of the IoT building, and it is the part that you, as an end user, interact with. Its goal is to handle and offer applications that can be used all around the world on the basis of the information gathered by the perception layer and processed by the information processing unit. Think of it as the place where you get access to customized services over the internet using your smartphones, tablets, and other devices. It is further subdivided into two parts: the application support layer and the IoT applications, each of which plays a role in ensuring that the services you need are met.

2.4.1 The Application Support Layer

This layer sits right above the network layer in the IoT architecture. Its main goal is to assist various business services and perform smart calculations and data processing. It is similar to a filter that checks data to determine if it is valid, invalid, potentially harmful, malicious, or just spam

[17]. To make things work smoothly, it uses service-oriented architecture (SOA). This helps ensure that things such as quality of service (QoS) and directory services are in place. There are various methods for organizing this layer on the basis of the services that are needed. It depends on some technical aids, such as middleware, which manage intelligent computations and functions across several platforms. M2M application models, which directly connect devices through either wireless or wired links; cloud computing, which can be seen as a network of distant servers for data processing and storing; and the customer service platform, which provides support services and the application interface. These support services can include general things such as data processing, data storage, and services that are specific to certain applications. Machine-to-machine (M2M) communication is becoming increasingly important in the IoT space, as seen by the advancements achieved in cellular wide-area M2M connection solutions and low-power wide-area M2M technologies.

2.4.2 IoT Applications

IoT applications can be divided into three main classes on the basis of their goals: information gathering, analytics, and actual decision-making applications. Information gathering apps are responsible for gathering data from sensors and storing them locally. Analytics applications involve processing the collected data offline to create a general model for evaluating future data. Actual decision-making applications make immediate decisions on the basis of the analysed sensor data. The IoT encompasses a wide range of uses across various domains [34], as shown in Fig. 3, including the following:

- Applications geared toward consumers include wearable technology, smart homes, and medical technologies [35].
- Commercial applications in logistics and retail [36].
- Industrial uses in manufacturing, automated transportation, and resource and energy management [37].
- Public sector applications, such as developing smart cities and enhancing safety and surveillance, are all intended to increase the standard of living for people [38].

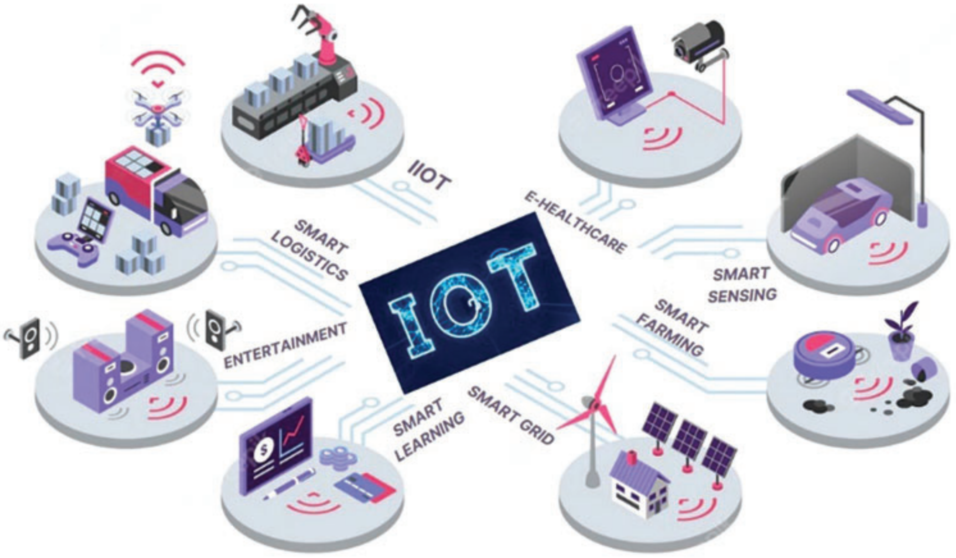


Figure 3: IoT applications

Users can directly access these IoT applications and services via a range of handheld devices, including laptops, personal digital assistants (PDAs), and mobile phones. The firmware and physical components of devices are susceptible to attacks that might harm data and operation in any consumer IoT application (perception layer security risk). Data transmission routes are frequently utilized with the intention of intercepting or obstructing data flow (network layer security risk). If user interfaces and software are not developed with strong security safeguards, they can be misused (application layer security risk).

Summary: This section discusses the layered architecture of the IoT. It addresses the perception layer (data collecting through sensors), the network layer (data transmission), the middleware layer (data processing), and the application layer (service delivery). In Internet of Things systems, these layers facilitate scalability and effective device connectivity.

3 Key Security Features of the IoT

The IoT continues to grapple with numerous security challenges due to the diversity of IoT components and the constrained computational and energy capabilities of IoT devices. These factors raise additional concerns. Ensuring a secure IoT system necessitates the incorporation of the IoT security features depicted in Fig. 4 throughout the development and operational phases of IoT devices.

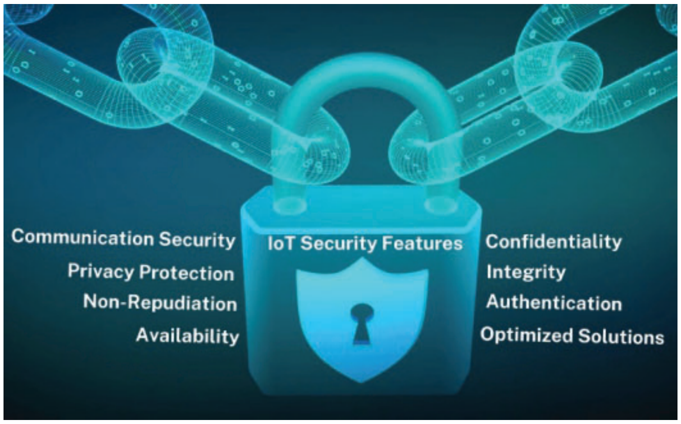


Figure 4: Key security features of the IoT

3.1 Confidentiality

Confidentiality signifies that information is exclusively accessible to authorized parties. It is crucial to safeguard data by controlling access, permitting only authorized users, and preventing devices from sharing data with neighbouring devices, whether they are services, individuals, or other devices, among others [39]. Presently, there are numerous security mechanisms available to ensure data confidentiality, including two-step verification and data encryption. However, these mechanisms demand substantial computational resources. Hence, sensors must possess an appropriate encryption mechanism that aligns with their computational and energy capabilities to guarantee data confidentiality. Additionally, it is essential to define an IoT service capable of accessing and managing data.

3.2 Integrity

In the realm of the IoT, various IoT devices engage in extensive data exchange, both among themselves and with cloud computing resources. Given this scenario, ensuring data integrity, verifying its origin as the correct sender and confirming that it remains unaltered during the transfer process, regardless of intentional or unintentional interference by attackers, users, or eavesdroppers, becomes paramount [40]. Traditional systems typically uphold data integrity by fortifying the security of node-to-node connections and managing data traffic through protocols, firewalls, and similar measures. However, within the context of the IoT, these methods fall short of ensuring security at the endpoints owing to the unique characteristics of the IoT infrastructure.

3.3 Authentication

Authentication is a crucial process that enables IoT devices to secure data and restrict access to only those with appropriate permissions. Every IoT device must be able to easily authenticate other devices [41]. Nevertheless, the complexity of the IoT structure and the diverse elements involved, including devices, clients, and services, make authentication procedures inherently challenging. Additionally, limitations such as constrained storage space, computational power, energy resources, and the absence of a user interface impose constraints on IoT devices. Furthermore, it is essential to implement a mutual authentication mechanism for various IoT entities because, during initial connections, devices must authenticate other newly introduced devices that have not previously undergone authentication.

3.4 Optimized Solutions

The implementation of IoT systems extends into numerous sensitive domains where information protection is paramount. Consequently, it becomes imperative to account for the limitations of IoT devices during the design and implementation phases of protocols. These protocols must be tailored to suit the capabilities and constraints of IoT devices. As a result, there is a need to develop suitable optimized solutions that can fulfil the rigorous data security requirements while maintaining a delicate balance between power consumption, security measures, and overall system performance.

3.5 Availability

Availability is a fundamental assurance that a system will function reliably under all operating conditions, and it holds particular significance as a key feature in the IoT, especially in critical sectors. For example, in health monitoring systems, the real-time collection of patient health data is of utmost importance, and any disruption in availability can have life-threatening consequences for patients [42]. Ensuring availability in an IoT system necessitates the harmonious integration of various factors. These factors collectively work towards upholding system availability in the IoT, including the implementation of energy-efficient protocols, the incorporation of energy harvesting methods, and the adoption of lightweight and efficient encryption mechanisms, among others. This challenge is further compounded in the IoT because of its intricate and heterogeneous nature, making it susceptible to energy depletion attacks.

3.6 Non-Repudiation

Nonrepudiation is a fundamental assurance of the identity of an entity that generates services and transmits data, instructions, or orders, making it impossible for any involved entity to deny its involvement. Nonrepudiation holds exceptional importance, particularly in sensitive systems. For example, in the healthcare sector, the system for modifying medication must ensure that modifications can be made only by the patient's healthcare provider. Typically, signatures are employed to achieve nonrepudiation, as they establish the party responsible for creating a service or message, helping to trace unauthorized or criminal activities [43]. Nonetheless, enforcing nonrepudiation is imperative in IoT applications as well.

3.7 Privacy Protection

IoT privacy protection involves ensuring that users' personal information and privacy are protected when IoT systems and devices are used. Encryption, data anonymization, user permission methods, access controls, and adherence to privacy rules and regulations are just a few of the privacy protection techniques that can be used to safeguard sensitive data from being compromised and unwanted access.

3.8 Communication Security

The term communication security, or "comsec", refers to a set of procedures and controls intended to safeguard the privacy, accuracy, and integrity of data transmitted between people, groups, or systems. It includes a range of methods and security measures to guard against unauthorized access to or the interception, alteration, or eavesdropping of transmitted data [44]. Fig. 5 presents the security issues within each layer of the IoT architecture.

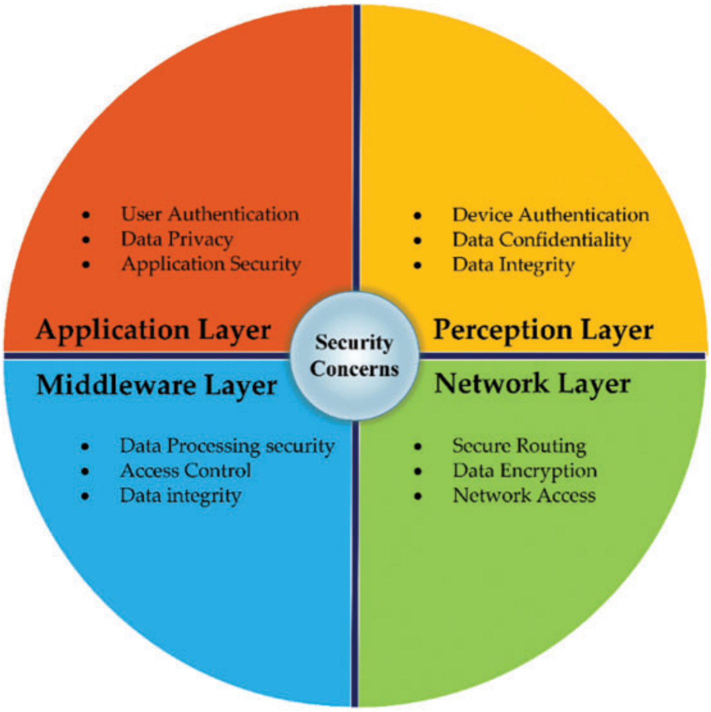


Figure 5: Security features in each layer of the IoT

Summary: The key security features of the IoT systems are outlined in this section. These characteristics include confidentiality (keeping information safe from unwanted access), integrity (keeping data accurate), authentication (confirming user identities), optimized solutions (boosting security effectiveness), availability (keeping the system up and running), non-repudiation (avoidance denial of actions), privacy protection, and communication security. Protecting IoT environments against new attacks requires these features.

4 Various Attacks on Each Layer of the IoT

The issue of IoT security is escalating as attacks on embedded devices continue to rise. In this section, we outline the primary types of attacks on each layer of the IoT architecture [20,45], as illustrated in Fig. 6.

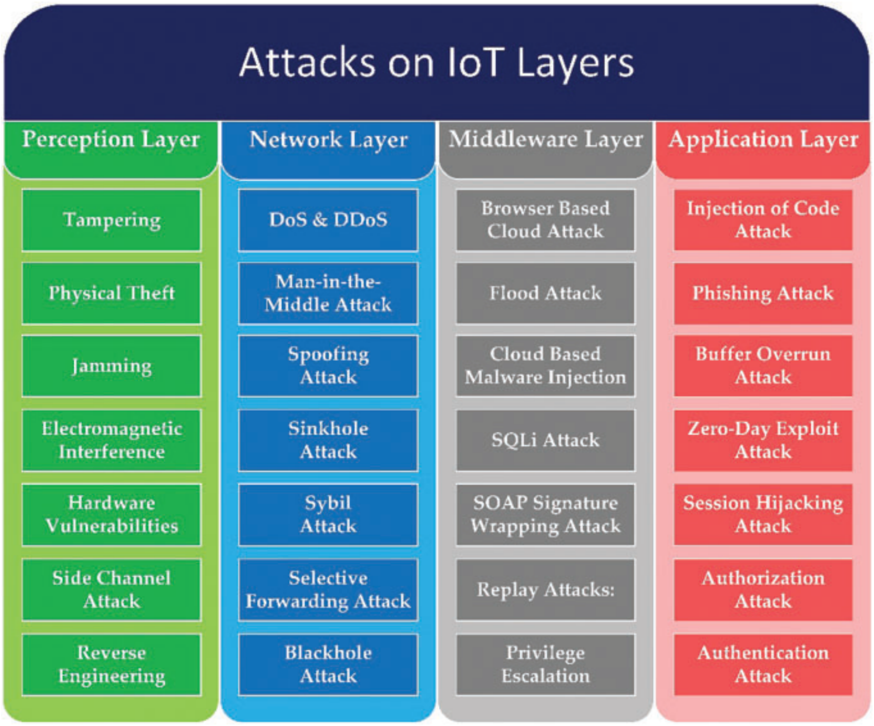


Figure 6: Different attacks on each layer of the IoT architecture

4.1 Attacks on the Perception Layer

Attacks on the perception layer focus primarily on disrupting and obstructing both communication and data collection processes [46]. Some of these attacks are listed below, and their impacts and methods of mitigation are summarized in Table 3.

Table 3: Summary of the attacks on the physical layer of the IoT

Attacks	Impact	Mitigation
Tampering	Data integrity and device operation may be compromised by tampering.	Apply tamper detection mechanisms and appropriate responses to physical intrusion.

(Continued)

Table 3 (continued)

Attacks	Impact	Mitigation
Physical theft	Unauthorized access to confidential information, device modification, or even resale on the black market.	Place locks, tamper-evident seals, and secure enclosures as physical security measures. When unauthorized access is found, use intrusion detection systems (IDS) to send out an alarm.
Physical interception	Stolen or compromised sensitive data.	Utilize physically secure communication methods and apply encryption.
Jamming	Data loss or equipment malfunction.	Putting anti-jamming strategies in place, like frequency hopping, power regulation, signal redundancy, and spread spectrum technology utilization, to ensure dependable communication in the presence of interference.
Electromagnetic Interference (EMI)	Data corruption, device malfunctions, or permanent hardware damage.	Use electromagnetic compatibility (EMC) testing and shield IoT devices from EMI.
Environmental factor	Failure of the device, inaccurate sensor readings, or damage.	Utilize IoT ruggedized hardware and test new products in various settings before releasing them.
Hardware vulnerabilities	Persistent threats, compromising the security and functionality of the devices.	Apply secure design principles, hardware audits, and the use of Hardware Security Modules (HSMs).
Supply chain	During production or distribution, hackers insert hardware implants or backdoors into IoT devices.	Implement supply chain security measures, and monitor device behaviour for anomalies.
Side-chain	Reveal sensitive information by analysing unintended emissions.	Implement encryption, and noise reduction techniques.
Reverse engineering	Attackers can access the electronic and physical components exposing the weakness and confidentiality.	Using hardware obfuscation methods, tamper-evident packaging, and routine security audits.

4.1.1 Tampering

During this attack, hardware on IoT devices is physically changed or opened. To gain access without authorization or alter device behaviour, attackers may tamper with sensors, circuits, or connections. Data integrity and device operation may be compromised by tampering.

4.1.2 Physical Theft

IoT device theft is an easy-to-detect but potent threat. Device theft can result in unauthorized access to confidential information, device modification, or even resale on the black market. Vulnerabilities can also be found through reverse-engineering stolen devices [47].

4.1.3 Jamming

Attacks that jam wireless signals prevent them from passing through the physical layer. By sending interference signals at the same frequency as the IoT devices, attackers disrupt communication. Data loss or equipment malfunction may result from these interruptions [48].

4.1.4 Electromagnetic Interference (EMI)

To interfere with IoT device functions, attackers generate EMI. Sensors, communication, and data processing can all be affected by EMI, which could result in inaccurate readings or broken equipment [49].

4.1.5 Hardware Vulnerabilities

One frequent attack method takes advantage of flaws in the actual hardware components of IoT devices. To undermine the security of a device, attackers may target weaknesses in sensors, microcontrollers, or the power supply [50].

4.1.6 Side-Channel Attacks

Attackers examine physical traits such as power usage or electromagnetic emissions to learn more about how a device works. These assaults can be used to retrieve sensitive data such as encryption keys [51].

4.1.7 Reverse Engineering

Attackers dismantle IoT devices in this attack to learn about their electronic and physical components. This may expose weaknesses, confidential information, or intellectual property, opening the door for further attacks or copying.

4.2 Attacks on the Network Layer

The network layer is responsible for ensuring information security and facilitating network communication. Some of these attacks are outlined below, and their impacts and methods of mitigation are summarized in Table 4.

4.2.1 Denial of Service (DoS) and Distributed Denial of Service (DDoS)

DoS attacks overwhelm a network with excessive traffic, making it unavailable to users. DDoS attacks use numerous compromised machines, frequently forming a botnet, to carry out an organized attack [52]. A notable example is the takeover of health information systems and services that operate in environments with limited bandwidth capacity. This situation poses life-threatening risks and can lead to financial losses for IoT networks.

