GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

Exploring security, performance and privacy in the internet of things: A comprehensive survey

Abura Samson *

Jaramogi Oginga Odinga University of Science and Technology, 40601, Bondo.

GSC Advanced Research and Reviews, 2024, 21(01), 280–319

Publication history: Received on 13 September 2024; revised on 19 October 2024; accepted on 22 October 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.21.1.0388

Abstract

The Internet of Things (IoT) has rapidly emerged as a transformative technology, enabling a vast network of interconnected devices that collect, exchange, and act on data across diverse applications. However, the pervasive integration of IoT into critical sectors such as healthcare, smart cities, and industrial automation has raised significant concerns regarding security, privacy, and performance. This survey provides a comprehensive overview of the key challenges and advancements in these areas. It begins by exploring the fundamental security vulnerabilities in IoT systems, including threats from malicious actors, weak authentication protocols, and software vulnerabilities. Privacy concerns are then discussed, focusing on issues related to data collection, user consent, and the risk of data breaches. Furthermore, the paper examines the performance challenges in IoT environments, such as limited computational resources, network latency, and energy efficiency. Through an analysis of current solutions, including encryption techniques, privacy-preserving frameworks, and performance optimization strategies, this survey highlights ongoing research efforts and identifies areas requiring further investigation. By synthesizing the state-of-the-art approaches, this paper aims to guide future developments towards a more secure, privacy-conscious, and efficient IoT ecosystem.

Keywords: IoT security; Privacy preservation; Performance optimization; Threat mitigation; Data Protection; Network efficiency

1. Introduction

The Internet of Things (IoT) represents a rapidly evolving paradigm that connects billions of devices, ranging from smart home appliances and wearable gadgets to large-scale industrial systems [1-4]. As shown in Figure 1, these devices communicate and share data over the internet, enabling a wide range of applications, such as smart cities, healthcare, transportation, and manufacturing. Communication in the Internet of Things (IoT) involves the seamless exchange of data between interconnected devices, sensors, and systems over networks. These devices use various communication protocols, such as Wi-Fi, Bluetooth, Zigbee, and cellular networks, to transmit data to cloud platforms or other devices for analysis and action. The communication in IoT is typically characterized by low-power, short-range transmissions, often optimized for efficiency and scalability in environments with a large number of devices. Reliable and secure communication is crucial for IoT, as the data exchanged often powers real-time applications, automation, and smart systems in industries like healthcare, agriculture, and smart cities.

* Corresponding author: Abura Samson

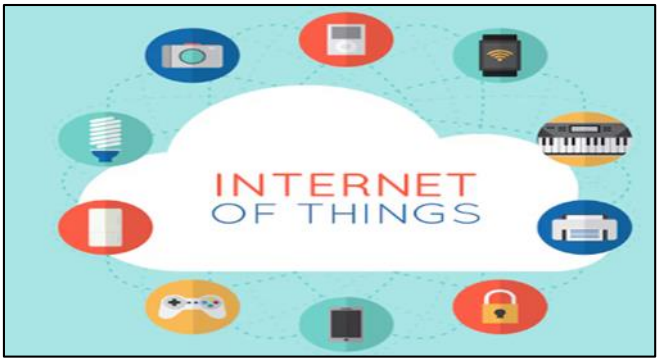

Figure 1 IoT applications

IoT's ability to provide real-time data, enhance automation, and streamline operations has led to its widespread adoption [5], with forecasts predicting exponential growth in the number of connected devices over the coming years. As shown in Figure 2, IoT protocols are essential for enabling communication between devices in the Internet of Things ecosystem, ensuring efficient data transmission and interoperability. Common IoT protocols include MQTT (Message Queuing Telemetry Transport), which is lightweight and suited for low-bandwidth, high-latency networks, and CoAP (Constrained Application Protocol), designed for resource-constrained devices. Other protocols like Zigbee and Z-Wave are widely used for short-range, low-power wireless communication in smart homes and industrial automation. Bluetooth Low Energy (BLE) is also popular for short-range, low-power communication in consumer devices. These protocols are crucial for ensuring secure, reliable, and scalable communication in diverse IoT applications.

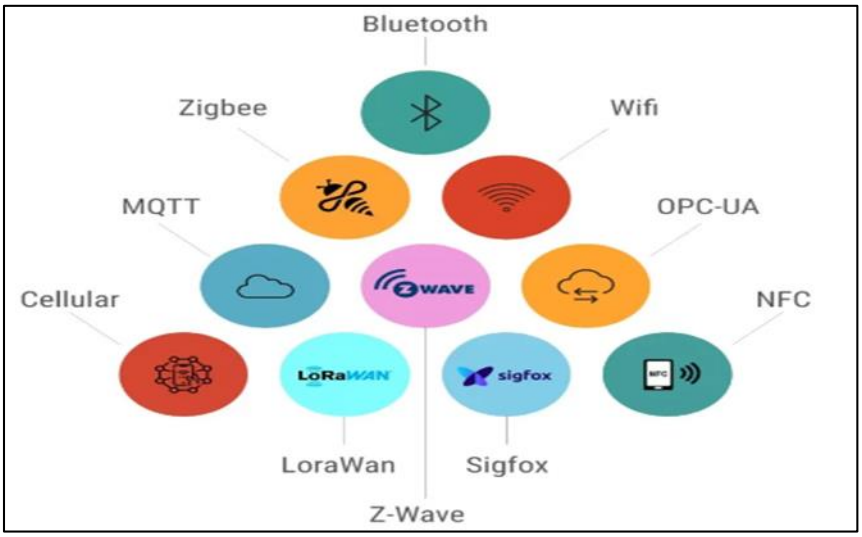

Figure 2 IoT protocols

However, as the IoT ecosystem expands, it introduces a complex set of challenges, particularly in the areas of security, privacy, and performance [6]. IoT devices often operate with limited computational power, memory, and energy resources, which complicates the implementation of robust security mechanisms [7]-[11]. The diversity of devices, networks, and protocols also increases the attack surface, making IoT systems vulnerable to a variety of cyber threats, including unauthorized access, data breaches, denial-of-service (DoS) attacks, and the spread of malware.

Privacy concerns are equally pressing. IoT devices continuously gather and transmit sensitive personal and organizational data, often without transparent mechanisms for user consent or control [12], [13]. The pervasive nature of IoT in everyday life exacerbates these privacy risks, as data can be exploited for surveillance, profiling, or unauthorized sharing with third parties. Safeguarding user privacy while maintaining the functionality and benefits of IoT remains a significant challenge [14]-[16].

In addition to security and privacy issues, performance is a critical consideration in IoT environments. The constrained resources of many IoT devices [17], coupled with the need for real-time processing, pose challenges for maintaining

network efficiency, latency, and energy consumption [18]. Balancing the demand for high-performance IoT systems with the need for secure and privacy-respecting solutions requires careful attention to trade-offs between these competing factors.

This survey aims to provide a comprehensive overview of the state of the art in IoT security, privacy, and performance. It explores the key challenges, threats, and vulnerabilities that affect IoT ecosystems, while also highlighting the most promising approaches for mitigating these issues. By synthesizing the latest research developments, this paper seeks to identify gaps in current solutions and offer insights into future directions for creating secure, privacy-aware, and high-performing IoT systems.

1.1. Motivation

The proliferation of Internet of Things (IoT) technologies has dramatically transformed industries, public infrastructure, and personal life, with estimates projecting that billions of devices will be interconnected in the near future [19]. This rapid growth of IoT promises substantial economic, operational, and societal benefits, particularly through enhanced automation, data-driven decision-making, and improved efficiency across diverse domains such as healthcare, smart cities, industrial automation, and environmental monitoring [20], [21].

However, the success of IoT hinges on addressing critical security, privacy, and performance concerns. The interconnected nature of IoT networks and the limited computational capabilities of many devices make them prime targets for cyberattacks [22]. Incidents such as the Mirai botnet, which exploited IoT devices to launch large-scale Distributed Denial-of-Service (DDoS) attacks, illustrate the severe consequences of poor security in IoT systems. The growing reliance on IoT for critical functions, such as medical monitoring or industrial control, magnifies the potential risks posed by these vulnerabilities [23], making it imperative to develop more robust security measures.

In parallel, the unprecedented amount of data generated by IoT devices raises serious privacy issues. These devices often collect sensitive information—ranging from health metrics and personal habits to location data—sometimes without explicit consent from users [24]. The absence of clear data governance frameworks and privacy-preserving mechanisms has led to widespread concerns about data misuse, unauthorized surveillance, and the potential for malicious exploitation of personal information [25], [26]. Ensuring that IoT solutions respect user privacy while maintaining functionality is a growing challenge, particularly in light of increasing regulatory requirements like the General Data Protection Regulation (GDPR).

Moreover, the performance of IoT networks is paramount to their effectiveness. Many IoT applications demand real-time data processing and low-latency communication, while operating on devices with constrained energy, memory, and processing capabilities [27], [28]. Striking a balance between high performance and resource efficiency [29], while simultaneously integrating security and privacy controls, is a complex task that has become a critical area of research.

Given these challenges, a comprehensive survey of IoT security, privacy, and performance is urgently needed. Such a survey can serve as a roadmap for researchers and practitioners to understand the current landscape, identify gaps in existing solutions, and propose new approaches that can meet the evolving demands of IoT ecosystems. This paper aims to bridge that gap by synthesizing the latest advances in these domains, while offering insights into how future IoT architectures can be made more secure, privacy-preserving, and high-performing.

1.2. Contribution

This survey paper offers a comprehensive examination of the key challenges and recent advancements in IoT security, privacy, and performance. The main contributions of this work are outlined as follows:

- *Comprehensive analysis of IoT security threats and vulnerabilities:* This paper provides an extensive review of the various security challenges faced by IoT ecosystems. It categorizes common threats, such as malware, denial-of-service (DoS) attacks, and data manipulation, and explores the underlying vulnerabilities in IoT architecture, including weak authentication mechanisms, insecure communication protocols, and firmware flaws. The survey also highlights notable real-world incidents and their implications for the broader IoT landscape.
- *Review of privacy risks and protection mechanisms:* This paper systematically address privacy concerns associated with IoT devices, focusing on issues such as data collection, user consent, and the risk of unauthorized data sharing. This survey evaluates current privacy-preserving techniques, including data anonymization, differential privacy, and encryption protocols, and discusses their effectiveness and limitations in IoT environments.

- *Evaluation of performance challenges in IoT systems:* The paper offers an in-depth exploration of the performance bottlenecks in IoT networks, including latency, bandwidth constraints, energy efficiency, and scalability. This study reviews recent approaches aimed at optimizing IoT performance, such as edge computing, lightweight protocols, and resource management techniques, while discussing trade-offs between performance, security, and privacy.
- *Synthesis of state-of-the-art solutions for IoT security, privacy, and performance:* By surveying existing solutions and frameworks, this paper provides a holistic overview of the current landscape. The paper evaluates the effectiveness of different techniques and proposes how they can be integrated to create a balanced approach that addresses security, privacy, and performance in tandem.
- *Identification of research gaps and future directions:* This survey highlights the open challenges and areas requiring further research in IoT security, privacy, and performance. This study identifies gaps in existing solutions, such as the lack of standardized security protocols, insufficient privacy frameworks for dynamic IoT environments, and the need for energy-efficient performance optimization. The paper outlines future research directions, offering insights into emerging trends and potential areas for innovation.

2. IoT architecture

The architecture of the Internet of Things (IoT) comprises several layers that enable the seamless interaction between devices, networks, and applications. As shown in Figure 3, these layers are typically organized in a multi-tiered structure, ensuring data flow from physical objects to actionable insights.