Table 4: Summary of the attacks on the network layer of the IoT

Attacks	Impact	Mitigation
DoS & DDoS	Disrupt IoT services, rendering devices and networks unavailable, causing widespread service disruption.	To recognize and restrict malicious communications, implement traffic filtering, device authentication, and rate limiting. Utilize DDoS mitigation services and install both intrusion detection and prevention systems (IDS and IPS).
Man-in-the-Middle (MitM)	Compromising the integrity and confidentiality of data, enabling attackers to grab crucial information.	Use robust authentication techniques and encryption protocols, such as secure socket layer and transport layer security (SSL/TLS).
Spoofing	Compromised network integrity, and unauthorized access.	Use robust authentication methods like certificates and intrusion detection to spot abnormal device behaviour.
Sinkhole	Compromised the data integrity and behaviour of IoT devices.	To stop devices from connecting to malicious nodes, use secure device authentication and network access controls.
Sybil	Attack the system by modifying the node.	Utilizing techniques like Sybil Guard, and Sybil Shield.
Selective forwarding	Sends a limited number of messages while discarding the others.	Multipath routing probes, the combination of multipath routing, and sequential nodes are used.
Blackhole	Considerable loss of data.	Topology graph based anomaly detection (TOGBAD), which is based on topology graphs for the optimized link state routing protocol (OLSR) protocol, incorporates features like sequence check numbers, adaptive algorithms, and *ad hoc* on-demand distance vector security extension (AODVSEC) for enhanced performance and security.

4.2.2 Man-in-the-Middle (MitM) Attack

Attackers might intercept and change communications between IoT devices and their target locations. The communication channel that is exposed to unauthorized users becomes susceptible to attack. When nodes exchange keys, an attacker can intercept the connection and acquire the key. Consequently, the attacker gains the ability to encrypt and decrypt all the data transmitted between these nodes.

4.2.3 Spoofing Attack

The identities of IoT devices or network components may be spoofed by attackers, making distinguishing between trustworthy and unfriendly entities challenging. Once the attacker has obtained complete access to the system, they will proceed to transmit malicious data into the system [53].

4.2.4 Sinkhole Attack

In a sinkhole attack scenario, the attacker pretends to be the optimal route provider to a specific target, typically offering a low-latency path. When legitimate nodes in the network use this fake route to transmit data packets, the attacker either manipulates or discards the packets. This allows the attacker to exploit the packets for various malicious purposes, such as eavesdropping, altering the packet's contents, retransmitting it, and selectively forwarding packets from specific nodes [54].

4.2.5 Sybil Attack

To confound other nodes, a malicious node adopts multiple identities within the network, creating the illusion that an adversary occupies multiple positions simultaneously. In a network where all nodes collaborate in decision-making, an attacker can provide incorrect sensing information, leading to erroneous decisions and the propagation of false data through the network channels. To counteract this attack, nodes employ an identity validation mechanism that utilizes both direct and indirect validation methods. In direct validation, each node verifies the authenticity of the identities of others, whereas in indirect validation, confirmed nodes vouch for the identities of other nodes. All participating nodes must confirm their identities by possessing a unique key shared exclusively with the base station [55].

4.2.6 Selective Forwarding Attack

In a multihop network system, all nodes must forward messages accurately, especially in dense WSNs. However, an attacker may compromise the system by configuring a node to transmit only a select few messages while discarding others. To avoid such attacks, it is crucial to periodically assess the support vector machines used in the attack and keep a close eye on packet sequence numbers.

4.2.7 Black Hole Attack

In this type of attack, network traffic is directed toward a particular node that does not actually exist within the network. As a consequence, packets are dropped, leading to substantial data loss. To counteract this, a security-aware routing (SAR) protocol is employed in WSNs to thwart blackhole attacks.

4.3 Attacks on the Middleware Layer

By targeting the middleware layer, attackers have the ability to disrupt the application layer, which supplies services to the application layer. This type of attack, which is directed at servers and databases, impacts both the system's information and its operational capabilities. Attacks on cloud servers predominantly focus on virtualization and big data, posing a substantial threat to user privacy. Below is a description of some of these attacks, along with their impact and methods of mitigation, which are summarized in Table 5.

Table 5: Summary of the attacks on the middleware layer of the IoT

Attacks	Impact	Mitigation
Browse-based cloud attack	Data accessed by individuals who do not have proper authorization.	Employ secure browsing practices, and a web application firewall (WAF).
Flood attack	Impact the reliability and availability.	Employ rate limiting, traffic limiting, traffic balancing, Content Delivery Networks (CDNs), and anomaly detection.
Cloud-based malware injection	Data loss, service interruptions, loss of data confidentiality, and reputational harm to a company.	Employ secure coding practices, regular patching and updates, and cloud antivirus.
SQLi	Impact SQL database.	To guarantee that user inputs follow the intended information formats, always validate and filter them.
SOAP signature wrapping attack	Impact the signature algorithm, leading to eavesdropping attacks.	Apply canonicalization and exclusive XML canonicalization, use appropriate XML signature libraries, and structure validation of messages.
Replay attack	Attackers can gain unauthorized access to the IoT system by replaying valid authentication tokens or credentials, leading to potential data breaches and unauthorized control over IoT devices.	Include timestamps and nonces (randomly generated numbers used only once) in communications. This helps ensure that each message is unique and can only be processed once within a valid time frame. Use session tokens that are valid for a limited time period and are refreshed periodically to prevent reuse of old tokens.
Privilege escalation	Attackers can gain access to sensitive data and critical system functions, leading to potential data breaches and unauthorized control over IoT devices.	Implement robust access control mechanisms, including role-based access control (RBAC), to enforce strict access policies and limit the exposure of sensitive resources.

4.3.1 Browser-Based Cloud Attack

When a web browser is used to access cloud-based services, applications, or resources, harmful actions or security risks are referred to as browser-based cloud attacks. These attacks make use of browser-based interactions with cloud-based platforms or flaws or vulnerabilities in the browser itself. Cross-site scripting (XSS) attacks are one example of this, which include inserting malicious scripts into web pages that other users are viewing [56].

4.3.2 Flood Attack

A cyberattack known as a "flood" seeks to destroy a network or service by flooding it with a large volume of traffic or requests. A flooding attack aims to take up all of the target's resources, including memory, computing power, bandwidth, and network connections, making it unreachable to authorized users. Typically, flooding attacks aim to disrupt services and cause delays [57]. Examples of floods include the Ping flood, synchronous (SYN) flood, user datagram protocol (UDP) flood, and HTTP flood [58].

4.3.3 Cloud-Based Malware Injection

Malicious code or malware is injected into cloud-based services, apps, or infrastructure in a cyberattack known as a cloud-based malware injection attack. The main objective of such an attack is to jeopardize the security and integrity of cloud resources and possibly infect data, programs, or virtual environments housed in the cloud [59].

4.3.4 Structured Query Language Injection (SQLi) Attack

A cyberattack known as an SQLi attack targets databases and web applications by taking advantage of flaws in how user inputs are handled and incorporated into structured query language (SQL) queries. To maintain and obtain data from relational databases, a computer language called SQL is utilized. By manipulating input fields on a website, attackers can execute illegal SQL queries. This is known as an SQL injection attack.

4.3.5 SOAP Signature Wrapping Attack

A security defect that affects web services employing the simple object access protocol (SOAP) is the SOAP signature wrapping attack [60]. This attack, which falls under the category of extensible markup language (XML) Signature Injection attack [61], takes advantage of flaws in the way electronic signatures are carried out in SOAP-based online services.

4.3.6 Replay Attack

In this type of attack, an attacker intercepts and captures a valid data transmission and then fraudulently repeats or delays it.

4.3.7 Privilege Escalation

Privilege escalation in middleware refers to a security breach where an attacker gains elevated access rights to resources that are typically restricted [62,63].

4.4 Attacks on the Application Layer

The application layer plays a crucial role in delivering on-demand tasks and services to users. It is responsible for processing data from the network layer. The primary threats faced by this layer are software attacks and issues related to permissions over the lifetime of a device. These attacks are geared towards gaining access to sensitive information of IoT users, which can lead to breaches in data confidentiality and privacy [64]. The following is a description of certain attacks, their impact, and strategies for mitigating them. These details are condensed in Table 6.

Table 6: Summary of attacks targeting the application layer in the IoT

Attacks	Impact	Mitigation
Injection of code	Retrieve passwords, expose confidential data, acquire system entry, rob information, or propagate worms.	Authentication, routine similarity checks, and system testing before installation.
Phishing	Gains access to sensitive information, such as usernames and passwords.	Multi-Factor Authentication (MFA) verification, and raising awareness.
Buffer overrun	Undermining a system's integrity and credibility.	Use secure coding practices and Address Space Layout Randomization (ASLR) to provide memory protection.
Zero-day exploit	Result in serious security lapses and unauthorized access to IoT data or devices.	Adopt proactive security techniques like vulnerability management and security monitoring.
Session hijacking	Lead to unwanted access to sensitive data and control of IoT devices.	Employ token-based authentication, secure session management, and keep an eye out for suspicious activity.
Authorization	When a hacker gets around or takes advantage of holes in an application's authorization controls to access resources or carry out operations that are not authorized.	Use access control list (ACLs) to define and enforce precise access rules for different resources, ensuring that only authorized users can access specific data or perform certain actions.
Authentication	Attackers have the ability to interrupt services, resulting in lost productivity and downtime.	Use secure password storage techniques like salting and hashing using robust algorithms (like bcrypt or Argon2).

4.4.1 Injection of Code Attack

An injection of a code attack is a type of cyberattack that takes advantage of a security flaw by injecting malicious code into a system or a particular software. The program or system often runs the injected code, which can result in unauthorized operations, data breaches, or system compromise [65]. Different programming languages and environments are vulnerable to code injection attacks. The most common forms of code injection include script and hypertext mark-up language (HTML) injections.

4.4.2 Phishing Attack

A phishing attack is a type of cyberattack that targets applications and user interfaces of IoT devices or their users through deceptive methods in an effort to persuade them to expose sensitive information, login credentials, or provide illegal access to IoT devices or networks. It can have major repercussions for both persons and enterprises employing IoT technology. They are often conducted via email, social engineering, or malicious websites.

4.4.3 Buffer Overrun Attack

A buffer overrun is a type of attack where an attacker writes more data into a buffer than its capacity permits. The ultimate goal is to replace the existing data in the buffer with malicious code, enabling them to gain control of the entire machine. Examples of such attacks include stack overflow and global data area overflow. Typically, attackers employ assembly code to execute such attacks. These assaults are crafted to compromise a system's integrity and reliability. Their impact is considered "substantial," and the likelihood of occurrence is deemed "possible."

4.4.4 Zero-Day Exploit Attack

Cyberattacks that target previously unidentified vulnerabilities in IoT software applications or services are referred to as zero-day exploit attacks. It makes use of a security flaw that has not yet been made public or known to the software vendor, giving the vendor no time to deploy a security patch or update [66].

4.4.5 Session Hijacking Attack

Session hijacking attacks seek to acquire unauthorized access to ongoing user or device sessions, giving attackers control over IoT hardware, software, or services. This type of attack focuses on session management systems' security holes, which can result in serious security lapses and improper usage of IoT resources.

4.4.6 Authorization Attack

In IoT devices, there is a lack of standardized authorization techniques, which means that there is no one-size-fits-all authorization mechanism suitable for all types of IoT devices [67]. This attack occurs when a hacker approaches or takes advantage of holes in an application's authorization controls to access resources or carry out operations that are not authorized.

4.4.7 Authentication Attack

These attacks target the systems and user identity verification processes. For example, attackers may exploit an application update to introduce a harmful payload into an IoT device or system, thereby gaining access to or control over the IoT device or system.

Summary: Potential security attacks that target specific IoT architecture layers are examined in this section. It includes attacks on the perception layer (such as tampering, jamming, etc.), attacks on the network layer (like DoS, MitM, etc.), attacks on the middleware layer (such as browser-based cloud attacks and flood attacks), and attacks on the application layer (like Phishing attack, authorization attack, etc.). The section sheds light on the ways in which these multi-layered attacks affect IoT systems, emphasizing the necessity of strong defences that are specific to each tier.

5 Recent Attacks Targeting IoT Technologies

This section discusses recent attacks targeting IoT technologies.

5.1 In 2024

Cybersecurity Ventures projects that during the next two years, the cost of cybercrime would increase by 15% yearly, hitting $9.5 trillion USD worldwide this year and staggering $10.5 trillion USD yearly by 2025. A global team of researchers created the first-ever "World Cybercrime Index," which ranks the most important sources of cybercrime at the national level and identifies the world's major hotspots for cybercrime after three years of extensive research. The index, which was released in April 2024, demonstrates that the greatest threat from cybercriminals is concentrated in a small number of nations. Russia is ranked first, followed by Ukraine, China, the United States, Nigeria, and Romania. The United Kingdom is ranked eighth [68,69]. The Q1 2024 MetLife & U.S. Chamber of Commerce Small Business Index shows that ransomware, malware, and phishing are among the top concerns for 60% of small firms in regard to cybersecurity. By 2031, ransomware attacks are expected to surpass $265 billion USD yearly, according to Cybersecurity Ventures. Over the following seven years, ransomware attacks on devices, corporations, governments, and individuals will increase in frequency until they affect one person per second by 2031. According to Verizon's 2024 Data Breach Investigation Report (DBIR) [70], ransomware or other forms of extortion were used in 32% of all data breaches, with an average loss of $46,000 per incident. The percentage of breaches that were only extorted rose to 9%.

Together, NETGEAR and Bitdefender, two of the top providers of cybersecurity software worldwide, are looking at the security threats that modern smart homes face and those that lie ahead. They examined threat information from 3.8 million NETGEAR ArmorTM-protected households worldwide. Enabled by Bitdefender®, the study examined over 50 million IoT devices, producing over 9.1 billion security events. The aim was to identify the most prevalent vulnerabilities and attack scenarios, with the goal of enhancing the safety of homes and families for all members. The 2024 IoT Security Landscape Report [71] presents several startling findings, which are shown below:

- Home network devices experience 10 attacks an average of every 24 h.
- Bitdefender smart home security systems stop a typical of 2.5 million threats, or approximately 1736 threats per minute.

Below are some of the most renowned cybersecurity attacks of 2024.

5.1.1 French State DDoS Attack

A cyberattack that targeted many French public systems in March was characterized by Prime Minister Gabriel Attal's office as a breach of "unprecedented intensity." Nearly 300 web domains, including 177,000 IP addresses connected to the government, were affected for nearly a full day, with significant interruptions to prominent public service websites. Because of a DDoS assault, websites were rendered inaccessible by hackers flooding systems with data [72].

5.1.2 The $872 Million Cyberattack on UnitedHealth

Ransomware is still a major issue. In April 2024, the UnitedHealth Group released its Q1 financial report, which included a staggering $872 million loss caused by ransomware. According to the report, the company's cyberattack response steps, which included financing acceleration to care providers, had an approximately $3 billion impact on the $1.1 billion cash flows from operations from the first quarter of 2024. The timing of public sector revenue receipts also had an impact [73]. The hack affected UnitedHealth's ChangeHealthcare platform. Transactions between physicians, pharmacists, and other healthcare providers in the USA are managed by this payment platform. The BlackCat/ALPHV group claimed to have stolen 6 TBs of data, leading to the suspension of the ChangeHealthcare platform as a result of the attack.

5.1.3 Hacking of Roku Credentials

According to the TV streaming company Roku, hackers use hijacked login credentials to enter accounts. Following an attack that affected 15,000 accounts previously in the year, Roku increased its surveillance of account activity, which is how the breach was found. The very first attack occurred in March 2024, and it was discovered that the cause was "credential stuff," a tactic used by malicious actors to try to compromise other systems by using login credentials they obtained from other websites. After that, Roku received wind from another incident that affected 576,000 more accounts. The effects include a large loss of money, a decline in customer confidence, and more regulatory scrutiny [74,75].

5.1.4 Hacking Tangerine Telecom's Credentials

Over 200,000 customers' complete identities, dates of birth, email addresses, and cell phone numbers were stolen by intruders in a data breach that affected the web hosting company Tangerine. Customers' confidential data were compromised on the 18th of February, Tangerine claimed in an email, and management was notified two days later [76].

5.1.5 VARTA Group Cyberattack

The VARTA Group was the victim of an online attack on the 12th of February, 2024, affecting operations and five manufacturing facilities. The manufacturing process was proactively stopped, and the IT systems were subsequently disconnected from the internet for reasons of security [77,78].

5.1.6 Payroll Hack of the UK Ministry of Defence

The payroll system of the UK Ministry of defence was the subject of a serious cyberattack in March 2024. It is believed that the hack, which revealed 270,000 service members' personal information, including names, bank account information, and even residential addresses, is connected to a cyber-espionage scheme [77].

5.1.7 Twitter Data Breach

A serious data breach that affected Twitter in 2024 resulted in the exposure of more than 200 million users' personal data. This hack, which was discovered in July, featured a 9.4 GB database that was compromised and contained user information such as email addresses, names, and account information. The information was split into ten 1 GB files and posted for download at no charge on a reputable hacker forum [77].

5.2 In 2023 and Earlier

According to the 2023 Global Threat Report, during the first two months of 2023, there was a significant increase in cyberattack attempts targeting organizations. On average, nearly 54% of organizations experienced these attack attempts each week, with nearly 60 attacks targeting IoT devices per organization per week. This represents a 41% increase compared with the previous year and more than a threefold rise in attacks compared with two years ago [79]. The range of targeted IoT devices encompasses various common items, including routers, IP cameras, digital video recorders (DVRs), network video recorders (NVRs), printers, etc. [80].

IoT devices such as speakers and IP cameras have become increasingly prevalent, especially in remote work and learning setups, offering cybercriminals numerous potential entry points for exploitation. This trend was observed across all geographical regions and industry sectors. Among these regions, Europe experienced the greatest number of attacks on IoT devices, averaging nearly 70 attacks per organization every week, followed by Asia–Pacific (APAC), with 64 attacks; Latin America, with 48; North America, with 37 attacks (notably showing the most significant increase from 2022, with a 58% rise); and Africa, with 34 weekly IoT cyberattacks per organization [81].

The education and research sector, in particular, witnessed an unprecedented surge in attacks targeting IoT devices, averaging 131 weekly attacks per organization. This figure is more than twice the global average and represents a remarkable 34% increase compared with the previous year. Various sectors are also experiencing a notable increase in cyberattacks, with the majority of them showing double-digit growth [82]. The details [83] can be found in Fig. 7.