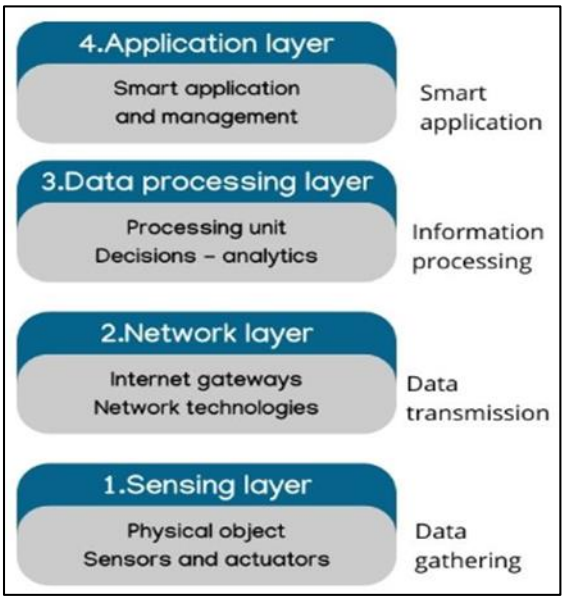

Figure 3 IoT architecture

While specific architectures can vary depending on use cases, a common IoT architecture is structured into four main layers: the Perception Layer, the Network Layer, the Processing Layer, and the Application Layer.

2.1. Perception Layer (Device Layer)

The Perception Layer is the foundation of the IoT architecture, responsible for sensing and collecting data from the physical environment [30]. It includes various IoT devices, sensors, and actuators that interact with the real world to gather data such as temperature, humidity, motion, light, and other environmental factors [31]. This layer plays a critical role in converting physical phenomena into digital signals. The components of this layer include sensors, actuators, RFID tags, smart devices, and embedded systems. Its function include data acquisition and measurement, device identification (e.g., using RFID), and transmission of raw data to the network layer for further processing.

2.2. Network Layer (Communication Layer)

The Network Layer facilitates the transmission of data gathered by the perception layer to higher layers for processing [32]. It connects IoT devices to the cloud, gateways, or local servers using various communication protocols and

technologies [33]. This layer ensures the secure, reliable, and efficient flow of data across different network infrastructures. Its key components include gateways, routers, and communication protocols (Wi-Fi, Bluetooth, Zigbee, LTE, 5G, LoRa, NB-IoT). Its functions include data routing and transmission from devices to data centers or processing units, ensuring data integrity and secure communication through encryption, and enabling connectivity across heterogeneous networks and protocols.

2.3. Processing Layer (Middleware Layer)

The Processing Layer is responsible for data storage, analysis, and processing. It acts as an intermediary, handling the heavy lifting of data analytics and decision-making processes [34]. This layer can reside in the cloud or at the edge, where data is processed closer to where it is generated. It often employs machine learning [35], artificial intelligence, and big data analytics to derive insights from the vast amounts of data collected. The main components of this layer include cloud computing platforms, edge computing devices, databases, middleware, and analytic tools. Its core functions include data filtering, aggregation, and transformation; real-time or batch processing of large datasets; application of algorithms for predictive analytics, anomaly detection, and decision-making; and coordination of communication between devices and applications.

2.4. Application Layer

The Application Layer is the topmost layer in the IoT architecture, responsible for delivering specific services and applications to end-users [36]. It interprets the processed data and translates it into meaningful actions or insights, which are utilized across various IoT applications, such as smart homes, healthcare, industrial automation, agriculture, and transportation [37]. The crucial components of this layer include user interfaces, dashboards, mobile and web applications, APIs. Its main functions include providing domain-specific services and applications (e.g., smart city monitoring, predictive maintenance); enabling interaction with end-users through intuitive interfaces and implementing control actions (e.g., turning on/off devices based on data insights). Table 1 presents some of the cross-cutting concerns in this IoT architecture.

Table 1 Cross-Cutting Concerns

Concern	Description
Security and privacy	Ensuring secure communication, data encryption, authentication, and access control across all layers to prevent unauthorized access and data breaches [38].
Data management	Efficient handling of large volumes of data in terms of storage, retrieval, and processing [39].
Scalability and performance	Supporting the growth of the IoT network by optimizing resource usage, managing latency, and improving system efficiency [40], [41].
Interoperability	Ensuring different devices, platforms, and protocols can communicate and work together seamlessly.

2.5. Edge and fog computing in IoT architecture

In traditional IoT architectures, much of the processing is performed in the cloud (centralized). However, edge and fog computing architectures have gained prominence to address performance and latency concerns by processing data closer to the source (e.g., at the edge devices or in fog nodes between the edge and the cloud) [42], [43]. In edge computing, data processing occurs on the device itself or near the sensors to reduce latency and enhance real-time responsiveness [44]. On the other hand, fog computing represents a distributed computing model that extends the cloud to be closer to the edge, allowing intermediate processing and storage, improving overall network efficiency and speed [45].

As shown in Figure 4, IoT fog computing architecture extends cloud computing to the edge of the network, closer to where data is generated by IoT devices. This architecture aims to address the challenges of latency, bandwidth, and real-time processing, which can be problematic when relying solely on centralized cloud servers. Fog computing pushes computation, storage, and network resources closer to IoT devices, enabling faster data processing and decision-making. By offloading tasks from the cloud to the fog layer, the architecture reduces the amount of data sent to distant cloud servers, minimizing latency and improving responsiveness, especially in applications like autonomous vehicles, industrial automation, and smart cities.

The architecture typically involves three layers: IoT devices, the fog layer, and the cloud layer. IoT devices at the edge capture data from sensors and send it to fog nodes, which are intermediate devices such as gateways, routers, or local servers. These fog nodes process the data locally or perform pre-processing tasks like filtering or aggregation before sending only relevant or summarized information to the cloud. This distributed computing model allows real-time analytics and decision-making at the fog layer, reducing the need for constant communication with the cloud. The cloud layer, meanwhile, serves as a centralized platform for large-scale data storage, deeper analytics, and long-term decision-making, with less frequent communication with the fog nodes.

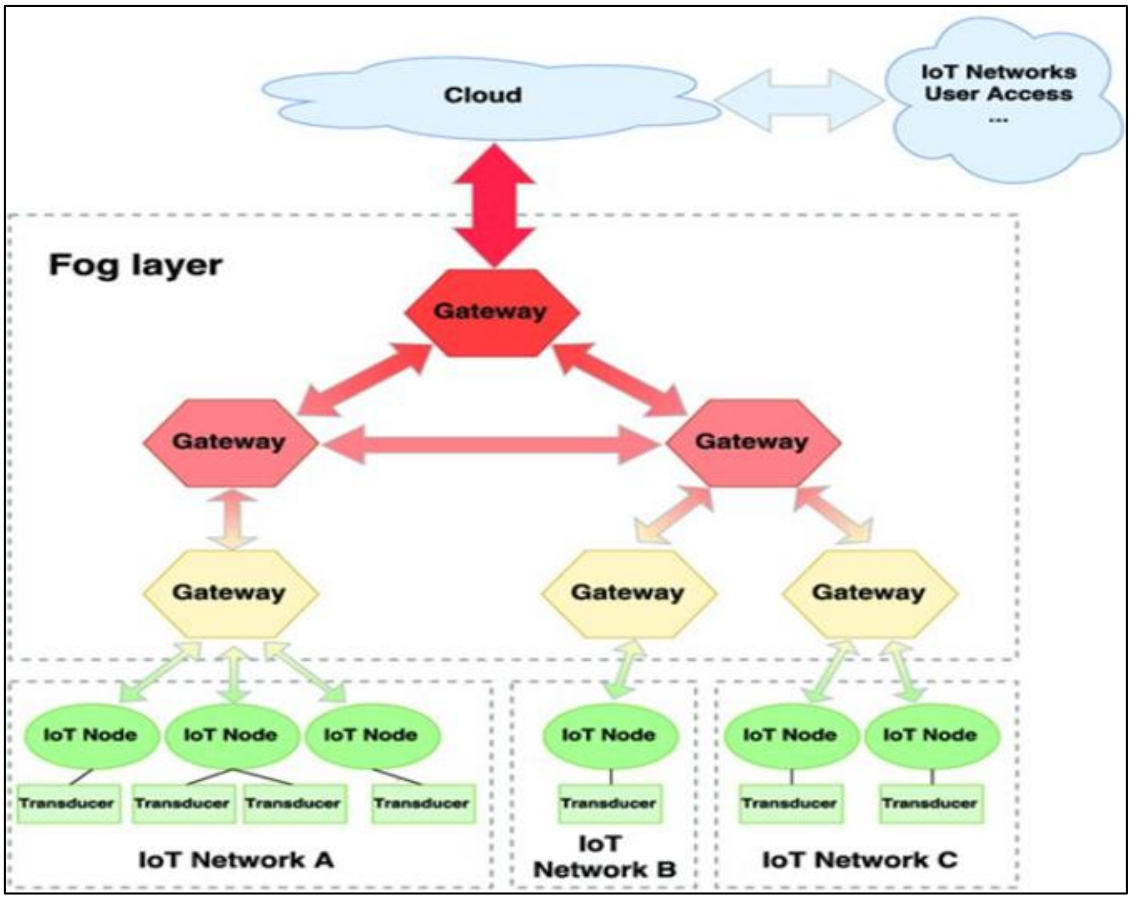

Figure 4 IoT fog computing architecture

Fog computing offers several advantages for IoT systems, including reduced latency, improved data security, and better bandwidth utilization. By processing data closer to the source, it can also address privacy concerns by keeping sensitive data local rather than transmitting it over the internet. This makes it particularly useful in critical IoT applications such as healthcare, financial services, and smart manufacturing, where both speed and data privacy are essential. The fog computing model supports scalability, as additional fog nodes can be deployed to accommodate the growing number of IoT devices, creating a robust and flexible architecture for future IoT innovations.

As evidenced in Figure 5, IoT edge computing architecture involves processing data closer to the source of generation—on IoT devices themselves or on nearby edge nodes, such as routers, gateways, or specialized servers. Unlike cloud computing, which requires data to be transmitted to distant data centers, edge computing processes data locally, reducing latency, improving real-time response, and alleviating network bandwidth limitations. This approach is particularly beneficial in scenarios where immediate decision-making is critical, such as autonomous vehicles, industrial robotics, and remote healthcare monitoring, where milliseconds can be the difference between success and failure.

The architecture of edge computing typically consists of IoT devices, edge nodes, and the cloud. IoT devices equipped with sensors capture data, and this data is processed either on the device or sent to edge nodes for processing. These nodes can handle tasks such as real-time analytics, AI-driven decision-making, or data filtering, reducing the volume of data that needs to be sent to the cloud. The cloud remains an important component in edge computing for long-term

data storage, in-depth analysis, and coordination across multiple edge nodes. However, by minimizing the reliance on centralized cloud systems, edge computing offers faster responses and better data management at the local level.

Edge computing offers numerous advantages in IoT ecosystems, including enhanced speed, improved privacy, and better resilience. By processing data locally, edge computing reduces the need for constant data transmission to the cloud, which can help alleviate security concerns, especially in industries like healthcare or finance where sensitive information is involved.

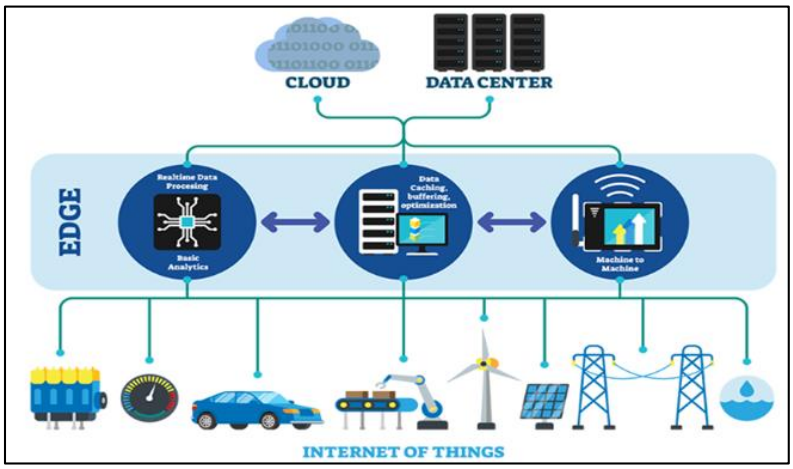

Figure 5 IoT edge computing architecture

Furthermore, edge computing can continue functioning even if cloud connectivity is lost, making it more resilient for remote or critical applications. This architecture is especially suited for IoT systems that require real-time decision-making, lower latency, and a distributed approach to data processing, paving the way for innovations in smart cities, agriculture, and industrial automation.

In a nutshell, the IoT architecture is a complex, multi-layered system designed to support the interaction between the physical world and digital systems [46]. Each layer plays a distinct role in ensuring data is captured, transmitted, processed, and acted upon efficiently and securely. As IoT continues to evolve, the architecture must adapt to accommodate the growing number of devices, the diversity of applications, and the increasing demands for security, privacy, and performance.

3. Security and privacy issues in IoT

The widespread adoption of the Internet of Things (IoT) has opened up numerous opportunities across sectors, but it has also introduced significant security and privacy challenges [47], [48]. These challenges arise from the unique characteristics of IoT systems, such as the vast number of devices, heterogeneous architectures, and the limited resources of IoT devices. Given the sensitive nature of data collected by IoT devices and their integration into critical infrastructure, addressing these security and privacy concerns is paramount [49]. The sub-sections below presents an extensive description of the major security and privacy challenges in IoT.

3.1. Security challenges in IoT

The main concerns in this domain include the following:

- *Device heterogeneity and interoperability:* IoT ecosystems consist of a wide variety of devices with different hardware, software, and communication protocols [50]. This diversity creates compatibility issues and complicates the design of a unified security framework. IoT devices range from simple sensors to complex smart devices, each with distinct security capabilities [51], [52]. Many devices are not designed with security in mind, particularly low-cost sensors, making it difficult to deploy universal security protocols across all devices.
- *Resource constraints:* Many IoT devices operate with limited computational power, memory, and energy resources [53]. These constraints make it difficult to implement robust security measures such as encryption, authentication, and secure communication protocols [54], [55]. Traditional security solutions, which are often

computationally intensive, may not be feasible for resource-constrained IoT devices. This makes IoT systems vulnerable to attacks that exploit weak security configurations.

- *Weak authentication and access control*: Weak or nonexistent authentication mechanisms are a common vulnerability in IoT devices [56]. Many devices come with default, hardcoded passwords or lack proper mechanisms to authenticate users and other devices in the network [57]. As demonstrated in Figure 6, poor access control measures can lead to unauthorized access, allowing attackers to control devices or manipulate the data being collected [58].

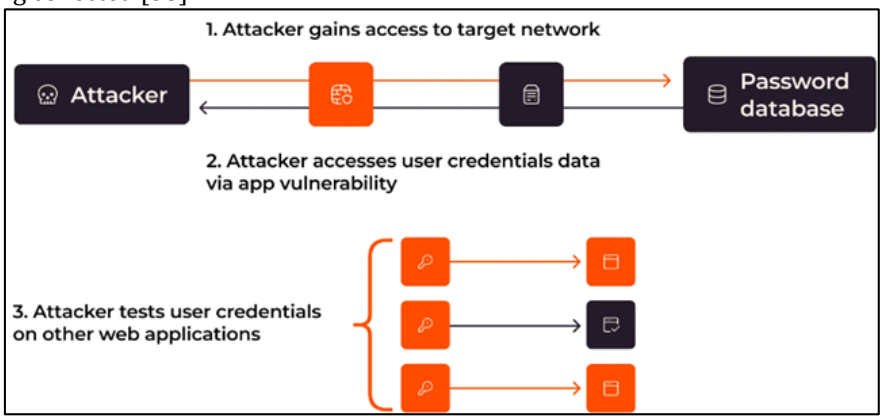

Figure 6 Weak authentication and access control in IoT

Furthermore, the lack of centralized management in distributed IoT systems complicates the enforcement of consistent access control policies. Weak authentication and access control in IoT pose significant security risks, as they can allow unauthorized users to access, manipulate, or control connected devices. Many IoT devices are designed with limited processing power and memory, leading to the implementation of weak or default passwords, insufficient encryption, and inadequate authentication mechanisms. Without robust access control policies, attackers can exploit these vulnerabilities, gaining unauthorized access to networks, intercepting data, or launching large-scale attacks such as Distributed Denial of Service (DDoS) attacks. Strengthening authentication methods, using multi-factor authentication, and implementing strong access control policies are essential to secure IoT ecosystems and protect sensitive data and infrastructure from potential threats.

- *Insecure communication*: IoT devices frequently rely on wireless communication channels, such as Wi-Fi, Bluetooth, Zigbee, or cellular networks, which are inherently susceptible to interception, jamming, and eavesdropping [59]-[63]. If communication is not properly encrypted, attackers can intercept sensitive data or launch man-in-the-middle (MITM) attacks to alter or manipulate the data in transit [64]. Figure 7 shows some of the sources of insecure communication in IoT environment.

Figure 7 Insecure communication in IoT

Insecure communication protocols increase the risk of data breaches and compromise the integrity and confidentiality of the transmitted information. Insecure communication in IoT refers to the lack of proper encryption and security protocols when transmitting data between devices, gateways, and cloud servers. This vulnerability exposes sensitive information, such as user data or device control commands, to interception, tampering, or eavesdropping by malicious actors. Many IoT devices, especially low-powered or resource-constrained ones, may use outdated or weak encryption standards, or none at all, making communication channels highly susceptible to attacks. Insecure communication can lead to privacy breaches, data theft, and unauthorized control of IoT systems. Ensuring secure communication through encryption, authentication, and secure protocols like TLS or DTLS is crucial to protect IoT ecosystems.

- *Firmware vulnerabilities*: IoT devices often run outdated or poorly maintained firmware, making them susceptible to attacks that exploit known vulnerabilities [65]. Many IoT devices do not receive regular software updates or lack mechanisms for secure firmware updates [66]. As a result, these devices can become easy targets for attackers who exploit vulnerabilities to gain control over devices, inject malware, or compromise the entire network.
- *Botnet attacks and DDoS*: IoT devices are prime candidates for inclusion in botnets—networks of compromised devices controlled by attackers to carry out large-scale cyberattacks [67]. As shown in Figure 8, botnets can be used to launch Distributed Denial of Service (DDoS) attacks that overwhelm websites, services, or entire networks.

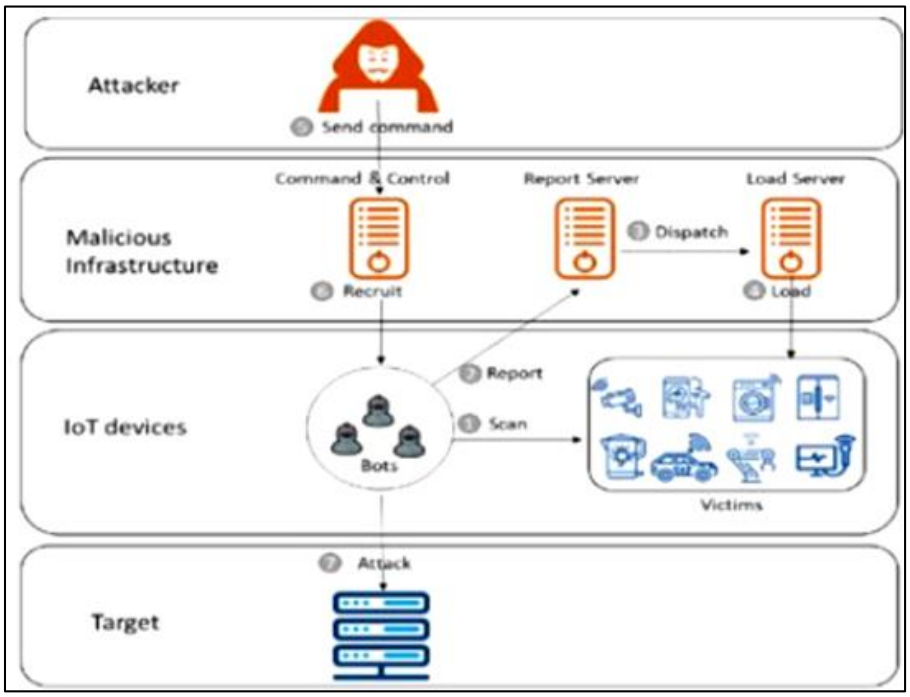

Figure 8 Botnets in IoT

For example, the Mirai botnet attack exploited IoT devices with weak security configurations, causing widespread disruption by flooding servers with traffic [68], [69]. Such attacks highlight the need for improved IoT device security to prevent them from being co-opted into botnets.

- *Physical security threats*: Many IoT devices are deployed in remote or unattended environments, making them vulnerable to physical tampering [70], [71], as shown in Fig.9. Attackers can physically access devices to manipulate their hardware, extract sensitive data, or inject malware. Physical attacks are particularly concerning in critical infrastructure systems [72], such as smart grids or industrial control systems, where tampering with devices could have serious consequences. Physical threats in IoT involve the risk of direct tampering, theft, or destruction of IoT devices, which are often deployed in accessible or remote environments. Unlike traditional IT systems that are housed in secure data centers, IoT devices may be located in homes, public spaces, factories, or even outdoor areas, making them more vulnerable to physical attacks. Attackers could manipulate devices to disrupt services, steal sensitive data, or use them as entry points into larger networks. For instance, tampering with sensors in industrial systems or medical devices can cause malfunctions with

serious safety consequences. To mitigate physical threats, measures such as tamper-proof enclosures, regular inspections, and physical access control are essential.

- *Side-channel attacks*: Side-channel attacks exploit physical characteristics of IoT devices, such as power consumption, electromagnetic emissions, or timing information, to infer sensitive data [73], [74], as evidenced in Figure 9. These attacks can be particularly effective on resource-constrained devices, which may lack the ability to implement countermeasures against side-channel exploits. For example, attackers could use power analysis to extract cryptographic keys from devices, compromising the security of the entire system.

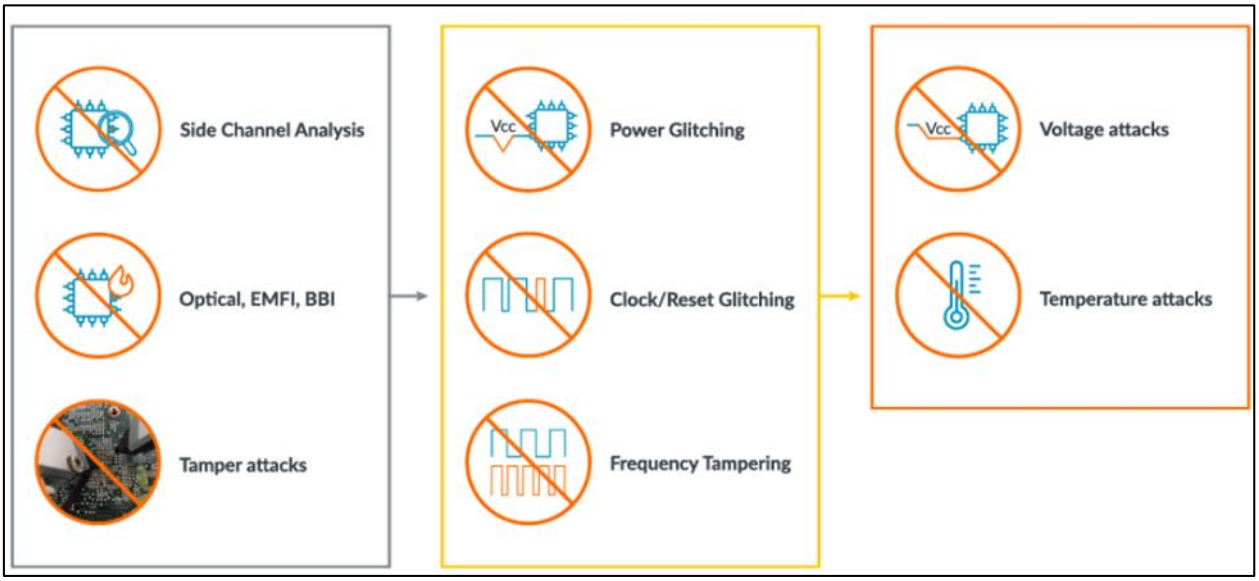

Figure 9 Physical security threats in IoT

Side-channel attacks in IoT exploit the unintended physical or electromagnetic emissions of IoT devices to gain unauthorized access to sensitive information. Rather than directly targeting the software or network, attackers observe factors like power consumption, electromagnetic leaks, or timing information during the operation of a device to infer data such as encryption keys or passwords. Due to the resource constraints of many IoT devices, they often lack robust protections against such attacks. Side-channel attacks can compromise data confidentiality, integrity, and even device functionality, particularly in sensitive environments like healthcare or smart grids. Mitigating these attacks requires physical shielding, better cryptographic algorithms, and side-channel resistance techniques in device design. Table 2 below gives a summary of other attacks in an IoT environment.