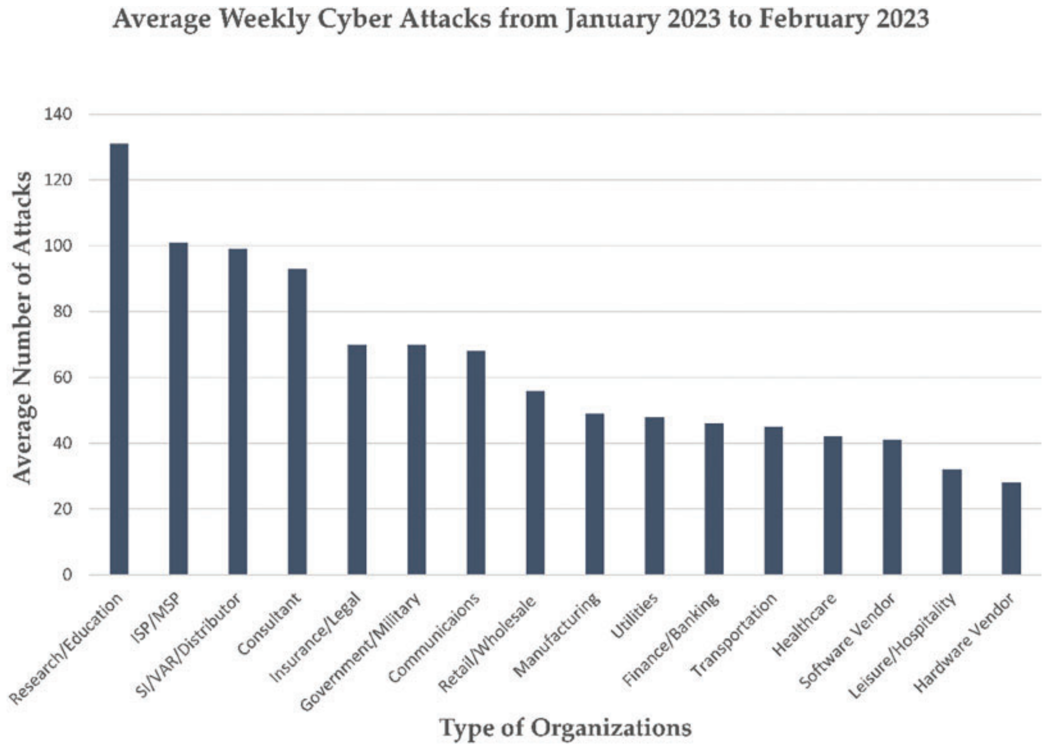


Figure 7: Depiction of the average weekly cyber attacks per organization by sector from Jan–Feb 2023

5.2.1 FLocker (Frantic Locker) Smart TV Attack

Ransomware is a type of cyberattack that is relatively straightforward to execute, and the potential rewards for hackers are substantial [84]. To carry out a ransomware attack, even individuals without advanced technical skills can conduct basic research on how these attacks work. They can then create an email containing a malicious link that, when clicked by a user, infects the user's device. Once inside the victim's system, ransomware typically leverages the user's privileges to move through the network, often encrypting all files accessible to that user. In more advanced cases, ransomware may even attempt to increase its privileges to infect a broader portion of the network, effectively making network files unreadable. The attackers then demand a random payment, typically in an untraceable form, in exchange for the decryption key. According to the FBI, ransomware attacks had already generated a staggering $209 million in just the first three months of 2016, and this number was on a sharp upwards trajectory [85].

One notable variant of ransomware that emerged in May 2015 is called FLocker, short for "Frantic Locker." Initially, targeted at mobile Android devices, FLocker has since expanded its scope. A smart TV that has been compromised by FLocker is locked and shut off, rendering factory reset unfeasible. FLocker not only turns off the TV but also projects a message onto the screen that seems to be from a government agency, such as the U.S. cyber police. The notification requests that you pay a ransom to unlock the smart TV, often in the form of digital currencies and an iTunes gift card for $200.

5.2.2 Smart Bulb Attack

Replay attacks and other security risks can be easily launched against many commercial IoT devices because of their weak authentication procedures. One example of this is commercial smart bulbs. In a recent demonstration, researchers conducted a test that revealed how these vulnerabilities could be exploited to establish a hidden channel for instigating a ransomware attack inside a company, using a seemingly innocuous device such as an office digital scanner [86]. In this case, the malware enters the organization's network through the office scanner, which serves as a gateway to establish a covert communication route among the hacker and the malware. The security flaw that was exploited centred around the sensitivity of the light sensor within the smart bulb. Even from remote locations, attackers can manipulate this sensitivity to gain control. When IoT devices lack proper security measures and protocols, they become susceptible to full control by malicious actors, essentially taking the entire IoT network hostage.

In the present study, an attack was successfully carried out on a commercial smart bulb. The attackers were able to make subtle changes to the bulb's brightness, adjusting it by just 5%, and switch the bulb on and off at a rapid rate of 25 ms, which falls below the threshold of detection by the human eye. This highlights the need for robust security measures and protocols to protect IoT devices from exploitation and unauthorized access.

5.2.3 Mirai DDoS Attack

Mirai is malicious software that targets smart devices via argonaut RISC core (ARC) processors, transforming them into a network of remotely controlled bots, often referred to as "zombies." These infected devices are then organized into a botnet, which is frequently utilized for launching DDoS attacks [87].

In September 2016, the creators of Mirai orchestrated a DDoS attack on the website of a prominent cybersecurity expert. Approximately one week later, they publicly released the source code of Mirai, possibly as an attempt to obscure the source of their initial attack. This move has been proven to have significant consequences, as cybercriminals quickly replicated the code. Mirai is believed to be responsible for the massive DDoS attack that disrupted the services of Dyn, a domain registration services provider, in October 2016 [88]. Mirai operates by scanning the internet for IoT devices powered by the ARC processor. These processors run a simplified version of the Linux operating system. If the device's default username and password combination has not been changed, Mirai can gain access to the device and infect it. Mirai botnet, at its peak, harnessed the power of hundreds of thousands of compromised IoT devices to execute large-scale DDoS attacks, which could overwhelm and disrupt targeted online services [89].

5.2.4 *Most Formidable DDoS Attack*

In April 2023, a well-known cryptocurrency platform faced one of the most formidable DDoS attacks on record, as reported by Cloudflare. The attackers unleashed an astonishing 15.3 million requests per second. What made this attack particularly severe was its use of HTTPS requests instead of the traditional HTTP, significantly increasing the computational demands on the target [90].

The sheer scale of resources mobilized for this attack indicates that DDoS threat actors are acquiring increasingly potent capabilities. Cloudflare identified approximately 6000 bots responsible for carrying out the attack, with the capacity to generate up to 10 million requests per second. These bots were distributed across 112 countries, with Indonesia contributing approximately 15% of the attack's fire power, followed by Russia, Brazil, India, Colombia, and the United States. Interestingly, the majority of the attack traffic comes from data centres, indicating that DDoS attackers are now more focused on cloud computing ISPs than domestic network ISPs. The attackers used hosting service providers' compromised servers, most of which operated with Java-based software. There were also a significant number of MikroTik routers implicated, which most likely used the same vulnerability that Meris botnet had exploited. The ongoing rivalry in cybersecurity among adversaries and cybersecurity companies is highlighted by this occurrence.

5.2.5 *Ransomware Attack Targeting Royal Mail*

In January, the Royal Mail service in the UK encountered significant disruption due to a ransomware incident. This attack specifically targeted the international shipping facilities of Royal Mail, causing a complete halt in the transportation of parcels and letters across its extensive network of post office branches throughout the country. This disruption caused substantial inconvenience for Royal Mail's customers [91]. The responsibility for this attack was claimed by the LockBit ransomware group, which has links to Russia. They demanded £67 million as ransom. However, Royal Mail firmly rejected this demand, with their negotiators deeming the amount "absurd" [92].

Royal Mail remained resolute in their decision not to engage in negotiations with the attackers, firmly refusing to meet the ransom demands. In response, the persistent hackers threatened to release the hijacked and encrypted data online, suggesting that this action would have severe financial consequences for both the company and its customers. However, this assertion was rejected by the ransom negotiator, who clarified that the adversary had misinterpreted the nature of the business. Consequently, the Royal Mail board categorically refused to pay the requested ransom. This episode made it much more crucial for firms to resist the need to pay ransoms in the wake of ransomware assaults. It also emphasized the importance of using experienced negotiators in these kinds of circumstances. The Royal Mail efficiently recovered its systems in the latter half of February, despite a six-week stoppage to its worldwide mail services. LockBit then went ahead and posted the stolen data on the dark web. LockBit, accounting for 33% of ransomware attacks in the last half of 2022, has become one of the world's most active ransomware gangs [93]. This represents a substantial 94% increase compared with its activity in 2021.

5.2.6 *JD Sports Data Attack*

JD Sports revealed in January that it had been victim to a cyberattack that exposed the financial and personal data of ten million of its customers who had made online purchases from November 2018 to October 2020. The last four digits of the payment cards, client names, addresses, phone numbers, and order details were among the information that was compromised [94].

Following the revelation of the cyber-attack, JD Sports has confirmed its intention to enhance its cybersecurity measures in response to the significant breach earlier in the year. Despite initial concerns that the company might incur a substantial fine for the data breach, the Information Commissioner's Office (ICO) has informed JD Sports that it will not be subject to enforcement action as a consequence of the incident. However, the ICO has highlighted some areas where business data security procedures need to be improved [95].

5.2.7 Surge of Ransomware Attacks by Black Basta

The Black Basta ransomware group has gained interest as one of the world's most notorious cybercriminal organizations. While it has been active since 2022, its activity significantly increased in 2023. The group has targeted several governmental and business sector organizations within Europe and nations that speak English throughout this time. This Russia-linked gang employs a dual extortion approach, wherein it pilfers and encrypts victims' data, subsequently demanding a ransom for its decryption. In cases where victims refuse to comply with the ransom demand, the gang resorts to publishing their data on its dark web blog [96].

One notable target of Black Basta's operations was asea brown boveri (ABB), a Swiss-based automation giant boasting a workforce of over 100,000 employees and reporting revenues of $29.4 billion in 2022. In May 2023, the gang launched an attack on ABB by exploiting its Windows Active Directory. This attack had widespread repercussions, impacting hundreds of devices and causing disruptions across ABB's operations, factories, and projects. In response, ABB took the precaution of suspending VPN connections with its clients to prevent the further spread of the malware [97]. Additionally, several U.S.-based companies fell victim to a campaign orchestrated by Black Basta affiliates in June 2023, leveraging the QakBot banking trojan. This trojan serves as the initial entry point for these affiliates into victim networks, facilitating the swift deployment of ransomware and targeting businesses from a range of industries, including manufacturing, retail, healthcare, and finance.

Summary: Highlighting the increasing sophistication of threats, this section lists notable IoT-related attacks that occurred between 2024 and earlier. The French State DDoS Attack, the $872 million cyberattack on UnitedHealth, etc., are few notable incidents from 2024 that highlight the weaknesses of large networks. The section also discusses previous attacks that show how even seemingly simple IoT devices can be attacked, such as the Smart Bulb Attack, the FLocker malware, etc. As the deployment of IoT expands across businesses, these incidents underscore the pressing need for better security solutions.

6 Current Challenges in IoT Security and Their Possible Solutions

The IoT is still reshaping our digital world in 2024 as we move forward. IoT has tremendous potential due to its constantly growing network of linked devices, but it also presents a number of challenges. Table 7 presents the literature that highlights the challenges associated with the IoT.

Table 7: Challenges related to the IoT that are discussed in the literature

Ref.	Targeted issue	Key points
[98,99]	Interoperability	Interoperability within the area of the IoT relates to the capacity of distinct devices, services, and systems to effectively share data and seamlessly integrate. These studies delve into a range of techniques and strategies accessible for mitigating interoperability concerns. Additionally, introducing a methodical categorization of the prevailing remedies aimed at surmounting the obstacles arising from the absence of interoperability.
[100,101]	Standardization	Standardization plays a key role in establishing universally accepted specifications and protocols, facilitating genuine interoperability among devices and applications. The adoption of standards not only guarantees solutions that are interoperable but also cost-effective. These researches offer insight into the existing IoT standards and their intricate interrelationships. They identify the challenges and complications linked with these standards while presenting prospective remedies. Additionally, the significance of nation-specific standardization is elucidated and substantiated through a pertinent illustration.
[41,102]	Scalability	IoT scalability denotes the capability to transition seamlessly from a prototype stage to full production. A scalable IoT system should facilitate interoperability among diverse devices and protocols, thereby enhancing the efficiency and effectiveness of data exchange. These studies delineate the critical aspects that warrant consideration when tackling scalability. Additionally, delves into an array of techniques employed to realize scalability, explores distinct forms of scalability, and digs into ongoing research initiatives and challenges within this sphere.
[103,104]	Infrastructure constraints	The integration of IoT devices into operations necessitates businesses to possess a resilient network infrastructure. IoT devices demand connections with high bandwidth and minimal latency, prompting businesses to allocate resources toward high-speed networks capable of accommodating the escalating device count. Examining the IoT infrastructure's responsiveness to the substantial data generated by IoT devices carries substantial significance. These researches thoroughly examine the performance challenges linked to IoT network infrastructures, investigating factors such as throughput, latency, and load, among others.

(Continued)

Table 7 (continued)

Ref.	Targeted issue	Key points
[105]	Complexity	IoT ecosystems exhibit a profound level of complexity, a trait that profoundly influences their performance and accessibility. Often, this complexity parallels the intricacy inherent in developing novel integrations or applications. This study undertakes an analysis of IoT traffic complexity from dual standpoints. As a result of these perspectives, two novel metrics to gauge the complexity of IoT network traffic are introduced.
[106]	Analytics and data management	IoT analytics constitutes a data analysis and management tool dedicated to evaluating the diverse array of data gathered from IoT devices. This analytical framework adeptly processes substantial data volumes, extracting valuable insights and actionable intelligence from this accumulation. This study brings to light that the diversity, heterogeneity, and vast data quantities generated by diverse IoT entities render conventional database management systems largely inadequate for many scenarios. When architecting IoT data management systems, it becomes imperative to account for a multitude of distinctive principles. The emergence of these distinct principles has catalysed the development of diverse approaches aimed at proficiently managing IoT data.
[107]	Regulation and legality	The regulatory framework for the IoT is undergoing swift evolution. This progression encompasses regulations formulated to establish a fundamental security foundation for IoT. While laws dictate the mandatory aspects of IoT devices, they frequently delegate the delineation of functionalities to standards bodies for each respective market. The rapid proliferation of IoT applications introduces substantial challenges in the realms of security, ethics, privacy, and legality, exerting a profound impact on our daily lives. This research underscores the criticality of instituting worldwide IoT regulations and underscores the imperative of educating the general populace about the security, ethical, and privacy risks posed by contemporary IoT devices.

Many current solutions have serious drawbacks, despite the technical components of IoT challenges, such as interoperability, standards, scalability, infrastructure limits, and data management-being thoroughly studied. Scalability solutions, for example, frequently find it difficult to manage high densities of devices, which makes it more difficult to move smoothly from prototypes to large-scale deployment. Region-to-region disparities in interoperability result from standardization attempts that fall short of unifying national and international laws. High data loads and low latency demands overburden current networks, particularly in real-time applications, making infrastructure restrictions more apparent. Furthermore, traditional database structures, which are ill-suited to effectively handle the variety and enormous data streams of the IoT are often the foundation of analytics and data management systems.

In 2024 and beyond, as IoT grows, a number of challenges will arise that must be resolved if the technology is to fulfil its promise. Table 8 presents an overview of the current challenges in IoT security, along with their real-world solutions, practical examples, and also possible future solutions.

Table 8: Current challenges related to the IoT

Challenges	Key points	Real-world solutions	Practical example	Possible future solutions
Device vulnerabilities and insecure firmware	Due to obsolete or insecure firmware, plenty of IoT devices are set up with vulnerabilities that leave them open to attack [108].	Devices get safely patched and updated by the use of secure boot methods and Over-the-Air (OTA) updates [109].	To ensure the integrity and validity of firmware updates, Tesla employs OTA updates with cryptographic signature [110].	AI-powered prediction and response to new threats via the creation of auto patch management tools [111] and ongoing zero-day vulnerability monitoring [112].
Inadequate interoperability and standards	Fragmented security measures due to the lack of interoperability and unified security standards for IoT devices [98].	Creation of industry frameworks and standards, like those from the IoT Security Foundation and the Internet Engineering Task Force (IETF) [113].	Matter protocol [114] an open-source connectivity standard aims to provide a general language for IoT devices.	Full acceptance of the Matter protocol across all IoT sectors [115].
Protection of data and privacy issues	A lot of sensitive data is gathered by IoT devices, which raises questions on data protection and user privacy [116].	Data is protected both at rest and in transit by using data anonymization and end-to-end encryption techniques [117].	End-to-end encryption is used by Google Nest devices [118] to protect communication between the devices and cloud services. Differential privacy approaches were used by Apple into their data acquisition procedures.	Revolutionary cryptographic methods, like zero-knowledge proofs and homomorphic encryption [119], offer safe data processing without revealing raw data.

(Continued)

Table 8 (continued)

Challenges	Key points	Real-world solutions	Practical example	Possible future solutions
Resource limitations and scalability	Implementing strong security measures is challenging because IoT devices frequently have limited memory, processing capacity, and energy resources [120].	Resource limits are balanced with security through the use of edge computing and lightweight cryptography methods [121].	To balance security and energy efficiency, LoRaWAN encrypts data being transmitted among IoT devices and the network server using AES-128 [32].	Creating energy-efficient, ultra-lightweight encryption algorithms [122], IoT devices may be able to dynamically assign security resources based on the threat level and available device resources by combining such ciphers with AI-driven resource management.
Response to incidents and security management	It is difficult and costly to manage security across a large network of IoT devices and respond to problems quickly.	To monitor and address security threats, automatic incident response systems and centralized security management platforms are used [123].	For instantaneous threat detection and response, Splunk offers a security information and event management system that utilizes IoT data [124].	The foundation for AI-based security management systems is already being laid by current and future research and development projects from groups like Darktrace [125] and Microsoft Azure Sentinel [126], showing good results in prototype installations.
Access control and authentication	Unauthorized access to IoT devices and data is a result of weak or inadequate authentication and access control systems [41].	Implementation of MFA and role-based access control RBAC to strengthen device security [127].	Strong authentication and access control mechanisms are integrated into Cisco's IoT Threat Defence security framework [128].	Blockchain technology-based decentralized identity systems (DIS) [129] are becoming a viable future solution to improve IoT security.

(Continued)

Table 8 (continued)

Challenges	Key points	Real-world solutions	Practical example	Possible future solutions
Supply chain security	There is a chance that malicious software or components could be incorporated during manufacture due to a complicated IoT supply chain [130].	Application of safe manufacturing procedures and item verification in supply chain management systems [131].	Azure Sphere [132] from Microsoft is an excellent application platform that is secure by design and has security built in throughout the whole lifecycle of the device, including during manufacturing process.	Blockchain technology [133] and AI-driven platforms [134] can be able to automate the whole supply chain security procedure for IoT devices.
Botnets and DDoS attacks	Botnets, which are used to launch massive DDoS attacks, are frequently created via compromising IoT devices [52].	Botnet activity detection and mitigation through the use of network-level monitoring and device-level firewalls [135].	Large-scale DDoS attacks coming from compromised IoT devices can be identified and mitigated by Cloudflare's DDoS protection services [90].	Algorithms utilizing AI and ML, like Darktrace [136], can be utilized to identify abnormalities that may suggest malicious activities by modelling typical network behaviour.
Physical security risks	IoT devices are normally installed in settings where physical tampering with them could result in security lapses [47].	Tamper-evident materials, casings, and seals are being used in the design of devices indicating visually if an effort is made to open or modify the device.	Sensitive data is protected within a safe region of the device's processor thanks to a hardware feature called Apple's safe Enclave [137].	AI algorithms have the ability to learn a device's typical operating patterns and recognize variations that may indicate physical intervention [138].
Unsafe channels of communication	IoT devices are susceptible to man-in-the-middle attacks and eavesdropping because they frequently communicate across insecure channels [44].	Using VPNs and other secure communication protocols like TLS to encrypt data while it's being transferred [139].	Mutual TLS authentication is used by Amazon Web Services [140] to provide secure communication between IoT devices and the cloud.	Creation of encryption techniques that are resistant to quantum computing to safeguard IoT communications from potential threats [141].