Table 2 Attacks in an IoT Environment

Attack	**Details**
Physical layer attacks	The physical layer in IoT consists of the hardware devices (sensors, actuators, RFID tags, etc.) that collect and send data. Due to their often remote and unattended deployments, these devices are vulnerable to physical attacks [78], [79]. Specific threats under this category include the following *Device tampering and physical access attacks:* IoT devices in open or unsecured environments are susceptible to physical tampering [80]. An attacker could gain access to a device, modify its components, extract sensitive data, or disable the device entirely. Attackers might also exploit debug ports (e.g., JTAG, UART) to inject malicious firmware, change the behavior of the device, or intercept data [81], [82]. Once compromised, a device may be used as an entry point into the broader network. Example: An attacker gains physical access to an industrial sensor in a smart factory and tampers with the device to give incorrect readings, causing damage to operations.

	Node jamming: In wireless IoT environments, jamming attacks are used to disrupt communication between devices [83]. By generating electromagnetic interference, attackers can prevent devices from sending or receiving data, effectively rendering the system non-functional [84]. Example: In a smart home, an attacker jams the signal of wireless security cameras or door locks, rendering them ineffective and allowing physical entry into the property. *Side-channel attacks*: Side-channel attacks involve exploiting physical characteristics of IoT devices (e.g., power consumption, electromagnetic emissions, or timing information) to infer sensitive information [85], [86]. Attackers can use power analysis to extract cryptographic keys or eavesdrop on the internal workings of a device. Example: An attacker uses power analysis on a smart meter to reverse-engineer its cryptographic key, enabling them to forge meter readings.
Network layer attacks	The network layer handles the communication between IoT devices and between devices and central servers [87]. This layer is vulnerable to various types of attacks, primarily due to the wireless communication protocols used in IoT [88], which often lack strong encryption or authentication. Some of the network layer threats include the following: *Man-in-the-Middle (MitM) attacks*: In a MitM attack, an attacker intercepts the communication between two IoT devices or between a device and the server [89]. The attacker can eavesdrop, modify, or inject data into the communication without the knowledge of the legitimate parties [90], [91]. This type of attack is particularly dangerous in IoT environments where sensitive data, such as health metrics or industrial control data, is transmitted. Example: An attacker intercepts communication between a smart thermostat and the central heating system, altering temperature settings or injecting false commands. Replay attacks: In a replay attack, an attacker captures valid data transmissions between two devices and replays them at a later time to create unauthorized effects [92], [93]. Since many IoT devices do not use proper session management or timestamps, they may accept these replayed messages as legitimate [94]. Example: An attacker captures the wireless signal of a smart car key and replays it later to unlock the vehicle without the owner's knowledge. Spoofing attacks: Spoofing attacks occur when an attacker impersonates a legitimate IoT device to gain unauthorized access to the network or system [95]. The attacker may trick the system into accepting commands from a malicious device or extract sensitive information by pretending to be a trusted entity. Example: In a smart home environment, an attacker spoofs the identity of a smart light switch, gaining access to the network and compromising other devices [96]. *Routing attacks*: Routing attacks target the routing protocols used in IoT networks [97]. Since many IoT devices communicate over wireless mesh networks, attackers can exploit routing vulnerabilities to intercept or alter data packets [98]-[100]. Common types of routing attacks include: Sinkhole attack: An attacker attracts all traffic by advertising a high-quality route, only to drop or manipulate the data passing through [101]. Wormhole attack: Attackers create a virtual link between two distant points in the network, tunneling packets and disrupting normal traffic flow [102].

	Example: In a smart grid, a sinkhole attack diverts sensor data to a compromised node, disrupting electricity distribution by altering real-time grid information. *Denial of Service (DoS) attacks:* A Denial of Service (DoS) attack seeks to overwhelm an IoT device or network, making it unavailable to legitimate users [103], [104]. In many cases, IoT devices are resource-constrained and cannot handle large volumes of traffic, making them prime targets for DoS attacks. A variant of this attack is the Distributed Denial of Service (DDoS) attack, in which a large number of compromised IoT devices (botnets) are used to flood the target system [105]. Example: The Mirai botnet attack in 2016 used compromised IoT devices, including security cameras and routers, to launch a massive DDoS attack, bringing down major websites and services globally. *Eavesdropping and sniffing:* Eavesdropping attacks involve intercepting data as it is transmitted between IoT devices [106]. Without proper encryption, attackers can easily capture sensitive data like login credentials, device control commands, or user information [107], [108]. Example: An attacker intercepts unencrypted communication between a fitness tracker and the cloud server to collect personal health data without the user's knowledge.
Application layer attacks	The application layer is where users interact with the IoT system through applications that control or monitor devices [109]. This layer is often targeted with attacks aimed at compromising user data, executing malicious code, or gaining unauthorized control of IoT devices [110], [111]. Some of the threats in the application layer include: *Injection attacks:* Injection attacks involve inserting malicious code or commands into an application's input fields [112]. In IoT environments, injection attacks can take the form of SQL injection, command injection, or script injection, exploiting vulnerabilities in the IoT application's software to gain unauthorized access or control [113]. Example: An attacker exploits a vulnerability in a smart thermostat's web interface to inject malicious commands that alter the device's temperature settings. *Firmware injection:* Firmware injection attacks occur when an attacker replaces or modifies the firmware on an IoT device with malicious code [114]. This allows the attacker to take control of the device, alter its functionality, or create a persistent backdoor for future attacks [115]. Example: An attacker injects malicious firmware into a smart refrigerator, which then becomes part of a botnet used in DDoS attacks. *Malware and ransomware:* IoT devices can be infected with malware that compromises their functionality or uses them for malicious purposes [116]. For example, IoT devices can be infected with ransomware, where the device's functionality is locked until a ransom is paid. Malware can also spread across the IoT network, affecting multiple devices and causing widespread damage. Example: A healthcare facility's IoT medical devices [117] are infected with ransomware, preventing doctors from accessing patient data or controlling critical devices until a ransom is paid. *Privilege escalation*: Privilege escalation attacks occur when an attacker gains higher access rights than initially intended [118]. This could allow an attacker to execute commands, access sensitive data, or reconfigure devices that should have been restricted [119]. Example: An attacker with access to a smart home camera system escalates privileges to gain control over other IoT devices on the network, such as smart locks and thermostats.

Table 2 above gives an extensive description of various types of attacks in IoT environments, categorized based on the layers of IoT architecture and the attack methodologies. Therefore, as the Internet of Things (IoT) grows, connecting billions of devices globally, it also introduces new attack vectors and vulnerabilities that can be exploited by malicious actors [75]. IoT environments are particularly attractive to attackers due to their vast scale, the diversity of devices, the critical nature of some of the systems they support (e.g., healthcare, smart cities, industrial controls), and the generally weak security measures that many devices employ [76], [77].

3.2. Privacy challenges in IoT

Privacy dangers in IoT arise from the vast amount of personal data that connected devices collect, store, and share, often without users' full awareness or control. Devices like smart home assistants, wearable health trackers, and connected vehicles gather sensitive information, including location, health metrics, and usage patterns. If not properly secured, this data can be accessed by unauthorized parties, leading to privacy breaches, identity theft, or profiling for malicious purposes. Furthermore, weak data protection practices by manufacturers or third-party services can increase the risk of data leaks or unauthorized sharing. To mitigate privacy risks, stronger data encryption, transparent data policies, and user control over data collection and sharing are essential in IoT ecosystems. Some of the prominent privacy challenges in an IoT environment include the following.

- *Massive data collection*: One of the core functions of IoT devices is to collect large volumes of data from the environment, often including sensitive information about individuals, such as location, health metrics, and behavioral patterns [120]. The continuous nature of data collection, coupled with the often opaque nature of data usage, raises significant privacy concerns [121]. Many users are unaware of the extent of data collection or how their data is being used, shared, or sold, creating an environment ripe for privacy violations.
- *Lack of user consent and control:* Many IoT systems fail to implement adequate mechanisms for obtaining user consent for data collection and processing [122]. In many cases, users are unaware of what data is being collected, where it is being stored, or how it is being used. Additionally, IoT systems often lack sufficient controls to allow users to manage or revoke access to their data, leading to privacy issues related to user autonomy and control [123], [124]. Regulatory frameworks like GDPR emphasize the importance of obtaining explicit user consent, but many IoT systems struggle to meet these requirements.
- *Data localization and ownership*: IoT devices generate data that may be stored in multiple locations, including cloud servers hosted in different countries [125]. This raises concerns about data ownership and jurisdiction. Different countries have different data protection laws, and users may not know where their data is stored or who has access to it [126]. Additionally, there is ambiguity about who owns the data generated by IoT devices, whether it is the user, the device manufacturer, or a third party providing cloud services.
- *Data inference and profiling*: IoT devices collect seemingly innocuous data, but when aggregated and analyzed, this data can reveal detailed insights about an individual's habits, preferences, and behaviors [127]. For example, smart home devices can infer when someone is home, asleep, or engaging in specific activities based on sensor data [128]. This aggregation and analysis can lead to unwanted profiling, allowing companies or third parties to use the data for targeted advertising or even discriminatory practices.
- *Anonymity and data de-anonymization*: Many IoT systems anonymize data to protect user privacy [129], as shown in Figure 10. However, anonymization is often inadequate, as de-anonymization techniques can be used to re-identify individuals by cross-referencing data from multiple sources [130], [131]. The combination of data from various IoT devices (e.g., smart home systems, wearable health devices, and location trackers) can create detailed profiles of individuals, even if the original data was anonymized.
- *Data breaches and unauthorized access*: Data breaches are a significant privacy threat in IoT systems [132]. As IoT devices collect sensitive data, a breach can expose personally identifiable information (PII) or confidential information [133]. Unauthorized access to IoT data can result from weak authentication mechanisms, poor encryption practices, or vulnerabilities in cloud infrastructure [134], [135]. This can lead to identity theft, surveillance, and other privacy violations.

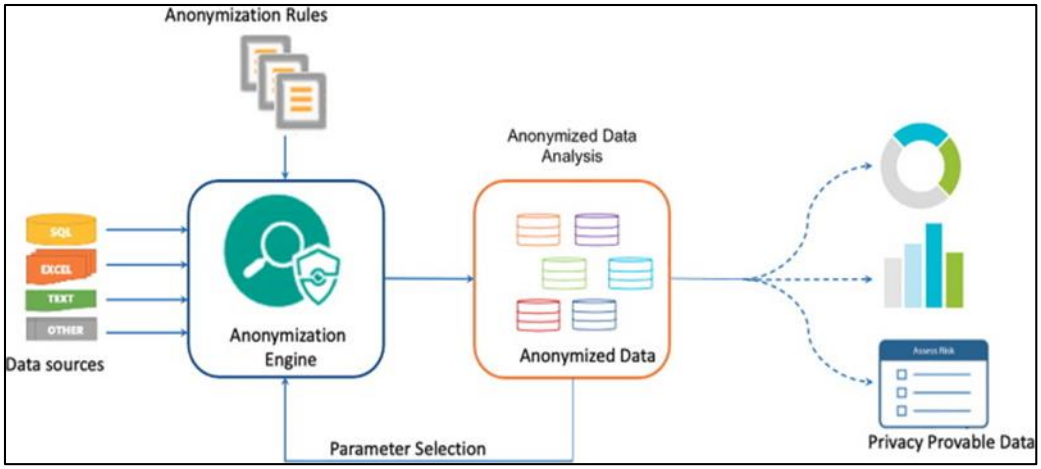

Figure 10 Data anonymization in IoT

Basically, data anonymization is masking users' identities when data is collected from connected devices, ensuring that personal details cannot be directly traced back to individuals. However, data de-anonymization occurs when supposedly anonymous data is cross-referenced with other datasets or analyzed to reveal identifying information. Due to the detailed, continuous nature of IoT data—such as location, behavior patterns, or device usage—it becomes easier for attackers or even legitimate entities to reverse-engineer the data and re-identify individuals. This poses significant privacy risks, as sensitive information can be exposed even when anonymization techniques are applied. Stronger anonymization methods, combined with limiting the amount of personal data collected, are key to protecting privacy in IoT systems.

Regulatory compliance: With the introduction of data protection regulations like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, IoT systems are under increasing pressure to comply with strict data protection requirements. However, due to the decentralized and distributed nature of IoT systems, compliance with regulations related to data minimization, user consent, and data retention can be challenging [136]. Non-compliance can result in legal penalties and damage to a company's reputation.

Data retention and deletion: IoT systems often store data for long periods, either locally on devices or in the cloud. However, these systems may lack proper data retention policies, leading to data being kept longer than necessary, which increases the risk of misuse or breaches [137]. Furthermore, data deletion policies may not be well-defined, making it difficult for users to ensure that their data is fully erased once they stop using a device or service, posing long-term privacy risks. Table 3 below summarizes some of the attacks against privacy in an IoT environment.

Table 3 Privacy attacks in IoT

Attack	Description
Data breaches	A data breach occurs when an attacker gains unauthorized access to the data stored on IoT devices or transmitted across IoT networks [138]. Given the sensitive nature of data collected by IoT devices—such as personal health information, location data, or behavioral patterns—data breaches can have severe privacy consequences for individuals and organizations [139]. *Example:* A breach in a smart healthcare system leads to the exposure of patients' medical histories, diagnoses, and treatments.
Tracking and surveillance	IoT devices that collect location data, such as smartwatches or connected vehicles, can be used for tracking individuals' movements and behaviors [140]. Attackers can exploit vulnerabilities in these devices to conduct unauthorized surveillance, posing significant privacy risks. *Example:* An attacker exploits vulnerabilities in a smart city's traffic management system [141] to track the movements of specific vehicles in real-time.

Inference attacks	Inference attacks occur when an attacker gathers seemingly benign data from IoT devices and correlates it with other data to infer sensitive information [142]. For example, patterns of electricity usage from a smart meter could reveal when residents are home or away, potentially aiding criminals in planning a burglary [143]. *Example:* An attacker infers a household's daily routine based on energy consumption data collected from smart home devices.

Since IoT environments are heavily data-driven, basically the privacy attacks exploit the sensitive personal or organizational data collected by IoT devices.

3.3. Attacks on the cloud and backend infrastructure

Many IoT devices rely on cloud-based infrastructure for data storage and processing [144]. Attacks on cloud services and backend systems can disrupt entire IoT ecosystems and expose vast amounts of sensitive data [145].

- *Cloud hijacking*: In cloud hijacking attacks, attackers gain control of the backend cloud infrastructure used to manage IoT devices [146]. It is the unauthorized takeover of cloud computing accounts or services, which can occur in IoT environments where devices rely heavily on cloud infrastructure for data processing, storage, and management. Attackers may exploit weak authentication mechanisms, phishing attacks, or vulnerabilities in the cloud provider's security to gain access to sensitive data, manipulate devices, or disrupt services. Once they hijack an account, malicious actors can access confidential information, deploy ransomware, or even use the compromised resources for illicit activities, such as launching DDoS attacks. To mitigate the risks of cloud hijacking, organizations should implement strong authentication protocols, regularly monitor cloud activity for unusual behavior, and employ comprehensive security measures to protect against potential breaches. Once compromised, the attacker can manipulate data, disrupt services, or even disable entire IoT networks.
  Example: A cloud-based IoT platform managing smart homes is compromised, allowing attackers to control devices like lights, locks, and thermostats across multiple homes [147].
- *Data poisoning*: Data poisoning attacks involve tampering with the data stored or processed in the cloud [148]. By altering or injecting false data, attackers can compromise the integrity of IoT services or make critical systems behave unpredictably [149].
  Example: In an industrial IoT system, attackers inject false sensor readings into the cloud platform, causing faulty decision-making and disrupting manufacturing processes.

It is clear that IoT environments face a wide range of sophisticated attacks across various layers of the architecture. From physical tampering of devices to cloud-based attacks, the vulnerabilities of IoT systems are numerous and diverse. As IoT continues to evolve and play a crucial role in everyday life, it is essential to develop robust security frameworks and privacy mechanisms to mitigate these threats. This requires a comprehensive approach that involves securing the hardware, network communication, data storage, and application software in IoT systems. The interconnected and pervasive nature of IoT devices creates a vast attack surface for both security breaches and privacy violations. Addressing these challenges requires a multifaceted approach, including stronger authentication mechanisms, secure communication protocols, robust data encryption, and privacy-by-design principles. As IoT ecosystems continue to evolve, collaboration between device manufacturers, network operators, and regulatory bodies is essential to create secure and privacy-aware systems that protect users and their data from exploitation and misuse.

3.4. Performance challenges in IoT

The Internet of Things (IoT) integrates vast numbers of devices, generating and processing data across diverse environments. As IoT systems grow in complexity and scale, several performance challenges emerge [150]. These challenges can impact the efficiency, responsiveness, and overall effectiveness of IoT applications. Below is an extensive discussion of the key performance challenges faced by IoT systems. Table 4 below gives a summary of the performance issues in an IoT environment.

Table 4 Performance issues in an IoT environment

Performance issue	Details
Scalability	*Device and network scalability:* As IoT networks expand, managing and maintaining a large number of devices becomes increasingly complex [151]. Scalability issues arise from the need to accommodate a growing number of devices, each generating data and requiring network resources [152]. This includes challenges related to addressing, managing, and coordinating communications among potentially millions of devices. Challenge: High overhead in managing device registration, network traffic, and resource allocation can lead to inefficiencies [153] and degraded performance as the number of devices scales up. *Data handling and processing:* With the proliferation of IoT devices, the volume of data generated is enormous [154]. The system must be capable of handling, storing, and processing this data efficiently. Scalability challenges arise in data management and analytics platforms, which must be able to scale horizontally to accommodate increasing data loads [155]. Challenge: Insufficient scalability in data processing systems can lead to bottlenecks, latency in data processing, and potential loss of valuable information.
Latency and response time	*Communication latency:* Latency refers to the time delay between sending a request and receiving a response [156]. In IoT systems, communication latency can be affected by factors such as network congestion, signal interference, and the distance between devices [157]. Low-latency communication is critical for applications requiring real-time responses, such as autonomous vehicles or industrial control systems. Challenge: High latency can impair the performance of time-sensitive applications, causing delays in critical operations or control commands [158]. *Data processing latency:* Data collected by IoT devices often needs to be processed and analyzed to derive actionable insights [159]. Processing latency, or the time taken to analyze and act on data, can be impacted by the computational power of devices, the efficiency of algorithms, and the workload on processing systems. Challenge: Excessive data processing latency can result in delayed decision-making [160], affecting the effectiveness of applications like predictive maintenance or real-time monitoring.
Bandwidth and throughput	*Bandwidth constraints:* refers to the maximum rate of data transfer across a network [161]. IoT devices often operate over wireless networks with limited bandwidth, which can be a bottleneck for applications that require high data rates or frequent data transmissions. Challenge: Limited bandwidth can restrict the volume of data transmitted [162], leading to potential data loss, reduced application performance, and increased latency. *Throughput:* This is the rate at which data is successfully transmitted through the network [163]. Ensuring sufficient throughput is essential for maintaining performance in IoT systems, especially when handling large volumes of data or high-frequency updates. Challenge: Low throughput can result in network congestion, packet loss, and reduced performance [164], particularly in dense or high-traffic environments.
Energy efficiency	*Power consumption:* Many IoT devices are battery-powered or energy-constrained, making energy efficiency a critical concern [165]. High power consumption can lead to frequent battery

	replacements or recharging, impacting the device's operational lifetime and overall system performance [166]. Challenge: Inefficient power usage can result in reduced device longevity, increased maintenance costs, and potential service interruptions. *Energy-aware protocols:* To address energy efficiency, IoT systems must implement energy-aware communication protocols and strategies [167]. These protocols aim to minimize power consumption while maintaining network performance and reliability [168]. Challenge: Ineffective energy management can lead to trade-offs between power savings and performance, affecting the balance between energy efficiency and system responsiveness.
Resource management	*Resource allocation:* IoT devices often have limited computational resources, including CPU power, memory, and storage [169]. Effective resource management is essential to ensure that devices can perform their tasks efficiently without overloading their limited resources [170]. Challenge: Poor resource allocation can lead to performance degradation, device crashes, or the inability to perform critical functions. *Load balancing:* In distributed IoT systems, load balancing ensures that computational and network loads are evenly distributed across devices and servers [171]. Effective load balancing is necessary to prevent overload on individual devices or components and to maintain overall system performance [172]. Challenge: Inefficient load balancing can lead to bottlenecks, reduced responsiveness, and increased latency in the system.
Reliability and robustness	*Fault tolerance:* IoT systems must be designed to handle faults and failures gracefully [173]. Ensuring reliability involves implementing fault tolerance mechanisms to detect, recover from, and mitigate the impact of device or network failures. Challenge: Lack of fault tolerance can result in system outages, data loss, and degraded performance during failures or disruptions [174]. *Robustness against attacks:* IoT systems are vulnerable to various security threats that can impact their performance [175]. Ensuring robustness against attacks involves implementing security measures that protect against attacks such as denial of service (DoS) [176], which can degrade system performance. Challenge: Security vulnerabilities can lead to performance degradation due to attacks that overwhelm or disrupt the system.
Data storage and management	*Storage constraints:* IoT devices and systems often deal with large volumes of data [177]. Efficient data storage solutions are needed to handle this data, including considerations for on-device storage, cloud storage, and data archiving. Challenge: Limited on-device storage can constrain the amount of data collected and processed locally [178], necessitating efficient data offloading and storage strategies. *Data management and retrieval:* Efficient data management and retrieval mechanisms are crucial for handling and accessing large datasets generated by IoT devices [179]. This includes indexing, querying, and ensuring fast access to stored data.

	Challenge: Inefficient data management can lead to slow data retrieval [180], impacting the performance of data-driven applications and analytics.
Interoperability and integration	*Protocol and standard compatibility:* IoT devices often use different communication protocols and standards, which can impact interoperability and integration [181]. Ensuring seamless communication and integration between diverse devices and systems is essential for maintaining performance. Challenge: Incompatibility between protocols can result in communication inefficiencies [182], data exchange issues, and performance degradation. *Integration with legacy systems*: Many IoT systems need to integrate with existing legacy systems, which may have different performance characteristics and requirements [183]. Effective integration is necessary to ensure that performance is not adversely affected by legacy components. Challenge: Poor integration with legacy systems can lead to inefficiencies, data synchronization issues, and performance bottlenecks.

Evidently, performance challenges in IoT systems are multifaceted and arise from the complexities of managing large-scale, heterogeneous networks of devices. Addressing these challenges involves optimizing scalability, reducing latency, managing bandwidth and energy consumption, and ensuring reliability and robustness. Effective solutions require a combination of advanced technologies, efficient protocols, and comprehensive system design strategies. As IoT continues to evolve, ongoing research and innovation will be crucial in overcoming these performance challenges and enabling the seamless operation of diverse IoT applications.

4. Current solutions for IoT security and privacy enhancement

As the Internet of Things (IoT) continues to expand, ensuring robust security and privacy is paramount. Various solutions have been developed to address the challenges inherent in securing IoT systems and protecting user privacy. Below is an exhaustive discussion of the current solutions for enhancing IoT security and privacy. Table 5 describes some of these current solutions.