(Continued)

Table 8 (continued)

Challenges	Key points	Real-world solutions	Practical example	Possible future solutions
Impact of 5G on IoT security	With increased device density and speed, 5G improves connectivity and may expand the attack surface [4].	To safeguard data transmissions in smart city projects and other initiatives, use strong encryption techniques and zero-trust architectures.	5G is being used in cities like Barcelona and Seoul to lower energy costs and accident rates through automated response systems and real-time monitoring [142].	By using AI-based threat detection, implementing zero-trust frameworks, and improving network slicing security to dynamically control risks across various 5G-enabled IoT ecosystems.
Security aspects of edge computing	Reduces latency by permitting localized data processing, but the decentralized nature of the data creates additional security risks [121].	To protect valuable data processed at the edge, a strong device authentication and secure data transmission routes are used.	Smart thermostats, cameras, and voice assistants (like Google Nest and Amazon Alexa) use edge computing to handle commands locally, enhancing privacy and cutting down on latency. For predictive maintenance, Siemens incorporates edge computing into its production lines [143].	Federated learning models for data analytics [144] that protects privacy and hardware-based "trusted execution environments" (TEEs) for enhancing security at the edge devices.

Summary: Important IoT current security challenges are listed in this section, including privacy concerns, device vulnerabilities, lack of standardized security standards, etc. It draws attention to how difficult it is to manage a wide range of devices and how important scalable security solutions are. Retaining low latency is vital for real-time responses in dynamic IoT situations like smart cities and vehicle networks. Lightweight security protocols, which minimize processing overhead while guaranteeing strong protection, can optimize current security methods. Delays are reduced by employing strategies like effective encryption techniques and flexible security measures. Furthermore, localized data processing made possible by utilizing edge computing reduces the need for centralized servers and helps to further reduce latency problems. Together, these strategies improve the security architecture and guarantee prompt data processing and responsiveness in IoT scenarios with high demand.

7 Practical Case Studies and Examples

This section offers various practical case studies and realistic examples that demonstrate how AI is being used to secure IoT systems, as shown in Fig. 8.

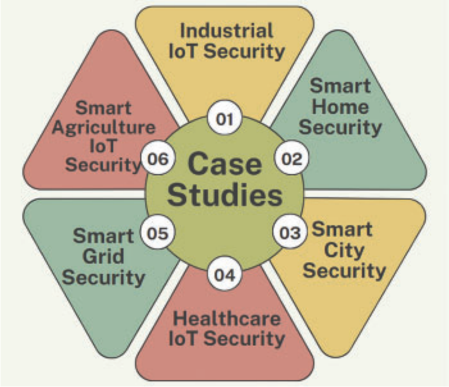

Case Studies
01 Industrial IoT Security
02 Smart Home Security
03 Smart City Security
04 Healthcare IoT Security
05 Smart Grid Security
06 Smart Agriculture IoT Security

Figure 8: Practical cases signifying the applications of AI in securing IoT systems

7.1 Industrial IoT (IIoT) Security

Critical infrastructure is frequently managed via industrial IoT systems. It is imperative to guarantee their security to prevent disruptions that may result in severe and broad consequences. IIoT system security breaches can result in large financial losses because of lost productivity, broken equipment, and theft of data. By protecting these systems, expensive repairs and disruptions can be avoided [145]. Fig. 9 presents the major threats to IIoT security.

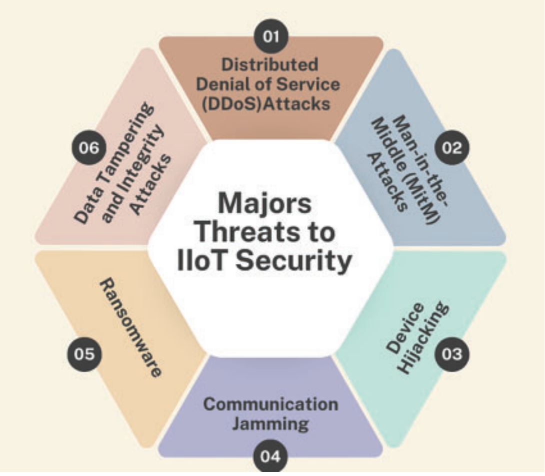

Majors Threats to IIoT Security
01 Distributed Denial of Service (DDoS)Attacks
02 Man-in-the-Middle (MitM) Attacks
03 Device Hijacking
04 Communication Jamming
05 Ransomware
06 Data Tampering and Integrity Attacks

Figure 9: Major threats to IIoT security

Numerous IIoT applications involve equipment and procedures that, in the event of a breach, might seriously jeopardize public and worker safety. To avoid mishaps and casualties, effective security measures are crucial. Continuous and effective operations are ensured in industrial settings by IIoT.

Solutions that are dependable and secure [146]. Security must come first for operational resilience since cyberattacks have the potential to interrupt supply chains and production lines.

The industrial sector's vital position in the economy makes it a prominent target for cyberattacks. Strong IIoT security protocols are required to ward off potential attacks and keep up with changing cyber threats. AI approaches are used to protect critical infrastructure from cyberattacks, identify discrepancies in operational data, and safeguard industrial control systems [147]. For example, when Cisco's Cyber Vision is utilized, Siemens improves security and visibility throughout its commercial network by incorporating security controls directly into automated processes [148].

Apart from these conventional techniques, a promising hybrid strategy for protecting software defined network SDN-based IIoT networks blends blockchain technology with entropy-based anomaly detection. This approach offers a scalable, decentralized security solution that can detect threats in real time without taxing the system's limited resources. Blockchain guarantees data integrity and decentralized trust, while entropy-based methods assist in detecting anomalous network activity. The scalability and adaptability of IIoT security frameworks could be further improved by combining this hybrid solution with AI-driven resource management, which could enable IoT devices to dynamically modify security measures based on available resources and threat levels [149].

7.2 *Smart Home Security*

AI algorithms focus on odd behaviour from smart home devices, such as sudden changes in lighting, temperature, or device usage. Fig. 10 depicts the common threats to smart home security. Google Nest uses ML techniques to detect patterns and notify homeowners of possible security risks, such as unapproved entry or atypical behaviour during periods when the home is meant to be vacant [150]. Secure access control is made possible by AI-driven systems for facial recognition, which identify authorized users and prevent admission for unidentified faces. By limiting entry to the home to just those with a known face, Ring's smart doorbells and cameras improve security by using facial recognition technology to identify and record visitors [151].

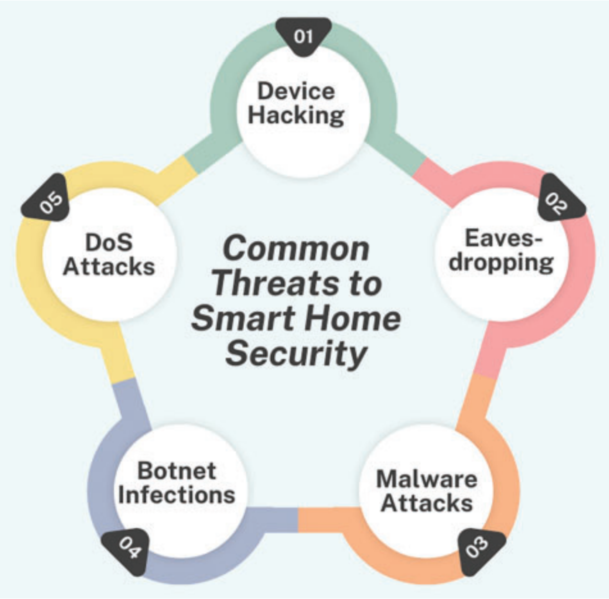


Figure 10: Common threats to smart home security

To identify and react to possible break-ins, AI-enhanced IDSs examine data from many sensors, including motion and doors/windows; for example, SimpliSafe reduces false alarms and provides homeowners with timely alerts by using AI to discern between typical household activities and possible invasions [152]. When an AI system detects a threat, it might immediately lock doors, sound alarms, or contact emergency numbers. When a threat is identified, advanced detection technology (ADT) smart security systems use AI to start automatic reactions, such as locking doors and alerting emergency numbers [153].

7.3 Smart City Security

Fig. 11 highlights the key security issues in smart city. AI-enhanced surveillance systems examine video streams from cameras located around a city to identify possible dangers instantly, identify suspicious activity, and identify faces [154]. For example, IBM Intelligent Video Analytics employs AI to monitor public areas and promptly notifies authorities of any odd activity, possible crimes, or incidents [155]. AI algorithms reduce traffic jams and improve road safety by evaluating data in real time from GPS units, IoT devices, and surveillance cameras. Using AI, Cisco's Smart + Connected Traffic solutions prioritize emergency vehicles, adjust traffic lights automatically, and lessen the chance of collisions and traffic bottlenecks [156].

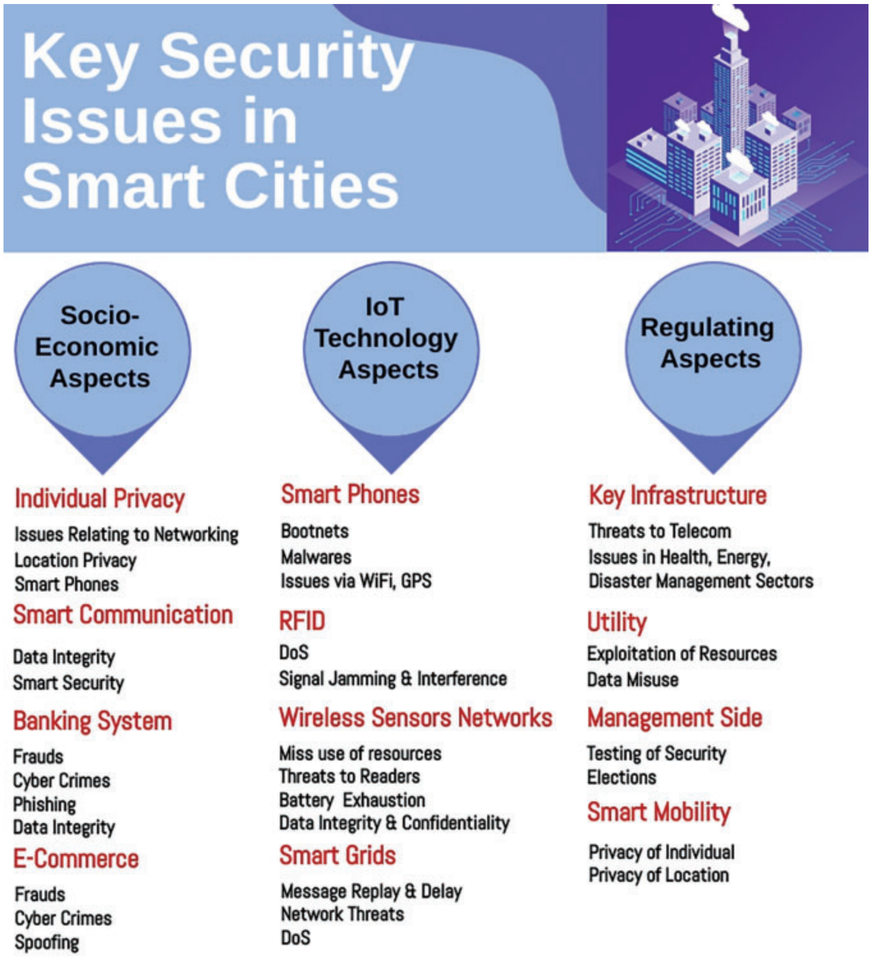


Figure 11: Key security issues in smart cities

AI services constantly scan citywide networks for anomalous activity, detecting and thwarting cyberattacks that aim to compromise vital infrastructure. For example, Darktrace's AI technology guards smart cities' digital infrastructure from cyberattacks by quickly identifying and mitigating cyber threats [136]. Parking systems with AI capabilities effectively manage parking spaces and maintain occupancy, which eases traffic and increases security. For example, ParkMobile streamlines the parking experience in smart cities by using AI to provide real-time parking availability information and safe payment processing [157].

7.4 Healthcare IoT Security

AI systems monitor patients' pulses continually, looking for anomalies and possible health problems, by analysing data from IoT medical equipment [158]. The key healthcare security threats are presented in Fig. 12. The Philips HealthSuite platform safely tracks and evaluates patient data, guaranteeing the confidentiality and integrity of the information while immediately warning medical professionals of possible issues [42]. To protect sensitive patient data sent between IoT devices and healthcare databases; AI improves encryption algorithms. For example, MedCrypt employs AI to safeguard medical device data by cutting-edge encryption, guaranteeing adherence to privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) and guarding against security breaches [159].

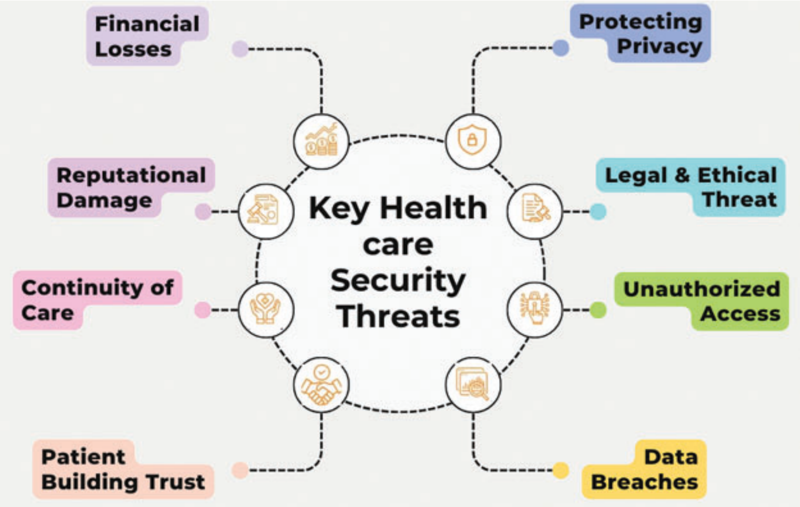


Figure 12: Depiction of key healthcare security threats

To safeguard patient confidentiality and defend against cyber-attacks, AI safeguards the data and communication channels used in telemedicine and remote surgery [160]. For example, Teladoc Health encrypts patient data and ensures safe video consultations between physicians and patients by utilizing AI to protect telemedicine systems. AI systems are capable of taking automatic action in response to the security dangers they identify, such as notifying IT security staff or isolating impacted devices. By preventing cyberattacks and limiting possible harm, Cylera's AI-driven cybersecurity technology automatically reacts to threats in real time, safeguarding healthcare IoT environments.

7.5 Smart Grid IoT Security

For smart grid the key security considerations are illustrated in Fig. 13. The smart grid's IoT sensor data are monitored and analysed by AI algorithms, which look for anomalies that can point to possible security risks such as illegal access or system failures. For example, Siemens MindSphere uses AI to regularly monitor patterns in energy consumption and identify any abnormalities that could point to equipment breakdowns or cyberattacks, enabling prompt repair and intervention [161]. By evaluating data from IoT sensors, AI forecasts probable malfunctions in smart grid components, facilitating preventive maintenance and lowering the likelihood of unplanned outages. As an illustration, General Electric's Predix platform uses AI to forecast when smart grid components are likely to break. This enables planned maintenance, which reduces downtime and improves overall grid reliability. By evaluating data from IoT sensors, AI enhances load balancing, guaranteeing effective power distribution and lowering the possibility of overloads. As an example, the EcoStruxureTM Grid from Schneider Electric [162] uses AI to optimize load balancing, guaranteeing safe and effective power distribution throughout the smart grid.

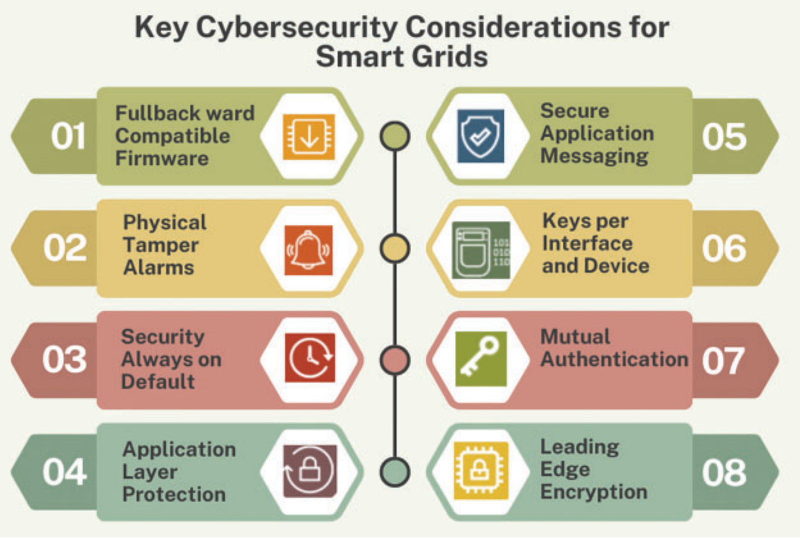
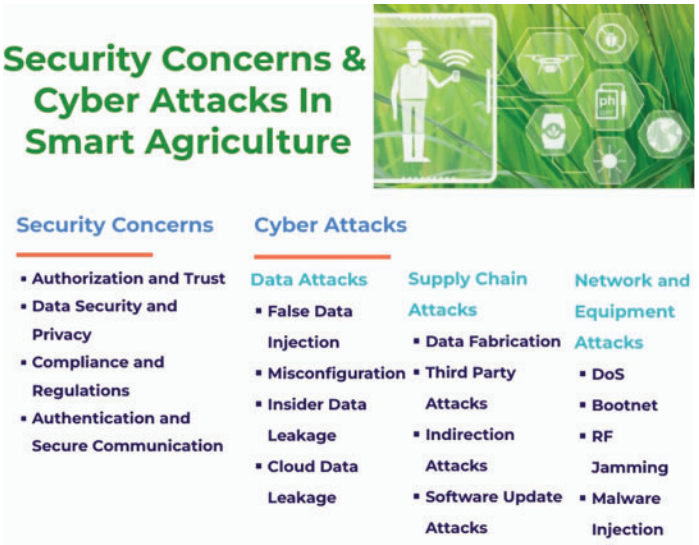

Key Cybersecurity Considerations for Smart Grids
01
Fullback ward Compatible Firmware
02
Physical Tamper Alarms
03
Security Always on Default
04
Application Layer Protection
Secure Application Messaging
05
Keys per Interface and Device
06
Mutual Authentication
07
Leading Edge Encryption
08

Figure 13: The key cybersecurity considerations for smart grids

7.6 Smart Agricultural IoT Security

The major security concerns and cyberattacks are depicted in Fig. 14. Sensitive agricultural data, including soil and crop health parameters, are safeguarded during transmission between IoT devices and central management systems through the use of AI-enhanced encryption methods [163]. For example, AI is used by John Deere's Operations Centre [164] to provide safe data transmission from agricultural equipment to cloud servers, shielding confidential data from potential cyberattacks and unauthorized access. With respect to AI, Trimble's agricultural platform analyses data from agricultural equipment to forecast maintenance requirements and lower the possibility of unplanned malfunctions that could affect farming operations. Similarly, by using AI, the IBM Watson IoT platform [165] monitors data from drones, irrigation systems, and soil sensors. It looks for anomalies that could point to a cyberattack or failure and allows prompt intervention.