Table 5 Current security and privacy solutions

Solution	**Particulars**
Security Solutions	*Authentication and Authorization* Multi-Factor Authentication (MFA) - MFA requires users to provide multiple forms of verification before accessing IoT devices or systems [184]. This usually includes a combination of passwords, biometrics, and security tokens. MFA can be integrated into device on-boarding and access controls. For example, a smart home system might require a password and a biometric scan for device access. Public Key Infrastructure (PKI) - PKI provides a framework for managing digital certificates and public-private key pairs, which are used for secure authentication and data encryption [185]. IoT devices use PKI to authenticate each other and establish secure communication channels [186]. This is commonly used in industrial IoT systems and critical infrastructure. OAuth and OpenID Connect - OAuth is an authorization framework that allows third-party applications to access user resources without exposing credentials. OpenID Connect extends OAuth to provide authentication. These protocols can be used for secure API access and user authentication in IoT ecosystems, enabling secure interactions between devices and applications. *Data encryption*

	End-to-End Encryption (E2EE) - E2EE ensures that data is encrypted on the sender's device and only decrypted on the receiver's device, preventing unauthorized access during transmission [188]. IoT devices can use E2EE for secure communication, such as encrypting sensor data transmitted to cloud platforms [189]. Common algorithms include AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman). TLS/SSL (Transport Layer Security / Secure Sockets Layer) - TLS/SSL protocols secure data transmission over networks by encrypting the communication channel between devices and servers [190]. IoT devices and servers use TLS/SSL to establish secure connections, protect data in transit, and prevent eavesdropping and man-in-the-middle attacks. *Device security* Secure Boot - Secure boot ensures that devices start up using only trusted software by verifying the integrity of the bootloader and firmware before executing [191]. IoT devices incorporate secure boot mechanisms to prevent unauthorized firmware from being executed, thus protecting against firmware tampering [192]. Hardware Security Modules (HSMs) and Trusted Platform Modules (TPMs) - HSMs and TPMs provide hardware-based security features, including cryptographic operations, secure key storage, and device authentication [193]. IoT devices integrate HSMs or TPMs to enhance security, manage cryptographic keys [194], and ensure secure boot and firmware integrity. Firmware and software updates - Regular updates address vulnerabilities and introduce security patches to protect against known threats. IoT devices support secure firmware updates through digital signatures and encrypted update channels to ensure the authenticity and integrity of updates. *Network Security* Network segmentation and isolation - Network segmentation involves dividing a network into smaller, isolated segments to limit the spread of security breaches [195]. In IoT environments, segments can isolate critical devices from less secure ones, reducing the risk of cross-device attacks. Intrusion Detection and Prevention Systems (IDPS) - IDPS monitors network traffic for suspicious activity and can take action to prevent or mitigate attacks [196]. IoT networks use IDPS to detect and respond to anomalies, such as unusual traffic patterns or unauthorized access attempts. Firewalls and Virtual Private Networks (VPNs) - Firewalls control incoming and outgoing network traffic based on security rules, while VPNs encrypt data transmitted over the internet [197]. IoT devices and networks use firewalls to block malicious traffic and VPNs to secure remote access and data transmission [198].
Privacy solutions	*Data anonymization* Data masking and obfuscation - Data masking replaces sensitive information with fictitious data, while obfuscation makes data more difficult to interpret [199]. IoT systems use data masking to protect personal information [200] while still allowing for data analysis and processing. Differential privacy - Differential privacy adds noise to data to prevent the identification of individual records while preserving overall data utility [201]. IoT platforms use differential privacy techniques to protect user data when performing analytics or sharing aggregated data with third parties [202].

	Access controls and permissions Granular access control - Granular access control allows for detailed permissions based on user roles, device capabilities, and data sensitivity [203]. IoT systems implement role-based access control (RBAC) or attribute-based access control (ABAC) to manage and restrict access to sensitive data and functions [204]. Data minimization - involves collecting and processing only the data necessary for a specific purpose [205], thereby reducing the risk of privacy breaches. IoT applications [206] adopt data minimization principles by limiting data collection to essential information and ensuring that data retention policies are adhered to. *User consent and control* Consent management platforms - allow users to provide, manage, and revoke consent for data collection and processing [207]. IoT devices and applications integrate consent management tools to enable users to control their data privacy preferences and manage consent settings [208]. Privacy policies and transparency - Providing clear privacy policies and transparency about data practices helps users understand how their data is used and protected. IoT providers offer accessible privacy notices and detailed information about data collection, usage, and sharing practices [209]. *Secure data storage* Encryption at rest - Encryption at rest protects data stored on devices and servers from unauthorized access by encrypting it when not in use [210]. IoT devices and cloud platforms use encryption algorithms to secure stored data [211], ensuring that even if physical devices are compromised, data remains protected. Access control mechanisms - Implementing strong access controls [212] ensures that only authorized users and systems can access stored data. IoT systems use access controls and authentication mechanisms to safeguard data stored in databases and cloud storage. *Regulatory compliance* Compliance frameworks - provide guidelines and standards for adhering to privacy regulations, such as GDPR, CCPA, and HIPAA [213]. IoT organizations adopt compliance frameworks to align their practices with regulatory requirements, ensuring that data handling and privacy practices meet legal standards. Privacy Impact Assessments (PIAs) - PIAs evaluate the impact of data processing activities on user privacy and identify potential risks [214]. IoT providers conduct PIAs to assess the privacy implications of new technologies or changes to existing systems [215], helping to mitigate privacy risks and improve data protection.

It is clear that current solutions for IoT security and privacy enhancement encompass a wide range of technologies and practices designed to address the unique challenges of IoT environments. These solutions include advanced authentication methods, data encryption, device security measures, network security protocols, and privacy-preserving techniques [216]-[218]. By implementing these solutions, IoT systems can better protect against security threats, safeguard user privacy, and ensure compliance with regulatory requirements. Ongoing research and innovation will continue to drive the development of more effective and adaptable solutions to meet the evolving needs of the IoT landscape.

5. Research gaps

The Internet of Things (IoT) presents significant opportunities but also poses complex challenges in the areas of security, privacy, and performance [219]. Despite considerable advancements, several research gaps remain in these areas. Addressing these gaps is crucial for enhancing the robustness and efficiency of IoT systems. Below is an extensive discussion of the research gaps across security, privacy, and performance domains.

5.1. Research gaps in IoT security

- *Advanced threat detection and mitigation* - Traditional security mechanisms often fall short in the dynamic and diverse landscape of IoT networks [220]. The rapid evolution of attack techniques and the vast number of devices make it challenging to detect and mitigate threats effectively.

There is a need for advanced threat detection and mitigation systems that can adapt to evolving threats and diverse device types [221], [222]. Research should focus on developing AI-driven anomaly detection systems [223], behavior-based intrusion detection systems, and real-time threat intelligence integration.

- *Securing resource-constrained devices* - Many IoT devices are resource-constrained, making it difficult to implement traditional security measures such as encryption and authentication [224]-[227].

There is a need for lightweight and efficient security protocols tailored for resource-constrained devices [228], [229]. Research should explore novel encryption methods, lightweight authentication schemes, and secure communication protocols that balance security and resource constraints.

- *Device identity and authentication* - Ensuring robust identity and authentication for a vast number of IoT devices is challenging [230], particularly when dealing with devices with limited computational resources.

There is a need for scalable and secure device identity management and authentication solutions [231], as shown in Figure 11. Research should investigate decentralized identity systems, blockchain-based authentication methods, and efficient key management schemes.

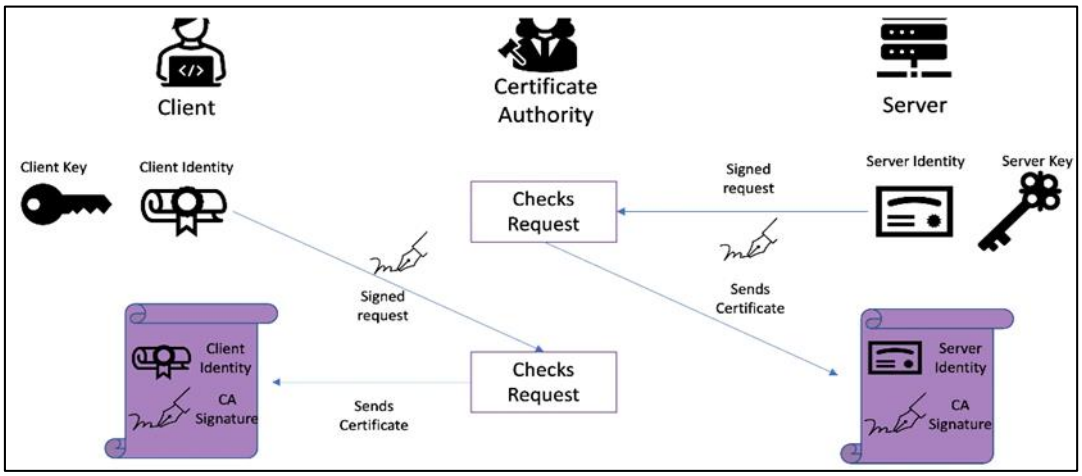

Figure 11 IoT device identity and authentication

Device identity and authentication in IoT are crucial for ensuring that only legitimate devices can connect to a network and communicate with other systems. Each IoT device must have a unique identifier to distinguish it from others, allowing for secure interactions within the network. Authentication mechanisms, such as digital certificates, cryptographic keys, or secure tokens, are employed to verify the identity of devices before granting access. However, many IoT devices lack robust authentication due to resource constraints, leading to vulnerabilities such as unauthorized access or impersonation. Effective device identity management and strong authentication practices are essential to securing IoT ecosystems, preventing malicious actors from exploiting weaknesses to gain control over devices or access sensitive data.

- *Interoperability and standardization* - The lack of standardization and interoperability among IoT devices and systems can lead to security vulnerabilities and integration issues [232].

There is a need for comprehensive standards and frameworks that ensure interoperability while maintaining security [233]. Research should focus on developing universal security standards, interoperable protocols, and secure integration practices.

- *Firmware and software security* - IoT devices often run outdated or vulnerable firmware, making them susceptible to attacks [234]. [235].

Research should address secure firmware updates, including mechanisms for verifying and validating firmware integrity, secure boot processes, and efficient patch management strategies.

5.2. Research gaps in IoT privacy

- *Data anonymization and de-anonymization* - Data anonymization techniques are often insufficient, and attackers can use de-anonymization methods to re-identify individuals [236].

There is a need for advanced anonymization techniques that resist de-anonymization attacks [237]. Research should explore privacy-preserving data mining, advanced cryptographic techniques, and robust anonymization algorithms.

- *User consent and data ownership* - Many IoT systems lack effective mechanisms for obtaining user consent and managing data ownership [238].

Research should focus on developing user-centric consent management systems, transparency mechanisms, and frameworks for data ownership and control. This includes exploring decentralized consent management and user-controlled data access models.

- *Privacy-preserving data aggregation* - Aggregating data from multiple IoT devices as shown in Figure 12, can compromise individual privacy if not handled properly [239].

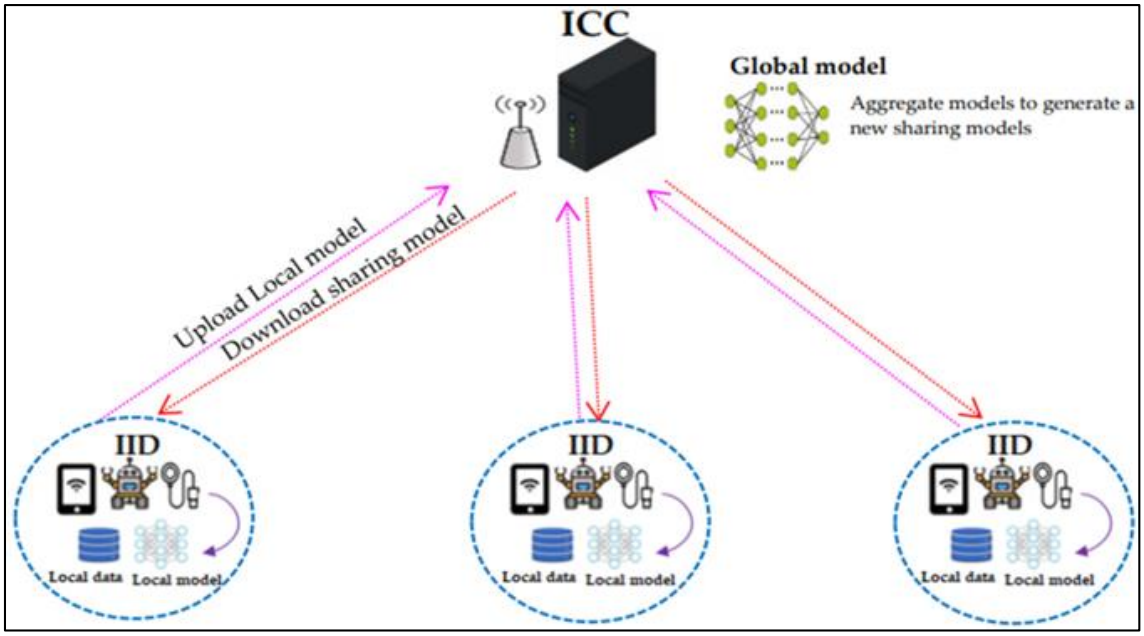

Figure 12 Data aggregation

Research should address privacy-preserving data aggregation techniques that allow for useful data analysis while protecting individual privacy [240], [241]. This includes exploring secure multi-party computation, federated learning, and differential privacy techniques.

- *Regulatory compliance and frameworks* - Compliance with privacy regulations (e.g., GDPR, CCPA) can be challenging due to the decentralized and diverse nature of IoT systems [242].

There is a need for research into privacy frameworks and tools that facilitate compliance with regulatory requirements in IoT environments [243]. This includes developing automated compliance tools, privacy assessment methodologies, and regulatory compliance frameworks tailored for IoT.

- *Context-aware privacy mechanisms* - Privacy needs can vary based on the context in which data is collected and used [244].

Research should focus on developing context-aware privacy mechanisms that adapt privacy controls based on the data context, user preferences, and environmental factors.

5.3. Research gaps in IoT performance

- *Scalability and resource management* - Managing performance and resource allocation in large-scale IoT networks is complex, and traditional approaches may not scale effectively.

Research should explore scalable resource management techniques, efficient load balancing [245], and dynamic resource allocation strategies that can adapt to varying network conditions and device capabilities.

- *Latency reduction and real-time processing* - Ensuring low latency and real-time processing in IoT systems, particularly in applications requiring immediate responses, is challenging [246].

Research should focus on optimizing communication protocols [247], data processing algorithms, and edge computing strategies to minimize latency and support real-time applications.

- *Energy efficiency and battery management* - Many IoT devices are battery-powered, and energy efficiency is crucial for maintaining long device lifetimes and operational efficiency [248].

Research should address energy-efficient communication protocols, energy-aware algorithms, and advanced battery management techniques [249]. This includes exploring energy harvesting technologies and low-power operation strategies.

- *Data storage and management* - Managing and storing large volumes of data generated by IoT devices poses performance and scalability challenges [250].

Research should explore efficient data storage solutions, data management frameworks, and distributed storage systems that can handle the high volume and velocity of IoT data [251].

- *Quality of Service (QoS) and network performance* - Ensuring consistent Quality of Service (QoS) in IoT networks is challenging due to variable network conditions and diverse device capabilities [252].

Research should focus on QoS management techniques, network performance optimization [253], and adaptive networking protocols that ensure reliable and efficient performance across diverse IoT environments.

Basically, addressing the research gaps in IoT security, privacy, and performance is essential for developing robust, efficient, and secure IoT systems. Advancements in these areas will require interdisciplinary approaches, innovative solutions, and collaboration among researchers, industry practitioners, and regulatory bodies. Continued research and development in these domains will contribute to overcoming current limitations and realizing the full potential of IoT technologies.

6. Future research scopes

The Internet of Things (IoT) is rapidly evolving, and with this growth come new challenges and opportunities in the realms of security, privacy, and performance. Future research in these areas will be pivotal in addressing existing issues and paving the way for more robust, efficient, and secure IoT systems. Table 6 summarizes some of the future research scopes in IoT security, privacy, and performance.

Table 6 Future research scopes

Scope	Details
Scopes in IoT security	*AI and Machine Learning for Threat Detection* Scope - Leveraging artificial intelligence (AI) and machine learning (ML) for advanced threat detection and response [254]-[257]. AI-driven solutions can analyze vast amounts of data to identify unusual patterns, detect anomalies, and predict potential security breaches [258]. Research focus - Developing adaptive machine learning models that can learn from evolving threats, improve detection accuracy, and minimize false positives. Investigating the integration of AI with existing security frameworks to enhance threat intelligence and automated response mechanisms. *Blockchain for IoT security* Scope - Utilizing blockchain technology to improve IoT security through decentralized and immutable ledgers [259]. Blockchain can offer enhanced device authentication, data integrity, and secure transaction processing. Research focus - Exploring blockchain-based identity management, secure communication protocols, and smart contracts for automating security operations. Investigating scalability, interoperability, and integration challenges of blockchain with IoT systems. *Secure edge and fog computing* Scope - Implementing security measures at the edge and fog layers of IoT architecture to protect data processing and storage closer to the source [260]. Research focus - Developing security protocols for edge and fog computing environments, addressing challenges related to heterogeneous devices, resource constraints, and dynamic deployment scenarios. Enhancing secure data aggregation and processing techniques at the edge. *Hardware-based security solutions* Scope - Investigating hardware-based security solutions to address vulnerabilities in IoT devices, such as secure enclaves, Trusted Platform Modules (TPMs), and hardware security modules (HSMs) [261], [262]. Research focus - Designing secure hardware architectures, developing secure boot mechanisms, and implementing hardware-based cryptographic operations. Evaluating the effectiveness and feasibility of integrating these solutions into diverse IoT devices. *Post-quantum cryptography* Scope -Preparing for the advent of quantum computing by researching cryptographic algorithms resistant to quantum attacks [263]. Research focus - Exploring post-quantum cryptographic algorithms and their integration into IoT systems. Evaluating the performance implications of quantum-resistant encryption and key management schemes.

Scopes in IoT privacy	*Advanced privacy-preserving techniques* Scope - Developing advanced techniques for preserving privacy in IoT environments [264], such as differential privacy, secure multi-party computation (MPC), and homomorphic encryption. Research focus - Enhancing privacy-preserving data aggregation methods, exploring privacy-preserving analytics, and evaluating trade-offs between privacy and data utility. Investigating the applicability and scalability of these techniques in real-world IoT scenarios. *User-centric privacy management* Scope - Creating systems and frameworks that empower users to manage their privacy preferences and data sharing practices effectively [265]. Research focus - Designing user-friendly privacy interfaces, developing granular consent management mechanisms, and exploring user-centric data control models. Investigating methods to integrate privacy management into IoT devices and applications seamlessly. *Privacy-Enhancing Technologies (PETs)* Scope - Incorporating Privacy-Enhancing Technologies (PETs) to enhance user privacy while interacting with IoT systems [266]. Research focus - Investigating the use of PETs such as anonymous credentials, privacy-preserving access controls, and secure data sharing protocols. Evaluating the effectiveness of PETs in protecting user data and ensuring compliance with privacy regulations. *Regulatory and compliance frameworks* Scope - Developing frameworks and tools to ensure compliance with privacy regulations and standards in IoT environments [267]. Research focus - Creating automated compliance tools, privacy impact assessment methodologies, and frameworks for regulatory adherence. Exploring the challenges of implementing and enforcing privacy regulations across diverse IoT systems and jurisdictions. *Context-aware privacy mechanisms* Scope - Implementing context-aware privacy mechanisms that adapt privacy controls based on the context of data collection and usage [268]. Research focus - Developing context-aware privacy models that consider factors such as user location, data sensitivity, and application usage. Investigating techniques to dynamically adjust privacy settings and ensure contextually appropriate data protection.
Scopes in IoT performance	*Next-generation network architectures* Scope - Exploring next-generation network architectures such as 5G and beyond [269], and their impact on IoT performance.

	Research focus - Investigating how emerging network technologies can address performance issues such as latency, bandwidth, and connectivity. Developing strategies to optimize IoT performance in high-speed, low-latency network environments. *Edge and fog computing enhancements* Scope - Enhancing edge and fog computing architectures [270] to improve performance by processing data closer to the source. Research focus - Developing efficient edge computing frameworks, optimizing data processing and storage at the edge, and exploring new fog computing models. Addressing challenges related to resource allocation, load balancing, and network latency. *Energy-efficient IoT solutions* Scope - Designing energy-efficient solutions [271] to extend the operational lifetime of battery-powered IoT devices. Research focus - Investigating low-power communication protocols, energy-efficient hardware design, and energy harvesting techniques. Exploring strategies to optimize power consumption while maintaining device performance. *Data management and storage innovations* Scope - Exploring innovative data management and storage solutions to handle the high volume and velocity of IoT data [272]. Research focus - Developing scalable data storage systems, efficient data retrieval mechanisms, and distributed data management frameworks. Investigating techniques for data compression, indexing, and analytics to enhance performance. *Quality of Service (QoS) optimization* Scope - Improving Quality of Service (QoS) management in IoT networks to ensure reliable and efficient performance [273], [274]. Research focus - Developing QoS frameworks, adaptive network protocols, and performance optimization techniques. Addressing challenges related to network congestion, resource allocation, and dynamic performance requirements.

It is obvious that future research in IoT security, privacy, and performance encompasses a wide range of innovative areas that are essential for advancing IoT technology. By addressing these research scopes, more secure, private, and high-performance IoT systems can be developed that meet the evolving needs of users and applications [275]-[277]. Collaboration among researchers, industry professionals, and regulatory bodies will be crucial in driving these advancements and overcoming the challenges in the rapidly expanding IoT landscape.

7. Conclusion

The Internet of Things (IoT) represents a transformative advancement in technology, connecting a diverse range of devices and enabling unprecedented levels of automation and data exchange. However, the rapid proliferation of IoT devices brings significant challenges in security, privacy, and performance that must be addressed to ensure the

technology's safe and effective deployment. The findings indicate that the IoT landscape is marked by diverse and dynamic security threats, including vulnerabilities in hardware and software, inadequate authentication mechanisms, and susceptibility to various cyberattacks. Effective solutions require advanced threat detection systems, robust encryption protocols, and secure device management practices. Form the privacy perspective, it has been noted that the collection and management of sensitive data pose substantial privacy risks. Challenges include ensuring data anonymization, managing user consent, and complying with privacy regulations. Solutions must focus on privacy-preserving technologies, user-centric privacy management, and adherence to regulatory standards. In term,s of performance, it has been noted that IoT performance issues include managing resource constraints, minimizing latency, and optimizing energy consumption. Addressing these requires advancements in network architectures, edge and fog computing, and efficient data management techniques. It has been noted that the current approaches to enhancing IoT security and privacy include multi-factor authentication, data encryption, and privacy-preserving technologies such as differential privacy. While these solutions offer substantial improvements, they also face limitations, particularly in resource-constrained environments and with regard to balancing data utility and privacy. In terms of performance, solutions like edge computing and advanced data storage techniques address many issues but encounter challenges related to scalability and efficiency. Continuous innovation and adaptation are necessary to overcome these limitations and improve IoT system performance.

Compliance with ethical standards

Disclosure of conflict of interest

The author holds no conflict of interest.

References

[1] Yalli JS, Hasan MH, Badawi A. Internet of things (iot): Origin, embedded technologies, smart applications and its growth in the last decade. IEEE Access. 2024 Jun 24.

[2] Rodney BD. Understanding the paradigm shift in education in the twenty-first century: The role of technology and the Internet of Things. Worldwide Hospitality and Tourism Themes. 2020 Mar 2;12(1):35-47.

[3] Ahmad T, Zhang D. Using the internet of things in smart energy systems and networks. Sustainable Cities and Society. 2021 May 1; 68:102783.

[4] Kumar A, Sharma S, Singh A, Alwadain A, Choi BJ, Manual-Brenosa J, Ortega-Mansilla A, Goyal N. Revolutionary strategies analysis and proposed system for future infrastructure in internet of things. Sustainability. 2021 Dec 22;14(1):71.

[5] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1; 24:100969.

[6] Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of things: Evolution, concerns and security challenges. Sensors. 2021 Mar 5;21(5):1809.

[7] Nag A, Hassan MM, Das A, Sinha A, Chand N, Kar A, Sharma V, Alkhayyat A. Exploring the applications and security threats of Internet of Thing in the cloud computing paradigm: A comprehensive study on the cloud of things. Transactions on Emerging Telecommunications Technologies. 2024 Apr;35(4): e4897.