Summary: In this section, important case studies of IoT security from a variety of industries are examined, including IIoT, smart grids, smart homes, smart cities, healthcare, and smart agriculture. Every case study demonstrates distinct security issues and the methods used to resolve them, emphasizing the necessity for industry-specific approaches to improve security and protect sensitive information.



Security Concerns & Cyber Attacks In Smart Agriculture

Security Concerns

- Authorization and Trust
- Data Security and Privacy
- Compliance and Regulations
- Authentication and Secure Communication

Cyber Attacks

Data Attacks

- False Data Injection
- Misconfiguration
- Insider Data Leakage
- Cloud Data Leakage

Supply Chain Attacks

- Data Fabrication
- Third Party Attacks
- Indirection Attacks
- Software Update Attacks

Network and Equipment Attacks

- DoS
- Bootnet
- RF Jamming
- Malware Injection

Figure 14: Majors security concerns and cyber attacks in smart agriculture

8 Securing Tomorrow's IoT: The Power of AI in Future Security

AI is the imitation of the cognitive abilities and reasoning that computer systems use to carry out different jobs. It imitates certain human characteristics, such as the ability to draw conclusions from prior experiences, recognize patterns, draw generalizations, and apply logic through particular tasks [166]. DL and ML are two areas of AI that enable systems to improve their performance on their own and learn from their interactions [167]. Three well-known learning AI methods are "supervised learning, unsupervised learning, and reinforcement learning techniques" [168].

The evolution of IoT smart technologies, which enable devices to both take action and gather sensory data, greatly enhances the efficiency of the IoT framework. However, the proliferation of these smart technologies interconnected within the system generates a substantial amount of data, presenting a significant challenge for processing within an IoT environment.

AI is incorporated into a more intelligent IoT network, which can fulfil the main goals of automating and adapting. AI is the process of teaching robots' things so that they can do things that normally need human intelligence. AI-based systems are evolving quickly in the context of the IoT in terms of their capabilities, applications, flexibility and processing speed [169].

AI has the ability to perform computations intelligently, and it can infuse intelligence into an IoT system while enhancing its security [170]. An IoT system powered by AI allows proactive decision-making, averting unfavourable outcomes. This can be achieved by establishing robust AI models as the foundation of the IoT system. Furthermore, addressing security complexities within an IoT network is essential to bolster its resilience. Various frameworks and mechanisms for the AI-based IoT can be found in the literature [171–173]. AI has the capacity to improve IoT system analysis, operational efficiency, and accuracy rates. The large volume of real-time data generated by IoT devices allows AI systems to achieve higher levels of accuracy. The implementation of AI and its techniques unlocks the true potential of IoT technology. Thus, it is crucial to understand the different types of algorithms and methods that AI and ML offer. The efficacy of any AI-based application is directly correlated with the calibre of the data it uses, underscoring the importance of a trustworthy framework for data collection to foster confidence [174]. Fig. 15 highlights the major advantages of AI in IoT.

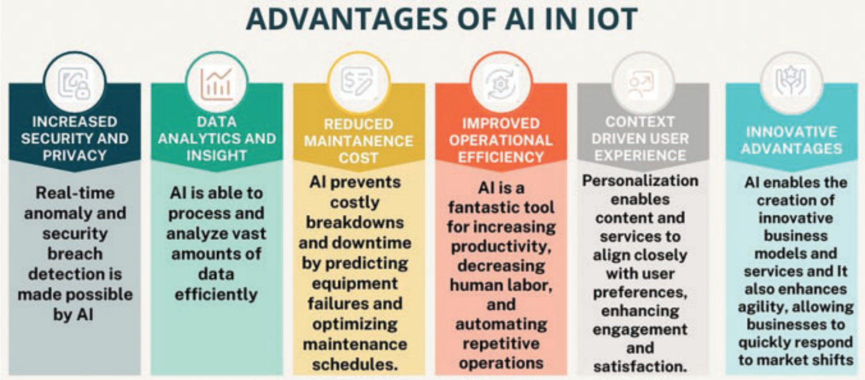

ADVANTAGES OF AI IN IOT
INCREASED SECURITY AND PRIVACY
Real-time anomaly and security breach detection is made possible by AI
DATA ANALYTICS AND INSIGHT
AI is able to process and analyze vast amounts of data efficiently
REDUCED MAINTENENCE COST
AI prevents costly breakdowns and downtime by predicting equipment failures and optimizing maintenance schedules.
IMPROVED OPERATIONAL EFFICIENCY
AI is a fantastic tool for increasing productivity, decreasing human labor, and automating repetitive operations
CONTEXT DRIVEN USER EXPERIENCE
Personalization enables content and services to align closely with user preferences, enhancing engagement and satisfaction.
INNOVATIVE ADVANTAGES
AI enables the creation of innovative business models and services and It also enhances agility, allowing businesses to quickly respond to market shifts

Figure 15: Major advantages of AI in IoT

8.1 Supervised Learning Methods

In supervised learning, a model is trained using a labelled dataset whose intended output is known. Using input feature data, the model learns to predict results. For example, it can be applied to IoT security to categorize network traffic as either malicious or authentic [175]. In addition, a reinforcement learning mechanism modifies the model's weights as data from the input is fed into it, improving the model's ability to fit the data. Algorithms that limit errors are used to quantify the correctness of the model; they are adjusted continuously until the errors are suitably reduced.

One subset of supervised learning known as regression techniques is mainly concerned with forecasting, and discovering correlations among primary datasets. Regression methods that are widely used include logistic regression, polynomial regression, and linear regression [176]. On the other hand, classification approaches aim to identify, examine, and group patterns within data in order to produce a particular outcome. Classification, for example, is a way to identify security risks in an IoT ecosystem. Classification algorithms assess, label, and define data in order to efficiently categorize it into different categories.

Federated Learning [177] offers novel AI solutions and is distributed and privacy-enhancing, it has revolutionized many intelligent IoT applications. With its advanced FL topologies, this new distributed AI technology has the ability to completely transform the way that intelligent IoT systems are currently designed. FL has emerged as a particularly attractive technique for creating distributed IoT systems, especially in light of the latest developments in mobile hardware and the growing worries about privacy violations [178]. Due to this, user data is never directly shared with a third party, while still allowing for the collaborative training of a global model, which enhances privacy and saves network resources for both network operators and IoT users. Thus, FL might serve as a powerful replacement for conventional centralized AI techniques and aid in accelerating the wider spread of IoT applications and services [179]. FL has strong benefits for facilitating decentralized applications, maintaining high privacy standards, and reducing latency in communications in smart cities [144]. In vehicle IoT networks, FL is used to protect data privacy [180]. A two-phase mitigation strategy is devised for intelligent data conversion and cooperative detection of data leakage [181]. In contrast to conventional techniques, this vehicular FL approach allows users, like vehicles, to train models independently using their own data, independent of a centralized system. By retaining sensitive data on each device, this decentralized strategy greatly improves data privacy. FL can be used to ensure network and service security in the IoT. FL has the ability to revolutionize existing intelligent healthcare systems and provide a number of effective smart healthcare solutions [182]. FL improves user privacy and lowers latency by enabling AI capabilities to assist healthcare services. This also makes it easier for multiple entities, like as healthcare professionals and patients in various medical institutions, to collaborate. FL can provide practical ways to integrate intelligence into IIoT systems, especially in areas like Industry 4.0 and robotics [183]. It prevents privacy leaks by enabling these developments without requiring data exchange between companies.

Maintaining constant contact with base stations (BSs) in UAV networks under dynamic aerial environmental conditions is difficult due to the extensive range and height of UAVs, which is essential for carrying out intelligent UAV operations. In these situations, classic centralized AI/ML techniques might not be the best option, especially if a lot of data needs to be sent over aerial networks [184]. Intelligent UAV networks can benefit from FL [185], which allows numerous UAVs to work together on learning tasks without sending raw data to BSs. This reduces the communication burden and protects data privacy [178].

8.2 Unsupervised Learning Methods

Unsupervised learning works with unlabelled data, in contrast to supervised learning. Without using predefined categories, it finds patterns and connections within the data. This can aid in anomaly detection in the IoT by highlighting unusual actions that might point to security vulnerabilities. It is critical to understand the fundamental methods in the field of unsupervised learning and how they enable IoT devices without requiring human interaction [186]. An array of techniques, such as anomaly detection, clustering, latent variable models, association mining, and more, fall under the umbrella of unsupervised learning [187].

Anomaly detection can uncover odd or unexpected actions within datasets, while clustering enables the system to arrange and combine related datasets into clusters [188]. Latent variable models are also used for information processing, like removing specific kinds of features from a dataset. This model's benefit is its capacity to identify any anomalies or atypical points in the system. Association mining is beneficial for finding patterns in a dataset that repeat, which is very helpful when spotting security vulnerabilities in an IoT network that occur regularly [189].

8.3 Reinforcement Learning Methods

Implementing reinforcement learning algorithms in IoT systems can empower IoT devices to autonomously select security protocols that effectively mitigate various types of threats [190]. Methods for reinforcement learning comprise multiple algorithms, such as "Q-learning, Dyna-Q, post-decision state (PDS), and deep Q-network (DQN)" [191]. This category of ML involves an operating agent learning to accomplish a task via repeated iterations of trial-and-error interactions with a dynamic environment. These methods deploy agents within an environment, allowing these agents to learn and make improved decisions through interactions with the environment. Within the model, such functional agents learn from experience and stimulate themselves according to the direction they are given. Furthermore, by increasing the effectiveness of processes like identifying malware and authentication, Q-learning empowers IoT devices to improve their security and confidentiality [192].

Artificial Neural Networks (ANN) belong to a class of models that aim to simulate the functioning of human brain neurons [193]. For instance, ANN can be effectively employed to categorize network traffic originating from IoT devices [194]. Support vector machines (SVMs) can be incorporated into the network to aid in the detection of intrusions and spoofing attacks [195]. Moreover, methods like the random forest classifier and K-nearest neighbours (KNN) are essential for spotting malicious ransomware and other IoT system disruptions [196].

Likewise, deep neural networks (DNNs) can be employed for detecting spoofing attacks within IoT technologies, provided they have sufficient memory and computational resources [197]. By putting these strategies into practice, IoT devices become more capable of identifying different actions occurring within the system and preventing certain dangerous acts. Using ML techniques, an experiment was carried out on IoT devices to detect harmful behaviours within their apps. The random forest and KNN classification approaches were used in this investigation to find malware [23].

The application of these techniques resulted in a remarkably high detection rate, with the random forest achieving a 99.7% detection rate and KNN achieving a 99.9% detection rate for spotting malware within the IoT system [198]. A genetic-KNN-based machine learning model called Malicious Activities Recognition in Water-based IIoT (MARWIIoT) was applied in a recent study. Different ML techniques are investigated to detect malicious activity in Android-based systems.

8.4 Explainable AI (XAI)

The term "explainable AI" (XAI) describes a collection of procedures and techniques that enable human users to understand and have faith in the results and decisions made by AI models [199]. Since AI judgments are typically viewed as "black boxes" because of their complexity, XAI becomes essential in the framework of AI-driven security systems because it meets the requirement for accountability, transparency, and trust in AI decisions [200]. Supervised learning involves training AI models on labelled data to make estimations. When it comes to security applications like fraud detection, where knowing the rationale behind an alert for unusual activity is necessary for taking further action, XAI assists in clarifying why a model has categorized a particular input in a certain way. For example, with the help of XAI, security analysts would be able to comprehend and have faith in the conclusions made by the system when it comes to identifying potential phishing emails. These aspects might include email content and sender reputation [201]. Grouping or clustering data without labelled results is known as unsupervised learning and XAI can assist in elucidating the foundation upon which clusters grow, which is crucial in cyber anomaly detection systems to find odd patterns that might point to a security breach [202].

As an illustration, XAI in network security can clarify why specific traffic patterns are categorized as possibly hostile, assisting security teams in interpreting alarms and implementing the necessary countermeasures [203]. XAI plays a critical role in reinforcement learning by understanding the agent's decision-making process, particularly in dynamic situations such as auto threat response systems [204]. As an example, XAI could explain to an AI-backed firewall why, in light of the reward signals it gets during training, the system decided to restrict specific kinds of traffic. This aids security teams in assessing and optimizing the behaviour of the system [205,206].

Future XAI systems will have to do the following [207–209]: provide context-aware explanations that take into account the particular circumstances surrounding a security decision; concentrate on creating methods that can produce explanations in real-time without slowing down the system's response [210]; support decentralized explanations, in which the justification for security decisions can be understood locally on each device without depending on a central authority [211]; concentrate on combining explainability with privacy-preserving techniques [212]; provide cross-domain explanations that are comprehensible to a variety of industries and user groups [213]; and concentrate on improving the relationship between AI systems and human operators [214].

8.5 Generative AI (GenAI)

GenAI is a family of AI models that uses patterns found in previously collected data to generate new material, such as text, photos, music, and even entire films [215]. GenAI generates new data that closely resembles the features of the original data it has been trained on, in contrast to typical AI models that are concentrated on classification or prediction tasks. While there are several ML techniques that can be used to create GenAI, unsupervised learning and reinforcement learning are the most often used approaches. "Variational Autoencoders (VAEs)" [216], "generative adversarial networks (GANs)" [217], and language models like GPT [218] are some of the most widely used examples of GenAI models.

The application of GenAI could be crucial in the development of self-learning IoT security systems in the future. These systems would be able to recognize and react to threats on their own by continually generating scenarios of possible attacks [219]. GenAI can assist in developing adaptive security measures, which provide a customizable line of defence by adjusting to the unique behaviours of particular users or devices [220]. GenAI can generate encryption keys specific to every communication session, increasing the security of communication between IoT devices and making it tougher for intruders to capture or decrypt data [221].

The area of generative AI is expanding across multiple disciplines thanks to a number of important projects [222]. Future work by DeepMind will focus on simulating intricate biological systems, while its AlphaFold project in healthcare aims to predict protein structures to speed up medication discovery. Users of OpenAI's DALL-E art [223] and design tool can generate graphics from text; the tool's capabilities will eventually be expanded to accommodate more complex designs. The integration of GenAI for real-time protection is a continuing endeavour to improve the detection and response of threats with IBM Watson for Cybersecurity [224]. Software developers can benefit from OpenAI's Codex, which helps with code production. Future updates will enable more languages and more challenging tasks. Last but not least, IBM is working to improve AI-powered communication through Project Debater, which could have an effect on policy-making and legal reasoning [225]. Table 9 presents the concise effectiveness of different AI methods in IoT security.

Table 9: Effectiveness of different AI methods in IoT security

AI methods	Effectiveness	Optimization with IoT	Example
Supervised learning	Labelled data is used to train models for classification tasks like malware and intrusion detection. By assigning predefined labels to input features, it is a useful tool for detecting known attack patterns in IoT systems.	Features selection and dimensionality reduction like principal component analysis for resource constrained environment.	In healthcare IoT networks, FL-based solutions are employed in which many hospitals work together to train a security model to identify anomalous activity without exchanging patient data. This method guarantees privacy compliance in addition to model accuracy.

(Continued)

Table 9 (continued)

AI methods	Effectiveness	Optimization with IoT	Example
Unsupervised learning	These methods examine unstructured or unlabelled data to find hidden patterns and anomalies. These techniques work especially well for IoT system anomaly detection, as new and unforeseen attack behaviours that aren't in preset datasets can appear.	To improve scalability, use self-organizing maps and deep clustering.	Its ability to classify similar patterns and indicate outliers makes it an excellent tool to recognize zero-day attacks and odd activity. This qualifies it for dynamic IoT contexts like industrial networks.
Reinforcement learning	These algorithms use feedback from their surroundings to iteratively learn the best course of action. Real-time threat mitigation and traffic anomaly detection are two tasks in IoT security where it proves to be an efficient and flexible solution. Since it doesn't require labelled data, it can be used in dynamic attack scenarios.	Reduce computational load with model compression and transfer learning.	In smart grids, these methods are used to dynamically optimize energy distribution and identify and prevent cyberattacks in real time, resulting in uninterrupted and efficient energy flow.
Explainable AI	XAI improves the transparency of AI-powered security systems by giving model decisions explanations that are understandable to humans. Enhancing credibility and accountability in crucial applications, it guarantees that stakeholders in IoT security know why a system reported an activity as malicious.	Incorporates techniques for interpretability that clarify security judgments.	XAI supports patient data monitoring in the healthcare industry and notifies medical professionals of irregularities with explicable causes. It makes security alarms in smart homes more understandable, such as strange movements, so that homeowners can better evaluate the threats. It improves user confidence and safety by explaining critical decisions made by autonomous cars, like abrupt braking.

(Continued)

Table 9 (continued)

AI methods	Effectiveness	Optimization with IoT	Example
Generative AI	For the purpose of training IoT security systems, these models, especially those that employ DL techniques, are very good at identifying anomalies and producing synthetic datasets. With a wider range of training data, these models can simulate several attack scenarios, increasing the security measures' resilience.	Specifically designed to enhance training efficacy by taking into account unique IoT situations.	Smart assistants, which offer tailored interactions, content creation tools that make writing assignments easier, and cutting-edge image generation platforms that support artists in producing original graphics are just a few examples of how GenAI is revolutionizing daily life.

Summary: This section investigates how different AI learning methods, such as GenAI, XAI, unsupervised learning, reinforcement learning, and supervised learning, can enhance IoT security. To reduce computational burden, AI implementation in IoT devices with restricted resources needs to use optimization techniques like quantization and pruning. Edge computing helps both supervised and unsupervised models by reducing latency, while reinforcement learning makes sure that models can adapt to changing conditions. FL ensures speed and privacy while enabling collaborative AI without centralized data. Transparency is boosted by XAI, while anomaly detection and predictive maintenance are supported by GenAI. These techniques improve security while preserving real-time responsiveness and are customized to meet IoT restrictions. DL alternatives like SVM, random forests, and KNN offer low latency and efficient real-time security solutions. These algorithms provide fast decision-making without requiring a lot of computational resources; they are lightweight and ideal for IoT environments.

9 Conclusion

In conclusion, the IoT grew quickly and offered unparalleled connectedness and ease to our lives. However, it has also led to a wide range of IoT problems, particularly in the area of IoT security. It became clear that protecting this enormous ecosystem calls for a multifaceted strategy, as we investigated the intricate details of IoT architecture and its essential security aspects. It is crucial to understand how the attack landscape for each IoT layer is changing. The attack landscape is complex and constantly changing, spanning the physical layer to the application layer. Recent attacks on the IoT are also revealed in this study. It also presents the current challenges in IoT along with their real-world solutions, practical examples, and the possible future. It also offers practical case studies and uses examples that exemplify how AI is being applied to secure IoT systems in a variety of industries, such as the industrial IoT, smart homes, smart cities, healthcare, smart grids, and smart agriculture.

As we look into the future of IoT security, it is evident that the incorporation of AI technology will play a more significant role. However, researchers, programmers, and decision-makers must keep working together and innovating to chart the road for a safe and secure IoT environment in the years to come. By doing so, we can fully utilize the IoT while protecting our information, devices, and linked world.

As the IoT grows and changes, future research should concentrate on tackling new security issues, investigating novel AI strategies, and guaranteeing the ethical and responsible application of AI in IoT security.

Acknowledgement: None.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: literature review and analysis: Ali Hassan, N. Nizam-Uddin; study conception and design: Ali Hassan, N. Nizam-Uddin, Ateeq Ur Rehman; data collection: Ali Hassan, N. Nizam-Uddin; critical analysis and interpretation of results: Ali Hassan, N. Nizam-Uddin, Asim Quddus, Syed Rizwan Hassan; draft manuscript preparation: Ali Hassan, N. Nizam-Uddin, Asim Quddus, Ateeq Ur Rehman, Salil Bharany. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] J. Sun, W. Gan, H. -C. Chao, S. Y. Philip, and W. Ding, "Internet of behaviors: A survey," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11117–11134, 2023. doi: 10.1109/JIOT.2023.3247594.

[2] L. B. Furstenau *et al.*, "Internet of things: Conceptual network structure, main challenges and future directions," *Digit. Commun. Netw.*, vol. 9, no. 3, pp. 677–687, 2023. doi: 10.1016/j.dcan.2022.04.027.

[3] A. H. Najim, and S. Kurnaz, "Study of integration of wireless sensor network and Internet of Things (IoT)," *Wireless Pers. Commun.*, vol. 15, no. 4, 2023. doi: 10.1007/s11277-023-10556-4.

[4] M. Pons, E. Valenzuela, B. Rodríguez, J. A. Nolazco-Flores, and C. Del-Valle-Soto, "Utilization of 5G technologies in IoT applications: Current limitations by interference and network optimization difficulties—A review," *Sensors*, vol. 23, no. 8, 2023, Art. no. 3876. doi: 10.3390/s23083876.

[5] Y. B. Zikria, R. Ali, M. K. Afzal, and S. W. Kim, "Next-generation Internet of Things (IoT): Opportunities, challenges, and solutions," *Sensors*, vol. 21, no. 4, 2021, Art. no. 1174. doi: 10.3390/s21041174.

[6] C. Kaur, "The cloud computing and internet of things (IoT)," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 7, no. 1, pp. 19–22, 2020. doi: 10.32628/IJSRSET.

[7] O. Vermesan *et al.*, "Internet of things strategic research roadmap," in *Internet of Things-Global Technological and Societal Trends from Smart Environments and Spaces to Green Ict*, 1st ed. River Publishers, 2022, pp. 9–52.

[8] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Comput. Netw.*, vol. 144, pp. 17–39, 2018. doi: 10.1016/j.comnet.2018.07.017.

[9] A. Aziz, O. Schelén, and U. Bodin, "A study on industrial IoT for the mining industry: Synthesized architecture and open research directions," *IoT*, vol. 1, no. 2, pp. 529–550, 2020. doi: 10.3390/iot1020029.

[10] C. Bodei, S. Chessa, and L. Galletta, "Measuring security in IoT communications," *Theor Comput. Sci.*, vol. 764, no. 3–5, pp. 100–124, 2019. doi: 10.1016/j.tcs.2018.12.002.

[11] M. A. I. Mallick and R. Nath, "Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments," *World Sci. News.*, vol. 190, no. 1, pp. 1–69, 2024.

[12] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen and B. Stiller, "Landscape of IoT security," *Comput. Sci. Rev.*, vol. 44, 2022, Art. no. 100467. doi: 10.1016/j.cosrev.2022.100467.

[13] B. Hammi, S. Zeadally, and J. Nebhen, "Security threats, countermeasures, and challenges of digital supply chains," *ACM Comput. Surv.*, vol. 55, no. 14s, pp. 1–40, 2023, Art. no. 316. doi: 10.1145/3588999.

[14] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid and M. Assiri, "Securing the Internet of Things in artificial intelligence era: A comprehensive survey," *IEEE Access*, vol. 12, 2024. doi: 10.1109/ACCESS.2024.3365634.

[15] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: A survey," *Clust. Comput.*, vol. 27, no. 7, pp. 1–25, 2024. doi: 10.1007/s10586-024-04509-0.

[16] A. Pakmehr, A. Aßmuth, N. Taheri, and A. Ghaffari, "DDoS attack detection techniques in IoT networks: A survey," *Clust. Comput.*, vol. 27, no. 10, pp. 1–32, 2024. doi: 10.1007/s10586-024-04662-6.

[17] P. Sun, S. Shen, Y. Wan, Z. Wu, Z. Fang and X. -Z Gao, "A survey of IoT privacy security: Architecture, technology, challenges, and trends," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 34567–34591, 2024. doi: 10.1109/JIOT.2024.3372518.

[18] H. Taherdoost, "Security and internet of things: Benefits, challenges, and future perspectives," *Electronics*, vol. 12, no. 8, 2023, Art. no. 1901. doi: 10.3390/electronics12081901.

[19] S. Rekha, L. Thirupathi, S. Renikunta, and R. Gangula, "Study of security issues and solutions in Internet of Things (IoT)," *Mater. Today: Proc.*, vol. 80, no. 9, pp. 3554–3559, 2023. doi: 10.1016/j.matpr.2021.07.295.

[20] M. Ahmid and O. Kazar, "A comprehensive review of the internet of things security," *J. Appl. Secur. Res.*, vol. 18, no. 3, pp. 289–305, 2023. doi: 10.1080/19361610.2021.1962677.

[21] J. Zhao, H. Hu, F. Huang, Y. Guo, and L. Liao, "Authentication technology in Internet of Things and privacy security issues in typical application scenarios," *Electronics*, vol. 12, no. 8, 2023, Art. no. 1812. doi: 10.3390/electronics12081812.

[22] G. Alqarawi, B. Alkhalifah, N. Alharbi, and S. El Khediri, "Internet-of-Things security and vulnerabilities: Case study," *J. Appl. Secur. Res.*, vol. 18, no. 3, pp. 559–575, 2023. doi: 10.1080/19361610.2022.2031841.

[23] A. K. Abed and A. Anupam, "Review of security issues in Internet of Things and artificial intelligence-driven solutions," *Secur. Privacy*, vol. 6, no. 3, 2023, Art. no. e285. doi: 10.1002/spy2.285.

[24] J. Mohanty, S. Mishra, S. Patra, B. Pati, and C. R. Panigrahi, "IoT security, challenges, and solutions: A review,," presented at the Prog. Adv. Comput. Intell. Eng.: Proc ICACIE 2019, 2021.

[25] A. Jelić, "What is architecture for? Designing as enriching the landscape of affordances," *Adapt. Behav.*, vol. 30, no. 6, pp. 585–587, 2022. doi: 10.1177/1059712321994686.

[26] Y. Lu and J. Cecil, "An Internet of Things (IoT)-based collaborative framework for advanced manufacturing," *Int. J. Adv. Manuf. Technol.*, vol. 84, no. 2, pp. 1141–1152, 2016. doi: 10.1007/s00170-015-7772-0.

[27] M. A. Jabraeil Jamali *et al.*, "IoT architecture," in *Towards the Internet of Things*, 1st ed. Cham, Switzerland: Springer, 2020, pp. 9–31.

[28] Y. Fan *et al.*, "SNPL: One scheme of securing nodes in IoT perception layer," *Sensors*, vol. 20, no. 4, 2020, Art. no. 1090. doi: 10.3390/s20041090.

[29] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: A survey," *Wirel Pers. Commun.*, vol. 115, no. 2, pp. 1667–1693, 2020. doi: 10.1007/s11277-020-07649-9.

[30] Y. Al-Hadhrami and F. K. Hussain, "Real time dataset generation framework for intrusion detection systems in IoT," *Futur Gener. Comput. Syst.*, vol. 108, no. 1, pp. 414–423, 2020. doi: 10.1016/j.future.2020.02.051.

[31] M. Vaezi *et al.*, "Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 1117–1174, 2022. doi: 10.1109/COMST.2022.3151028.

[32] J. Qadir, "Cybersecurity in LoRaWAN networks: Vulnerability analysis and enhancing security measures for IoT connectivity," Ph.D. dissertation, Naval, Elect. Eng., Univ. Studi Genova, Genova, Italy, 2024.

[33] T. Alam, "Design a blockchain-based middleware layer in the Internet of Things architecture," *Int. J. Informat. Vis.*, vol. 4, no. 1, pp. 28–31, 2020. doi: 10.30630/joiv.4.1.334.

[34] A. Khanna and S. Kaur, "Internet of things (IoT), applications and challenges: A comprehensive review," *Wirel Pers. Commun.*, vol. 114, no. 2, pp. 1687–1762, 2020. doi: 10.1007/s11277-020-07446-4.

[35] H. Uddin *et al.*, "IoT for 5G/B5G applications in smart homes, smart cities, wearables and connected cars," in *2019 IEEE CAMAD*, Limassol, Cyprus, IEEE, 2019, pp. 1–5. doi: 10.1109/CAMAD.2019.8858455.

[36] E. U. Aydınocak, "Internet of things (IoT) in marketing logistics," in *Logistics 4.0 and Future of Supply Chains*, Singapore: Springer, 2021, pp. 153–169. doi: 10.1007/978-981-16-5644-6.

[37] T. Han, K. Muhammad, T. Hussain, J. Lloret, and S. W. Baik, "An efficient deep learning framework for intelligent energy management in IoT networks," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3170–3179, 2020. doi: 10.1109/JIOT.2020.3013306.

[38] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities," *IoT Commun., Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, 2022, Art. no. e3677. doi: 10.1002/ett.3677.

[39] Y. Zhang, Q. He, G. Chen, X. Zhang, and Y. Xiang, "A low-overhead, confidentiality-assured, and authenticated data acquisition framework for IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 12, pp. 7566–7578, 2019. doi: 10.1109/TII.2019.2957404.

[40] C. K. D. S. Rodrigues and V. Rocha, "Towards blockchain for suitable efficiency and data integrity of IoT ecosystem transactions," *IEEE Lat. Am. Trans.*, vol. 19, no. 7, pp. 1199–1206, 2021. doi: 10.1109/TLA.2021.9461849.

[41] M. Kokila and S. Reddy, "Authentication, Access control and scalability models in Internet of Things security–A review," *Cyber Secur. Appl.*, vol. 3, 2024, Art. no. 100057. doi: 10.1016/j.csa.2024.100057.

[42] M. Devi and A. Majumder, "Side-channel attack in Internet of Things: A survey," in *Appl. Internet Things: Proc. ICCCIOT 2020*, Singapore, Springer, 2021, pp. 213–222. doi: 10.1007/978-981-15-6198-6_20.

[43] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: A state of the art review," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–15, 2020. doi: 10.1186/s13638-020-01665-w.

[44] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on IoT platforms: Communication, security, and privacy perspectives," *Comput. Netw.*, vol. 192, 2021, Art. no. 108040. doi: 10.1016/j.comnet.2021.108040.

[45] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 21, 2020, Art. no. e4946. doi: 10.1002/cpe.4946.

[46] M. M. Nasralla, I. García-Magariño, and J. Lloret, "Defenses against perception-layer attacks on IoT smart furniture for impaired people," *IEEE Access*, vol. 8, pp. 119795–119805, 2020. doi: 10.1109/ACCESS.2020.3004814.

[47] X. Yang, L. Shu, Y. Liu, G. P. Hancke, M. A. Ferrag and K. Huang, "Physical security and safety of IoT equipment: A survey of recent advances and opportunities," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4319–4330, 2022. doi: 10.1109/TII.2022.3141408.

[48] N. Ambika, "Tackling jamming attacks in IoT," in *Internet of Things (IoT)*, M. Alam, K. Shakil, S. Khan, Eds. Singapore: Springer, 2020, pp. 153–165.

[49] K. Fang, T. Wang, X. Yuan, C. Miao, Y. Pan and J. Li, "Detection of weak electromagnetic interference attacks based on fingerprint in IIoT systems," *Futur Gener. Comput. Syst.*, vol. 126, no. 3, pp. 295–304, 2022. doi: 10.1016/j.future.2021.08.020.

[50] N. -F. Polychronou, P. -H. Thevenon, M. Puys, and V. Beroulle, "A comprehensive survey of attacks without physical access targeting hardware vulnerabilities in IoT/IIoT devices, and their detection mechanisms," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 27, no. 1, pp. 1–35, 2021. doi: 10.1145/3471936.

[51] M. Devi and A. Majumder, "Side-channel attack in Internet of Things: A survey," in *Appl. Internet Things: Proc. ICCCIOT 2020*, Springer, 2021, pp. 213–222.

[52] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," *Sustain. Eng. Innov.*, vol. 3, no. 1, pp. 23–28, 2021. doi: 10.37868/sei.v3i1.124.

[53] H. Aldabbas and R. Amin, "A novel mechanism to handle address spoofing attacks in SDN based IoT," *Clust. Comput.*, vol. 24, no. 4, pp. 3011–3026, 2021. doi: 10.1007/s10586-021-03309-0.

[54] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues and Y. Park, "Designing efficient sinkhole attack detection mechanism in edge-based IoT deployment," *Sensors*, vol. 20, no. 5, 2020, Art. no. 1300. doi: 10.3390/s20051300.

[55] A. Arshad, Z. M. Hanapi, S. Subramaniam, and R. Latip, "A survey of Sybil attack countermeasures in IoT-based wireless sensor networks," *PeerJ Comput. Sci.*, vol. 7, no. 2, 2021, Art. no. e673. doi: 10.7717/peerj-cs.673.

[56] G. E. Rodríguez, J. G. Torres, P. Flores, and D. E. Benavides, "Cross-site scripting (XSS) attacks and mitigation: A survey," *Comput. Netw.*, vol. 166, 2020, Art. no. 106960. doi: 10.1016/j.comnet.2019.106960.

[57] S. Evmorfos, G. Vlachodimitropoulos, N. Bakalos, and E. Gelenbe, "Neural network architectures for the detection of SYN flood attacks in IoT systems," in *Proc. 13th ACM Int. Conf. Pervasive Technol. Assist. Environ.*, 2020, pp. 1–4. doi: 10.1145/3389189.339800.

[58] D. Stiawan, M. E. Suryani, M. Y. Idris, M. N. Aldalaien, N. Alsharif and R. Budiarto, "Ping flood attack pattern recognition using a K-means algorithm in an Internet of Things (IoT) network," *IEEE Access*, vol. 9, pp. 116475–116484, 2021. doi: 10.1109/ACCESS.2021.3105517.

[59] P. Nuthakki and T. Gunasekhar, "A study on security issues and attacks, challenges and future improvements in cloud-based IoT," *Int. J. Sens. Wireless Commun. Control*, vol. 12, no. 2, pp. 96–107, 2022. doi: 10.2174/2210327911666210111124057.

[60] S. Modak, K. Majumder, and D. De, "Vulnerability of cloud: Analysis of XML signature wrapping attack and countermeasures," in *Proc. Int. Conf. Front. Comput. Syst.: COMSYS 2020*, Singapore, Springer, 2021, pp. 755–765. doi: 10.1007/978-981-15-7834-2_70.

[61] D. Swessi and H. Idoudi, "A survey on internet-of-things security: Threats and emerging countermeasures," *Wirel. Pers. Commun.*, vol. 124, no. 2, pp. 1557–1592, 2022. doi: 10.1007/s11277-021-09420-0.

[62] N. A. M. Alhammadi and K. H. Zaboon, "A review of IoT applications, attacks and its recent defense methods," *J. Glob. Sci. Res.*, vol. 7, no. 3, pp. 2128–2134, 2022. doi: 10.17148/IJIREEICE.2024.12433.

[63] V. V. Rao, R. Marshal, and K. Gobinath, "The IoT supply chain attack trends-vulnerabilities and preventive measures," in *2021 4th Int. Conf. Secur. Privacy (ISEA-ISAP)*, Dhanbad, India, IEEE, 2021, pp. 1–4.

[64] G. Nebbione and M. C. Calzarossa, "Security of IoT application layer protocols: Challenges and findings," *Futur Internet*, vol. 12, no. 3, 2020, Art. no. 55. doi: 10.3390/fi12030055.

[65] H. A. Noman and O. M. F. Abu-Sharkh, "Code injection attacks in wireless-based Internet of Things (IoT): A comprehensive review and practical implementations," *Sensors*, vol. 23, no. 13, 2023, Art. no. 6067. doi: 10.3390/s23136067.

[66] Y. Guo, "A review of machine learning-based zero-day attack detection: Challenges and future directions," *Comput. Commun.*, vol. 198, no. 10, pp. 175–185, Jan. 15, 2023. doi: 10.1016/j.comcom.2022.11.001.

[67] H. Kim and E. A. Lee, "Authentication and authorization for the Internet of Things," *IT Prof.*, vol. 19, no. 5, pp. 27–33, 2017. doi: 10.1109/MITP.2017.3680960.

[68] M. Bruce, J. Lusthaus, R. Kashyap, N. Phair, and F. Varese, "Mapping the global geography of cybercrime with the World Cybercrime Index," *PLoS One*, vol. 19, no. 4, 2024, Art. no. e0297312. doi: 10.1371/journal.pone.0297312.

[69] W. E. Forum, "Global cybersecurity outlook 2024," Switzerland, 2024. Accessed: Sep. 15, 2024. [Online]. Available: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

[70] Verizon, "2024 data breach investigations report," USA, 2024. Accessed: Sep. 15, 2024. [Online]. Available: https://www.verizon.com/business/resources/Tf8/reports/2024-dbir-data-breach-investigations-report.pdf

[71] N. A. Bitdefender, "The 2024 IoT security landscape report," Romania, 2024. Accessed: Sep. 15, 2024. [Online]. Available: https://blogapp.bitdefender.com/hotforsecurity/content/files/2024/06/2024-IoT-Security-Landscape-Report_consumer.pdf

[72] SOCRadar, "FRANCE threat landscape report," USA, 2024. Accessed: Aug. 10, 2024. [Online]. Available: https://socradar.io/wp-content/uploads/2024/07/SOCRadar-France-Threat-Landscape-Report-2024.pdf

[73] U. Group, "UNH-Q1-2024-release," USA, 2024. Accessed: Aug. 2, 2024. [Online]. Available: https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2024/UNH-Q1-2024-Release.pdf

[74] M. Grindey, "Rethinking how you safeguard data," *Comput. Fraud Secur.*, vol. 2024, no. 6, 2024. doi: 10.12968/S1361-3723(24)70022-0.

[75] Roku, "Notice of data breach," USA, 2024. Accessed: Aug. 3, 2024. [Online]. Available: https://thenationaldesk.com/resources/pdf/85786bd1-fb34-49ea-8ab2-53270b82d6a4-TemplateNotification3820241.pdf

[76] D. S. A. S. Ilanbey, *Internet Provider Tangerine Suffers Cyberattack*. Sydney, Australia: Sydney Morning Herald, 2024.

[77] SOCRadar, "MID-YEAR CYBER SECURITY review report," USA, 2024. Accessed: Aug. 4, 2024. [Online]. Available: https://socradar.io/wp-content/uploads/2024/07/SOCRadar-2024-Mid-Year-Cybersecurity-Report.pdf

[78] V. AG, *VARTA Affected by Cyber ATtack*. Ellwangen, Germany: VARTA, 2024.

[79] T. R. B. A. Y. Cherrat, "Cyber threats and engagements in 2022," USA, 2023. Accessed: Aug. 4, 2024. [Online]. Available: https://apps.dtic.mil/sti/trecms/pdf/AD1208002.pdf

[80] L. Einler Larsson and K. Qollakaj, "Cybersecurity of remote work migration: A study on the VPN security landscape post COVID-19 outbreak," M.S. thesis, Dept. of Comp. Sci., Karlskrona, Sweden, 2023. Accessed: Nov. 11, 2024. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1778036/FULLTEXT03

[81] M. Kirov, "Cyber security risks and opportunities of artificial intelligence: A qualitative study: How AI would form the future of cyber security," Sch. of Inf. Technol., Halmstad Univ., Halmstad, Sweden, 2023. Accessed: Nov. 11, 2024. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1775451/FULLTEXT02

[82] Socradar, "Education threat landscape report," USA, 2023. Accessed: Aug. 10, 2024. [Online]. Available: https://socradar.io/wp-content/uploads/2023/02/Education-Threat-Landscape-Report-v3.pdf

[83] A. D. H. Agency, "Cyber security report 2022," Australia, 2023. Accessed: Aug. 10, 2024. [Online]. Available: https://www.digitalhealth.gov.au/sites/default/files/documents/cyber-security-report-2022.pdf

[84] N. A. Hassan, "Ransomware overview," in *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks*, Berkeley, CA, USA: Apress, 2019, pp. 3–28.

[85] A. Lubin, "The law and politics of ransomware," *55 Vanderbilt J. Trans. Law 1177*, 2022. Accessed: Nov. 11, 2024. [Online]. Available: https://www.repository.law.indiana.edu/facpub/3063

[86] A. Dalvi, S. Maddala, and D. Suvarna, "Threat modelling of smart light bulb," in *2018 4th Int. Conf. Comput. Commun. Control Autom. (ICCUBEA)*, Pune, India, IEEE, 2018, pp. 1–4. doi: 10.1109/ICCUBEA.2018.8697723.

[87] L. E. S. Jaramillo, "Malware detection and mitigation techniques: Lessons learned from Mirai DDOS attack," *J. Inf. Syst. Eng. Manag.*, vol. 3, no. 3, 2018, Art. no. 19. doi: 10.20897/jisem/2655.

[88] A. Chadd, "DDoS attacks: Past, present and future," *Netw. Secur.*, vol. 2018, no. 7, pp. 13–15, 2018. doi: 10.1016/S1353-4858(18)30069-2.

[89] H. Griffioen and C. Doerr, "Examining mirai's battle over the internet of things," in *Proc. 2020 ACM SIGSAC Conf. Comput. Commun. Secur.*, 2020, pp. 743–756. doi: 10.1145/3372297.3417277.

[90] Integrity360, “The biggest cyber attacks of 2023,” 2023. Accessed: Aug. 10, 2024. [Online]. Available: https://insights.integrity360.com/the-biggest-cyber-attacks-of-2023-so-far-part-2

[91] T. Moffitt, “How SMBs can defeat the threat of ransomware,” *Netw. Secur.*, vol. 2023, no. 7, 2023. doi: 10.12968/S1353-4858(23)70033-0.

[92] O. Analytica, “UK royal mail attack exposes Russian crime risks,” in *Expert Briefings. UK: Emerald Publishing*, 2023. doi: 10.1108/OXAN-ES275289.

[93] M. Horduna, S. -M. Lăzărescu, and E. Simion, “A note on machine learning applied in ransomware detection,” *Cryptol. ePrint Arch.*, 2023. Accessed: Aug. 28, 2024. [Online]. Available: https://eprint.iacr.org/2023/045

[94] B. Toulas, “Cyber security incident regarding historic orders,” LSEG. 2023. Accessed: Aug. 28, 2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/jd-sports-says-hackers-stole-data-of-10-million-customers/

[95] J. S. F. PLC, “Cyber security incident regarding historic orders,” 2023. Accessed: Aug. 11, 2024. [Online]. Available: https://www.londonstockexchange.com/news-article/JD./cyber-security-incident-regarding-historic-orders/15815662

[96] J. Von der Assen, A. H. Celdrán, R. Sefa, G. Bovet, and B. Stiller, “MTFS: A moving target defense-enabled file system for malware mitigation,” in *2024 IEEE 49th Conf*., LCN, Normandy, France, 2024, pp. 1–6. doi: 10.1109/LCN60385.2024.10639803.

[97] L. Abrams, “BleepingComputer,” 2023. Accessed: Aug. 28, 2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/multinational-tech-firm-abb-hit-by-black-basta-ransomware-attack/

[98] S. S. Albouq, A. A. Abi Sen, N. Almashf, M. Yamin, A. Alshanqiti and N. M. Bahbouh, “A survey of interoperability challenges and solutions for dealing with them in IoT environment,” *IEEE Access*, vol. 10, pp. 36416–36428, 2022. doi: 10.1109/ACCESS.2022.3162219.

[99] H. Rasheed, A. A. Salih, O. M. Ahmed, A. A. Yazdeen, R. Majeed and T. M. G. S. Abdullah, “Consideration of cloud-web-concepts for standardization and interoperability: A comprehensive review for sustainable enterprise systems, AI, and IoT integration,” *J. Inf. Technol. Inform.*, vol. 3, no. 2, pp. 129–156, 2024.

[100] A. Pal, H. K. Rath, S. Shailendra, and A. Bhattacharyya, “IoT standardization: The road ahead,” in *Internet of Things-Technology, Applications and Standardization*, London, UK: IntechOpen, 2018, pp. 53–74.

[101] M. C. Marin, M. Cerutti, S. Batista, and M. Brambilla, “A multi-protocol IoT platform for enhanced interoperability and standardization in smart home,” in *2024 IEEE 21st Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, IEEE, 2024, pp. 1–6. doi: 10.1109/CCNC51664.2024.10454663.

[102] A. Gupta, R. Christie, and R. Manjula, “Scalability in internet of things: Features, techniques and research challenges,” *Int. J. Comput. Intell. Res.*, vol. 13, no. 7, pp. 1617–1627, 2017.

[103] W. Rafique and M. A. Shah, “Performance evaluation of IoT network infrastructure,” in *2016 22nd Int. Conf. Automat. Comput. (ICAC)*, IEEE, 2016, pp. 348–353. doi: 10.1109/IConAC.2016.7604944.

[104] J. M. Kizza, “Internet of things (IoT): Growth, challenges, and security,” in *Guide Comput. Netw. Secur. Texts Comput. Sci.*, Springer, 2024, pp. 557–573.

[105] L. Liu, D. Essam, and T. Lynar, “Complexity measures for IoT network traffic,” *IEEE Internet Things J.*, vol. 9, no. 24, pp. 25715–25735, 2022. doi: 10.1109/JIOT.2022.3197323.

[106] B. Diène, J. J. Rodrigues, O. Diallo, E. H. M. Ndoye, and V. V. Korotaev, “Data management techniques for Internet of Things,” *Mech. Syst. Signal Process*, vol. 138, 2020, Art. no. 106564. doi: 10.1016/j.ymssp.2019.106564.

[107] A. Karale, “The challenges of IoT addressing security, ethics, privacy, and laws,” *Internet Things*, vol. 15, 2021, Art. no. 100420. doi: 10.1016/j.iot.2021.100420.

[108] Y. Wu *et al.*, “Your firmware has arrived: A study of firmware update vulnerabilities,” in *33rd USENIX Secur. Symp. (USENIX Secur. 24)*, Philadelphia, PA, USA, 2023.

[109] S. El Jaouhari and E. Bouvet, “Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions,” *Internet Things*, vol. 18, 2022, Art. no. 100508. doi: 10.1016/j.iot.2022.100508.

[110] S. R. Boyd, “Over-the-air in personam: Purposeful availment through over-the-air updates,” *SCL Rev.*, vol. 75, no. 3, 2023, Art. no. 495.

[111] N. Dissanayake, A. Jayatilaka, M. Zahedi, and M. A. Babar, “Software security patch management-A systematic literature review of challenges, approaches, tools and practices,” *Inf. Softw. Technol.*, vol. 144, 2022, Art. no. 106771. doi: 10.1016/j.infsof.2021.106771.

[112] S. SakthiMurugan, S. Kumaar, V. Vignesh, and P. Santhi, “Assessment of zero-day vulnerability using machine learning approach,” *EAI Endorsed Trans. Internet Things*, vol. 10, 2024. doi: 10.4108/eetiot.4978.

[113] S. Zhang, H. Sullivan, K. K. Lahoti, and H. H. Gharakheili, “Systematic verification of IoT device conformance to IETF manufacturer usage description standard,” *TechRxiv*, pp. 1–8, 2024. doi: 10.36227/techrxiv.172054933.38594592/v1.

[114] C. Crawford, “Protocol power: Matter, IoT interoperability, and a critique of industry self-regulation,” *Internet Policy Rev.*, vol. 13, no. 2, pp. 1–26, 2024. doi: 10.14763/2024.2.1776.

[115] S. Singh, “Intercompatibility of IoT devices using matter: Next-generation IoT connectivity protocol,” in *Advances in IoT and Security with Computational Intelligence*, Singapore: Springer, 2023, pp. 49–58. doi: 10.1007/978-981-99-5088-1_5.

[116] A. Coiduras-Sanagustín, E. Manchado-Pérez, and C. García-Hernández, “Understanding perspectives on personal data privacy in Internet of Things (IoT): A systematic literature review (SLR),” *Heliyon*, vol. 10, no. 9, 2024. doi: 10.1016/j.heliyon.2024.e30357.

[117] M. Siddireddy, “A lightweight end-to-end encryption algorithm for IoT data integration: Blockchain framework,” M.S. thesis, SIU Carbondale, Carbondale, IL, USA, 2024.

[118] A. M. Hussain, G. Oligeri, and T. Voigt, “The dark (and bright) side of IoT: Attacks and countermeasures for identifying smart home devices and services,” in *Secur., Priv., Anonym. Comput., Commun., Storage: SpaCCS 2020 Int. Workshops*, Nanjing, China, Springer, 2020, pp. 122–136.

[119] Y. Zhang and Z. Fan, “Research on zero knowledge with machine learning,” *J. Comput. Electron. Inf. Manag.*, vol. 12, no. 2, pp. 105–108, 2024. doi: 10.54097/6awase9w.

[120] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, “Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions,” *J. Ambient Intell. Humaniz. Comput.*, vol. 15, no. 2, pp. 1–18, 2024. doi: 10.1007/s12652-017-0494-4.

[121] G. K. Mahato and S. K. Chakraborty, “Securing edge computing using cryptographic schemes: A review,” *Multimed. Tools Appl.*, vol. 83, no. 12, pp. 34825–34848, 2024. doi: 10.1007/s11042-023-15592-7.

[122] P. Suryateja and K. V. Rao, “A survey on lightweight cryptographic algorithms in IoT,” *Cybern. Inf. Technol.*, vol. 24, no. 1, pp. 21–34, 2024. doi: 10.2478/cait-2024-0002.

[123] A. K. Reddy Ayyadapu, “Optimizing incident response in cloud security with AI and big data integration,” *Chelon. Res. Found.*, vol. 18, no. 2, pp. 2212–2225, 2023.

[124] K. R. Saraf and P. Malathi, “Cyber physical system security by Splunk,” *i-Manag. J. Commun. Eng. Syst.*, vol. 9, no. 2, 2020. doi: 10.26634/jcs.9.2.18115.

[125] Darktrace, “The next paradigm shift AI-driven cyber-attacks,” UK, 2020. Accessed: Aug. 11, 2024. [Online]. Available: https://www.oixio.ee/sites/default/files/the_next_paradigm_shift_-_ai_driven_cyber_attacks.pdf

[126] M. Copeland, “Cloud defense strategies with azure sentinel: hands-on threat hunting in cloud logs services,” in *Azure Sentinel Overview*, Berkeley, CA, USA: Apress, 2021, pp. 3–38.

[127] V. Sivagami, M. Deekshitha, N. Devi, and S. S. Parvathi, “Authentication, authorization, and anonymization techniques in the IoT,” in *Secure Communication in Internet of Things*, 1st ed. Boca Raton, FL, USA: CRC Press, 2024, pp. 94–106.

[128] C. Wheelus and X. Zhu, “IoT network security: Threats, risks, and a data-driven defense framework,” *IoT*, vol. 1, no. 2, pp. 259–285, 2020. doi: 10.3390/iot1020016.

[129] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista and M. Conti, “A survey on decentralized identifiers and verifiable credentials,” presented at the ICBTA 2020 (3rd Int. Conf. Blockchain Technol. Appl.), 2024.

[130] E. O. Udeh, P. Amajuoyi, K. B. Adeusi, and A. O. Scott, “The role of IoT in boosting supply chain transparency and efficiency,” *Magna Sci. Adv. Res. Rev.*, vol. 12, no. 1, pp. 178–197, 2024. doi: 10.30574/msarr.2024.11.1.0081.

[131] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, “A survey on supply chain security: Application areas, security threats, and solution architectures,” *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6222–6246, 2020. doi: 10.1109/JIOT.2020.3025775.

[132] P. Borra, “Impact and innovations of azure IoT: Current applications, services, and future directions,” *Int. J. Recent Technol. Eng.*, vol. 13, no. 2, pp. 2277–3878, 2024. doi: 10.35940/ijrte.B8111.13020724.

[133] N. Mangala *et al.*, “Secure pharmaceutical supply chain using blockchain in IoT cloud systems,” *Internet Things*, vol. 26, 2024, Art. no. 101215. doi: 10.1016/j.iot.2024.101215.

[134] O. A. Adenekan, N. O. Solomon, P. Simpa, and S. C. Obasi, “Enhancing manufacturing productivity: A review of AI-Driven supply chain management optimization and ERP systems integration,” *Int. J. Manag. Entrep. Res.*, vol. 6, no. 5, pp. 1607–1624, 2024. doi: 10.51594/ijmer.v6i5.1126.

[135] A. Aldaej, T. A. Ahanger, M. Atiquzzaman, and I. Ullah, “A comprehensive node-based botnet detection framework for IoT network,” *Clus. Comput.*, vol. 27, no. 7, pp. 1–21, 2024. doi: 10.1007/s10586-024-04379-6.

[136] A. P. Shende, B. Shiragpur, G. Raj, and P. Tamhankar, “Securing the future,” in *Modelling of Virtual Worlds Using the Internet of Things*, 1st ed. Boca Raton, FL, USA: CRC Press, 2024, p. 19.

[137] A. B. Huang, “Betrusted: Improving security through physical partitioning,” *IEEE Pervasive Comput.*, vol. 19, no. 2, pp. 13–20, 2020. doi: 10.1109/MPRV.2020.2966190.

[138] A. A. Soofi, M. Tahir, and N. Raza, “Securing the Internet of Things: A comprehensive review of security challenges and artificial intelligence solutions,” *Found Univ. J. Eng. Appl. Sci.*, vol. 4, no. 2, pp. 1–20, 2024. doi: 10.33897/fujeas.v4i2.779.

[139] A. F. Gentile, D. Macrì, F. De Rango, M. Tropea, and E. Greco, “A VPN performances analysis of constrained hardware open source infrastructure deploy in IoT environment,” *Future Internet*, vol. 14, no. 9, 2022, Art. no. 264. doi: 10.3390/fi14090264.

[140] A. Tambe *et al.*, “Detection of threats to IoT devices using scalable VPN-forwarded honeypots,” in *Proc. 9th ACM Conf. Data Appl. Securr. Priv.*, 2019, pp. 85–96. doi: 10.1145/3292006.3300024.

[141] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, “Securing IoT devices: A novel approach using blockchain and quantum cryptography,” *Internet Things*, vol. 25, 2024, Art. no. 101019. doi: 10.1016/j.iot.2023.101019.

[142] A. Hassebo and M. Tealab, “Global models of smart cities and potential IoT applications: A review,” *IoT*, vol. 4, no. 3, pp. 366–411, 2023. doi: 10.3390/iot4030017.

[143] P. Lea, *Edge Computing Simplified: Explore All Aspects of Edge Computing for Business Leaders and Technologists*. Birmingham, UK: Packt Publishing Ltd., 2024.

[144] Z. Zheng, Y. Zhou, Y. Sun, Z. Wang, B. Liu and K. Li, “Applications of federated learning in smart cities: Recent advances, taxonomy, and open challenges,” *Connect. Sci.*, vol. 34, no. 1, pp. 1–28, 2022. doi: 10.1080/09540091.2021.1936455.

[145] C. L. Ni and S. Cang, “Machine learning enabled industrial IoT security: Challenges, trends and solutions,” *J. Ind. Inf. Integr.*, vol. 38, 2024, Art. no. 100549. doi: 10.1016/j.jii.2023.100549.

[146] D. Job and V. Paul, “Challenges, security mechanisms, and research areas in IoT and IIoT,” in *Internet of Things and Its Applications.*, Cham: Springer, 2022, pp. 523–538.

[147] J. Cecílio and A. Souto, “Security issues in industrial Internet-of-Things: Threats, attacks and solutions,” in *2024 IEEE Int. Workshop Metrol. Ind. 4.0 IoT (MetroInd4.0 and IoT)*, IEEE, 2024, pp. 458–463. doi: 10.1109/MetroInd4.0IoT61288.2024.10584217.

[148] T. Ollila, “Overview for capabilities of OT network monitoring tools,” M.S. thesis, Inf. Technol., Jyväskylä Univ. Appl. Sci., Jyväskylä, Finland, 2024.

[149] J. Su and M. Jiang, “A hybrid entropy and blockchain approach for network security defense in SDN-based IIoT,” *Chin. J. Electron.*, vol. 32, no. 3, pp. 531–541, 2023. doi: 10.23919/cje.2022.00.103.

[150] L. Pullagura, N. V. Kumari, and H. K. Bhuyan, “Smart home forensics,” in *Cyber Forens. Investig. Smart Dev.*, A. Bhardwaj and K. Kaushik, Eds. Bentham Science, Sharjah, United Arab Emirates, 2024, vol. 1.

[151] K. Kelly, “The ring video doorbell and the entry of amazon into the smart home: Implications for consumer-initiated surveillance,” *J. Consum. Policy.*, vol. 46, no. 1, pp. 95–104, 2023. doi: 10.1007/s10603-022-09534-3.

[152] S. R. Fuerte, X. Yu, and J. Saniie, “Fire security systems analysis and internet of things implications,” in *2023 IEEE Int. Conf. Electro Inf. Technol. (eIT)*, IEEE, 2023, pp. 248–253. doi: 10.1109/eIT57321.2023.10187236.

[153] R. Harvent and L. M. Ravu, “Android based smart security system using Internet of Things (IoT) and firebase,” Fac. Comput. Syst. Softw. Eng., Univ. Malaysia Pahang, Malaysia, 2019. Accessed: Aug. 10, 2024. [Online]. Available: https://core.ac.uk/download/pdf/237500385.pdf

[154] J. Laufs, H. Borrion, and B. Bradford, “Security and the smart city: A systematic review,” *Sustain. Cities Soc.*, vol. 55, 2020, Art. no. 102023. doi: 10.1016/j.scs.2020.102023.

[155] Q. Zhang, H. Sun, X. Wu, and H. Zhong, “Edge video analytics for public safety: A review,” *Proc. IEEE*, vol. 107, no. 8, pp. 1675–1696, 2019. doi: 10.1109/JPROC.2019.2925910.

[156] B. J. Ospina Cifuentes, Á. Suárez, V. García Pineda, R. Alvarado Jaimes, A. O. Montoya Benitez and J. D. Grajales Bustamante, “Analysis of the use of artificial intelligence in software-defined intelligent networks: A survey,” *Technologies*, vol. 12, no. 7, 2024, Art. no. 99. doi: 10.3390/technologies12070099.

[157] C. W. R. Johnson, “Platform, application, grid: Synthetic ecologies and everyday surveillance,” Ph.D. dissertation, Univ. Calif., Davis, 2022.

[158] S. S. Gopalan, A. Raza, and W. Almobaideen, “IoT security in healthcare using AI: A survey,” in *2020 Int. Conf. Commun., Signal Process. Appl. (ICCSPA)*, IEEE, 2021, pp. 1–6. doi: 10.1109/ICCSPA49915.2021.9385711.

[159] D. M. N. Sarika, A. Jain, N. Bajeja, P. Rawat, and C. Joseph, “Use of enhanced artificial intelligence in security business management in the digital economy era,” *J. Informatics Educ. Res.*, vol. 3, no. 2, pp. 1484–1494, 2023.

[160] E. P. Adeghe, C. A. Okolo, and O. T. Ojeyinka, “A review of emerging trends in telemedicine: Healthcare delivery transformations,” *Int. J. Life Sci. Res. Arch.*, vol. 6, no. 1, pp. 137–147, 2024. doi: 10.53771/ijlsra.2024.6.1.0040.

[161] C. Yorston, “Design of an interactive generalized testbed for continuous data collection and reduced maintenance downtime in industrial applications: A use case study using siemens mindsphere,” M.S. thesis, Univ. Georgia, Athens, GA, USA, 2023.

[162] A. Topa, J. Gil, J. Álvarez, and J. Torres, “A hybrid-MPC based energy management system with time series constraints for a bioclimatic building,” *Energy*, vol. 287, 2024, Art. no. 129652. doi: 10.1016/j.energy.2023.129652.

[163] K. Demestichas, N. Peppes, and T. Alexakis, “Survey on security threats in agricultural IoT and smart farming,” *Sensors*, vol. 20, no. 22, 2020, Art. no. 6458. doi: 10.3390/s20226458.

[164] V. -N. Arsenoaia, R. -N. Raşu, I. -D. Veleşcu, and I. Ţenu, “Field tests of a John Deere harvester for the purpose of production maps achievement,” *Lucrări Ştiinţifice*, vol. 66, no. 1, 2023.

[165] P. Thatipelli and R. Sujatha, “Smart agricultural robot with real-time data analysis using IBM Watson cloud platform,” in *Advances in Clean Energy Technologies. Springer Proceedings in Energy*, Springer, 2021, pp. 415–427. doi: 10.1007/978-981-16-0235-1_33.

[166] B. Zohuri and F. M. Rahmani, “Artificial intelligence versus human intelligence: A new technological race,” *Acta Sci. Pharm. Sci.*, vol. 4, no. 5, pp. 50–58, 2020. doi: 10.31080/ASPS.2020.04.0530.

[167] N. Sharma, R. Sharma, and N. Jindal, “Machine learning and deep learning applications-a vision,” *Glob. Trans. Proc.*, vol. 2, no. 1, pp. 24–28, 2021. doi: 10.1016/j.gltp.2021.01.004.

[168] S. K. Chinnamgari, *R Machine Learning Projects: Implement Supervised, Unsupervised, and Reinforcement Learning Techniques Using R 3.5* 1st ed. Packt Publ. Ltd., 2019.

[169] F. Al-Turjman, *Artificial Intelligence in IoT*, 1st ed. Cham: Springer, 2019.

[170] M. Padmaja, S. Shitharth, K. Prasuna, A. Chaturvedi, P. R. Kshirsagar and A. Vani, “Grow of artificial intelligence to challenge security in IoT application,” *Wirel. Pers. Commun.*, vol. 127, no. 3, pp. 1829–1845, 2022. doi: 10.1007/s11277-021-08725-4.

[171] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, “A machine learning security framework for IoT systems,” *IEEE Access*, vol. 8, pp. 114066–114077, 2020. doi: 10.1109/ACCESS.2020.2996214.

[172] H. Afreen, M. Kashif, Q. Shaheen, Y. H. Alfaifi, and M. Ayaz, “IoT-based smart surveillance system for high-security areas,” *Appl. Sci.*, vol. 13, no. 15, 2023, Art. no. 8936. doi: 10.3390/app13158936.

[173] A. H. Sodhro, S. Pirbhulal, and V. H. C. De Albuquerque, “Artificial intelligence-driven mechanism for edge computing-based industrial applications,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4235–4243, 2019. doi: 10.1109/TII.2019.2902878.

[174] M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, “Data governance: Organizing data for trustworthy artificial intelligence,” *Gov. Inform. Q.*, vol. 37, no. 3, 2020, Art. no. 101493. doi: 10.1016/j.giq.2020.101493.

[175] H. Keipour, S. Hazra, N. Finne, and T. Voigt, “Generalizing supervised learning for intrusion detection in IoT mesh networks,” in *Int. Conf. Ubiquitous Secur.*, Springer, 2021, pp. 214–228. doi: 10.1007/978-981-19-0468-4_16.

[176] S. Dridi, “Supervised learning-a systematic literature review,” *OSF Prepr.*, 2021. doi: 10.31219/osf.io/tysr4.

[177] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, “Communication-efficient learning of deep networks from decentralized data,” in *Proc. 20th Int. Conf. Artif. Intell. Statist.*, PMLR, 2017, pp. 1273–1282.

[178] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li and H. V. Poor, “Federated learning for internet of things: A comprehensive survey,” *IEEE Commun. Surv. Tutorials.*, vol. 23, no. 3, pp. 1622–1658, 2021. doi: 10.1109/COMST.2021.3075439.

[179] A. Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, “A survey on federated learning for resource-constrained IoT devices,” *IEEE Internet Things J.*, vol. 9, no. 1, pp. 1–24, 2021. doi: 10.1109/JIOT.2021.3095077.

[180] Z. Du, C. Wu, T. Yoshinaga, K. -L. A. Yau, Y. Ji and J. Li, “Federated learning for vehicular internet of things: Recent advances and open issues,” *IEEE Open J. Comput. Soc.*, vol. 1, pp. 45–61, 2020. doi: 10.1109/OJCS.2020.2992630.

[181] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, “Federated learning for data privacy preservation in vehicular cyber-physical systems,” *IEEE Netw.*, vol. 34, no. 3, pp. 50–56, 2020. doi: 10.1109/MNET.011.1900317.

[182] R. S. Antunes, C. André da Costa, A. Küderle, I. A. Yari, and B. Eskofier, “Federated learning for healthcare: Systematic review and architecture proposal,” *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 4, pp. 1–23, 2022. doi: 10.1145/3501813.

[183] Y. Jiang *et al.*, “Blockchained federated learning for internet of things: A comprehensive survey,” *ACM Comput. Surv.*, vol. 56, no. 10, pp. 1–37, 2024. doi: 10.1145/365909.

[184] Y. Wang, Z. Su, N. Zhang, and A. Benslimane, “Learning in the air: Secure federated learning for UAV-assisted crowdsensing,” *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1055–1069, 2020. doi: 10.1109/TNSE.2020.3014385.

[185] Q. -V. Pham, M. Zeng, R. Ruby, T. Huynh-The, and W. -J. Hwang, “UAV communications for sustainable federated learning,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3944–3948, 2021. doi: 10.1109/TVT.2021.3065084.

[186] G. James, D. Witten, T. Hastie, R. Tibshirani, and J. Taylor, “Unsupervised learning,” in *An Introduction to Statistical Learning: With Applications in Python*, 1 ed. Cham, Switzerland: Springer, 2023, pp. 503–556.

[187] J. P. Poh, J. Y. C. Lee, K. X. Tan, and E. Tan, “Physical access log analysis: An unsupervised clustering approach for anomaly detection,” in *Proc. 3rd Int. Conf. Data Sci. Inf. Technol.*, 2020, pp. 12–18. doi: 10.1145/3414274.3414285.

[188] J. M. Luna, P. Fournier-Viger, and S. Ventura, “Frequent itemset mining: A 25 years review,” *WIREs Data Min. Knowl.*, vol. 9, no. 6, 2019, Art. no. e1329. doi: 10.1002/widm.1329.

[189] F. Sanna Passino, “Latent factor representations of dynamic networks with applications in cyber-security,” Ph.D. thesis, Imperial College, London, UK, 2021.

[190] A. Uprety and D. B. Rawat, “Reinforcement learning for IoT security: A comprehensive survey,” *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8693–8706, 2020. doi: 10.1109/JIOT.2020.3040957.

[191] S. M. Tahsien, H. Karimipour, and P. Spachos, “Machine learning based solutions for security of Internet of Things (IoT): A survey,” *J. Netw. Comput. Appl.*, vol. 161, no. 1, 2020, Art. no. 102630. doi: 10.1016/j.jnca.2020.102630.

[192] R. Ali, Y. A. Qadri, Y. Bin Zikria, T. Umer, B. -S. Kim and S. W. Kim, “Q-learning-enabled channel access in next-generation dense wireless networks for IoT-based eHealth systems,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, no. 1, pp. 1–12, 2019. doi: 10.1186/s13638-019-1498-x.

[193] S. Walczak, “Artificial neural networks,” in *Adv. Methodol. Technol. Artif. Intell., Comput. Simul., Human-Comput. Interact.*, IGI Global, 2019, pp. 40–53.

[194] A. R. Abdellah, O. A. K. Mahmood, A. Paramonov, and A. Koucheryavy, “IoT traffic prediction using multi-step ahead prediction with neural network,” in *2019 11th Int. Congr. Ultra Mod. Telecommun. Control Syst. Workshops (ICUMT)*, IEEE, 2019, pp. 1–4. doi: 10.1109/ICUMT48472.2019.8970675.

[195] S. Zare Naghadehi, M. Asadi, M. Maleki, S. -M. Tavakkoli-Sabour, J. L. Van Genderen and S. -S. Saleh, “Prediction of Urban area expansion with implementation of MLC, SAM and SVMs’ classifiers incorporating artificial neural network using landsat data,” *ISPRS Int. J. Geo-Inf.*, vol. 10, no. 8, 2021, Art. no. 513. doi: 10.3390/ijgi10080513.

[196] G. Chhabra *et al.*, “Internet of things based smart framework for the safe driving experience of two wheelers,” *Sci. Rep.*, vol. 14, no. 1, 2024, Art. no. 21830. doi: 10.1038/s41598-024-72357-4.

[197] S. S. Hameed, H. R. Abdulshaheed, Z. L. Ali, and H. M. Gheni, “Implement DNN technology by using wireless sensor network system based on IOT applications,” *Period Eng. Nat. Sci.*, vol. 10, no. 2, pp. 128–137, 2022. doi: 10.21533/pen.v10i2.2831.

[198] G. E. Selim, E. E. D. Hemdan, A. M. Shehata, and N. A. El-Fishawy, “An efficient machine learning model for malicious activities recognition in water-based industrial internet of things,” *Secur. Privacy.*, vol. 4, no. 3, 2021, Art. no. e154. doi: 10.1002/spy2.154.

[199] R. Dwivedi *et al.*, “Explainable AI (XAI): Core ideas, techniques, and solutions,” *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–33, 2023. doi: 10.1145/3561048.

[200] R. Tiwari, “Explainable AI (XAI) and its applications in building trust and understanding in AI decision making,” *Int. J. Sci. Res. Eng. Manag.*, vol. 7, no. 1, pp. 1–13, 2023. doi: 10.55041/IJSREM17592.

[201] Z. Fan, W. Li, K. B. Laskey, and K. -C. Chang, “Investigation of phishing susceptibility with explainable artificial intelligence,” *Future Internet*, vol. 16, no. 1, 2024, Art. no. 31. doi: 10.3390/fi16010031.

[202] G. Montavon, J. Kauffmann, W. Samek, and K. -R. Müller, “Explaining the predictions of unsupervised learning models,” in *Int. Workshop Extend. Explain. AI Beyond Deep Models Classif.*, Springer, 2020, pp. 117–138.

[203] C. I. Nwakanma *et al.*, “Explainable artificial intelligence (XAI) for intrusion detection and mitigation in intelligent connected vehicles: A review,” *Appl. Sci.*, vol. 13, no. 3, 2023, Art. no. 1252. doi: 10.3390/app13031252.

[204] L. Wells and T. Bednarz, “Explainable AI and reinforcement learning—A systematic review of current approaches and trends,” *Front. Artif. Intell.*, vol. 4, 2021, Art. no. 550030. doi: 10.3389/frai.2021.550030.

[205] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, “Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions,” *IEEE Commun. Surv. Tutor.*, vol. 25, no. 3, pp. 1775–1807, 2023. doi: 10.1109/COMST.2023.3280465.

[206] M. J. P. Peixoto and A. Azim, “Explainable artificial intelligence (XAI) approach for reinforcement learning systems,” in *Proc. 39th ACM/SIGAPP Symp. Appl. Comput.*, 2024, pp. 971–978. doi: 10.1145/3605098.3635992.

[207] M. Mersha, K. Lam, J. Wood, A. AlShami, and J. Kalita, "Explainable artificial intelligence: A survey of needs, techniques, applications, and future direction," *Neurocomputing*, vol. 599, no. 5, 2024, Art. no. 128111. doi: 10.1016/j.neucom.2024.128111.

[208] M. U. Islam, M. Mozaharul Mottalib, M. Hassan, Z. I. Alam, S. Zobaed and M. Fazle Rabby, "The past, present, and prospective future of XAI: A comprehensive review," in *Explainable Artificial Intelligence for Cyber Security. Studies in Computational Intelligence*, Springer, 2022, pp. 1–29.

[209] W. Saeed and C. Omlin, "Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities," *Knowl.-Based Syst.*, vol. 263, no. 3, 2023, Art. no. 110273. doi: 10.1016/j.knosys.2023.110273.

[210] A. R. Javed, W. Ahmed, S. Pandya, P. K. R. Maddikunta, M. Alazab and T. R. Gadekallu, "A survey of explainable artificial intelligence for smart cities," *Electronics*, vol. 12, no. 4, 2023, Art. no. 1020. doi: 10.3390/electronics12041020.

[211] S. K. Jagatheesaperumal, Q. -V. Pham, R. Ruby, Z. Yang, C. Xu and Z. Zhang, "Explainable AI over the Internet of Things (IoT): Overview, state-of-the-art and future directions," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 2106–2136, 2022. doi: 10.1109/OJCOMS.2022.3215676.

[212] J. L. C. Bárcena, P. Ducange, F. Marcelloni, and A. Renda, "Increasing trust in AI through privacy preservation and model explainability: Federated learning of fuzzy regression trees," *Inf Fusion*, vol. 113, 2025, Art. no. 102598. doi: 10.1016/j.inffus.2024.102598.

[213] M. Nagahisarchoghaei *et al.*, "An empirical survey on explainable AI technologies: Recent trends, use-cases, and categories from technical and application perspectives," *Electronics*, vol. 12, no. 5, 2023, Art. no. 1092. doi: 10.3390/electronics12051092.

[214] R. Machlev *et al.*, "Explainable artificial intelligence (XAI) techniques for energy and power systems: Review, challenges and opportunities," *Energy AI*, vol. 9, no. 2, 2022, Art. no. 100169. doi: 10.1016/j.egyai.2022.100169.

[215] F. García-Peñalvo and A. Vázquez-Ingelmo, "What do we mean by GenAI? A systematic mapping of the evolution, trends, and techniques involved in Generative AI," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 8, no. 4, pp. 7–16, 2023. doi: 10.9781/ijimai.2023.07.006.

[216] L. Pinheiro Cinelli, M. Araújo Marins, E. A. Barros da Silva, and S. Lima Netto, "Variational autoencoder," in *Variational Methods for Machine Learning with Applications to Deep Networks*. Cham: Springer, 2021, pp. 111–149.

[217] S. S. Sengar, A. B. Hasan, S. Kumar, and F. Carroll, "Generative artificial intelligence: A systematic review and applications," *Multimed. Tools Appl.*, vol. 10, no. 2, 2024. doi: 10.1007/s11042-024-20016-1.

[218] J. G. Meyer *et al.*, "ChatGPT and large language models in academia: Opportunities and challenges," *BioData Min.*, vol. 16, no. 1, 2023, Art. no. 20. doi: 10.1186/s13040-023-00339-9.

[219] E. Skarzynska and J. Paliszkiewicz, "The use of generative artificial intelligence (GenAI) capabilities for early detection of threats in the digital environment: The good side of GenAI," in *Regulating Hate Speech Created by Generative AI*, 1 ed. Boca Raton, FL: Auerbach Publications, 2024, pp. 91–104.

[220] K. Huang, J. Ponnapalli, J. Tantsura, and K. T. Shin, "Navigating the GenAI security landscape," in *Generative AI Security*. Cham: Springer, 2024, pp. 31–58.

[221] K. Huang, J. Huang, and D. Catteddu, "GenAI data security," in *Generative AI Security*. Cham: Springer, 2024, pp. 133–162.

[222] M. Christodorescu *et al.*, "Securing the future of GenAI: Policy and technology," *Cryptol. ePrint Arch.*, 2024. doi: https://eprint.iacr.org/2024/855.

[223] A. Essa and M. Lataifeh, "Evaluating generative AI tools for visual asset creation–An educational approach," in *Proc. Third Int. Conf. Innov. Comput. Res. (ICR'24)*, 2024, pp. 269–282. doi: 10.1007/978-3-031-65522-7_25.

[224] F. Kalota, “A primer on generative artificial intelligence,” *Educ. Sci.*, vol. 14, no. 2, 2024, Art. no. 172. doi: 10.3390/educsci14020172.

[225] M. Mariani and Y. K. Dwivedi, “Generative artificial intelligence in innovation management: A preview of future research developments,” *J. Bus. Res.*, vol. 175, no. 3, 2024, Art. no. 114542. doi: 10.1016/j.jbusres.2024.114542.