[8] Tabaa M, Monteiro F, Bensag H, Dandache A. Green Industrial Internet of Things from a smart industry perspectives. Energy Reports. 2020 Nov 1;6:430-46.

[9] Jony AI, Arnob AK. Securing the Internet of Things: Evaluating Machine Learning Algorithms for Detecting IoT Cyberattacks Using CIC-IoT2023 Dataset. International Journal of Information Technology and Computer Science. 2024.

[10] Jony AI, Arnob AK. A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset. Journal of Edge Computing. 2024 May 21;3(1):28-42.

[11] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[12] Aouedi O, Vu TH, Sacco A, Nguyen DC, Piamrat K, Marchetto G, Pham QV. A survey on intelligent Internet of Things: Applications, security, privacy, and future directions. IEEE Communications Surveys & Tutorials. 2024 Jul 18.

[13] Elhoseny M, Thilakarathne NN, Alghamdi MI, Mahendran RK, Gardezi AA, Weerasinghe H, Welhenge A. Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions. Sustainability. 2021 Oct 21;13(21):11645.

[14] Farayola OA, Olorunfemi OL, Shoetan PO. Data privacy and security in it: a review of techniques and challenges. Computer Science & IT Research Journal. 2024 Mar 27;5(3):606-15.

[15] Sun P, Wan Y, Wu Z, Fang Z, Li Q. A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions. Computers & Security. 2025 Jan 1; 148:104097.

[16] Kathole AB, Kimbahune VV, Patil SD, Jadhav AP, Vhatkar KN. Challenges and Key Issues in IoT Privacy and Security. InCommunication Technologies and Security Challenges in IoT: Present and Future 2024 Mar 26 (pp. 37-50). Singapore: Springer Nature Singapore.

[17] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[18] Almutairi R, Bergami G, Morgan G. Advancements and Challenges in IoT Simulators: A Comprehensive Review. Sensors. 2024 Feb 26;24(5):1511.

[19] Nižetić S, Šolić P, Gonzalez-De DL, Patrono L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. Journal of cleaner production. 2020 Nov 20; 274:122877.

[20] Maksimovic M. Greening the future: Green Internet of Things (G-IoT) as a key technological enabler of sustainable development. Internet of things and big data analytics toward next-generation intelligence. 2018:283-313.

[21] Sharma N, Shamkuwar M, Singh I. The history, present and future with IoT. Internet of things and big data analytics for smart generation. 2019:27-51.

[22] Shah Y, Sengupta S. A survey on Classification of Cyber-attacks on IoT and IIoT devices. In2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) 2020 Oct 28 (pp. 0406-0413). IEEE.

[23] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[24] Ahmed SF, Alam MS, Afrin S, Rafa SJ, Taher SB, Kabir M, Muyeen SM, Gandomi AH. Towards a secure 5G-enabled Internet of Things: A survey on requirements, privacy, security, challenges, and opportunities. IEEE Access. 2024 Jan 10.

[25] Abrera J. Data Privacy and Security in Cloud Computing: A Comprehensive Review. Journal of Computer Science and Information Technology. 2024 Jul 9;1(1):01-9.

[26] Rafiq F, Awan MJ, Yasin A, Nobanee H, Zain AM, Bahaj SA. Privacy prevention of big data applications: A systematic literature review. SAGE Open. 2022 May;12(2):21582440221096445.

[27] Shukla S, Hassan MF, Tran DC, Akbar R, Paputungan IV, Khan MK. Improving latency in Internet-of-Things and cloud computing for real-time data transmission: a systematic literature review (SLR). Cluster Computing. 2023 Oct:1-24.

[28] Naveen S, Kounte MR, Ahmed MR. Low latency deep learning inference model for distributed intelligent IoT edge clusters. IEEE Access. 2021 Nov 30; 9:160607-21.

[29] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[30] Gupta BB, Quamara M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience. 2020 Nov 10;32(21):e4946.

[31] Zhang G, Kou L, Zhang L, Liu C, Da Q, Sun J. A new digital watermarking method for data integrity protection in the perception layer of IoT. Security and Communication Networks. 2017;2017(1):3126010.

[32] Qiu T, Chen N, Li K, Atiquzzaman M, Zhao W. How can heterogeneous internet of things build our future: A survey. IEEE Communications Surveys & Tutorials. 2018 Feb 8;20(3):2011-27.

[33] Zainaddin DA, Hanapi ZM, Othman M, Ahmad Zukarnain Z, Abdullah MD. Recent trends and future directions of congestion management strategies for routing in IoT-based wireless sensor network: a thematic review. Wireless Networks. 2024 Apr;30(3):1939-83.

[34] Shi H, Cao G, Ma G, Duan J, Bai J, Meng X. New progress in artificial intelligence algorithm research based on big data processing of IOT systems on intelligent production lines. Computational intelligence and neuroscience. 2022;2022(1):3283165.

[35] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[36] Alqahtani A, Li Y, Patel P, Solaiman E, Ranjan R. End-to-end service level agreement specification for iot applications. In2018 International Conference on High Performance Computing & Simulation (HPCS) 2018 Jul 16 (pp. 926-935). IEEE.

[37] Swamy SN, Kota SR. An empirical study on system level aspects of Internet of Things (IoT). IEEE Access. 2020 Oct 9;8:188082-134.

[38] Nzeako G, Okeke CD, Akinsanya MO, Popoola OA, Chukwurah EG. Security paradigms for IoT in telecom networks: Conceptual challenges and solution pathways. Engineering Science & Technology Journal. 2024 May 5;5(5):1606-26.

[39] Fu JS, Liu Y, Chao HC, Bhargava BK, Zhang ZJ. Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. IEEE Transactions on Industrial Informatics. 2018 Jan 15;14(10):4519-28.

[40] Velayutham A. Methods and algorithms for optimizing network traffic in next-generation networks: Strategies for 5g, 6g, sdn, and iot systems. Journal of Intelligent Connectivity and Emerging Technologies. 2021 May 4;6(5):1-26.

[41] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[42] Angel NA, Ravindran D, Vincent PD, Srinivasan K, Hu YC. Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. Sensors. 2021 Dec 28;22(1):196.

[43] Srirama SN. A decade of research in fog computing: relevance, challenges, and future directions. Software: Practice and Experience. 2024 Jan;54(1):3-23.

[44] La QD, Ngo MV, Dinh TQ, Quek TQ, Shin H. Enabling intelligence in fog computing to achieve energy and latency reduction. Digital Communications and Networks. 2019 Feb 1;5(1):3-9.

[45] Abdulqadir HR, Zeebaree SR, Shukur HM, Sadeeq MM, Salim BW, Salih AA, Kak SF. A study of moving from cloud computing to fog computing. Qubahan Academic Journal. 2021 Apr 27;1(2):60-70.

[46] Parween S, Hussain SZ, Hussain MA, Pradesh A. A survey on issues and possible solutions of cross-layer design in Internet of Things. Int. J. Comput. Networks Appl. 2021 Aug;8(4):311.

[47] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[48] Omolara AE, Alabdulatif A, Abiodun OI, Alawida M, Alabdulatif A, Arshad H. The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security. 2022 Jan 1;112:102494.

[49] Obaidat MA, Obeidat S, Holst J, Al Hayajneh A, Brown J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers. 2020 May 30;9(2):44.

[50] Bansal S, Kumar D. IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. International Journal of Wireless Information Networks. 2020 Sep;27(3):340-64.

[51] Lombardi M, Pascale F, Santaniello D. Internet of things: A general overview between architectures, protocols and applications. Information. 2021 Feb 19;12(2):87.

[52] Triantafyllou A, Sarigiannidis P, Lagkas TD. Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends. Wireless communications and mobile computing. 2018;2018(1):5349894.

[53] Duaa Fadhel Najem, Nagham Abdulrasool Taha, Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Junchao Ma and Dhafer G. Honi. Low-Complexity and Secure Clustering-Based Similarity Detection for Private Files. TEM Journal, 13(2), 2341-2349 (2024).

[54] Alsharif MH, Kelechi AH, Jahid A, Kannadasan R, Singla MK, Gupta J, Geem ZW. A comprehensive survey of energy-efficient computing to enable sustainable massive IoT networks. Alexandria Engineering Journal. 2024 Mar 1;91:12-29.

[55] Kumar PV, Kulkarni A, Mendhe D, Keshar DK, Babu SB, Rajesh N. AI-Optimized Hardware Design for Internet of Things (IoT) Devices. In2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST) 2024 Apr 9 (pp. 21-26). IEEE.

[56] Shahidinejad A, Abawajy J. An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT. ACM Computing Surveys. 2024 Apr 9;56(7):1-38.

[57] Bakhshi T, Ghita B, Kuzminykh I. A Review of IoT Firmware Vulnerabilities and Auditing Techniques. Sensors. 2024 Jan 22;24(2):708.

[58] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[59] Samaila MG, Neto M, Fernandes DA, Freire MM, Inácio PR. Challenges of securing Internet of Things devices: A survey. Security and Privacy. 2018 Mar;1(2):e20.

[60] Uribe JD, Guillen EP, Cardoso LS. A technical review of wireless security for the internet of things: Software defined radio perspective. Journal of King Saud University-Computer and Information Sciences. 2022 Jul 1;34(7):4122-34.

[61] Kampourakis V, Gkioulos V, Katsikas S. A systematic literature review on wireless security testbeds in the cyber-physical realm. Computers & Security. 2023 Jul 7:103383.

[62] Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. Anatomy of threats to the internet of things. IEEE communications surveys & tutorials. 2018 Oct 11;21(2):1636-75.

[63] Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials. 2018 Jul 12;20(4):3453-95.

[64] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[65] Bettayeb M, Nasir Q, Talib MA. Firmware update attacks and security for IoT devices: Survey. InProceedings of the ArabWIC 6th Annual International Conference Research Track 2019 Mar 7 (pp. 1-6).

[66] Tsaur WJ, Chang JC, Chen CL. A highly secure IoT firmware update mechanism using blockchain. Sensors. 2022 Jan 11;22(2):530.

[67] Singh M, Singh M, Kaur S. Issues and challenges in DNS based botnet detection: A survey. Computers & Security. 2019 Sep 1;86:28-52.

[68] McNulty L, Vassilakis VG. IoT botnets: Characteristics, exploits, attack capabilities, and targets. In2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP) 2022 Jul 20 (pp. 350-355). IEEE.

[69] Borys A, Kamruzzaman A, Thakur HN, Brickley JC, Ali ML, Thakur K. An evaluation of IoT DDoS cryptojacking malware and Mirai Botnet. In2022 IEEE World AI IoT Congress (AIIoT) 2022 Jun 6 (pp. 725-729). IEEE.

[70] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[71] Anusha G, Baigmohammad G, Mageswari U. Detection of cyber attacks on IoT based cyber physical systems. InMATEC Web of Conferences 2024 (Vol. 392, p. 01166). EDP Sciences.

[72] Riggs H, Tufail S, Parvez I, Tariq M, Khan MA, Amir A, Vuda KV, Sarwat AI. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors. 2023 Apr 17;23(8):4060.

[73] Méndez Real M, Salvador R. Physical side-channel attacks on embedded neural networks: A survey. Applied Sciences. 2021 Jul 23;11(15):6790.

[74] Ozmen MO, Farrukh H, Celik ZB. Physical Side-Channel Attacks against Intermittent Devices. Proceedings on Privacy Enhancing Technologies. 2024.

[75] Manaa ME, Hussain SM, Alasadi SA, Al-Khamees HA. DDoS attacks detection based on machine learning algorithms in IoT environments. Inteligencia Artificial. 2024 Jul 11;27(74):152-65.

[76] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[77] Arnob AK, Jony AI. Enhancing IoT Security: A Deep Learning Approach with Feedforward Neural Network for Detecting Cyber Attacks in IoT. Malaysian Journal of Science and Advanced Technology. 2024 Sep 8:413-20.

[78] Toman ZH, Hamel L, Toman SH, Graiet M, Valadares DC. Formal verification for security and attacks in IoT physical layer. Journal of Reliable Intelligent Environments. 2024 Mar;10(1):73-91.

[79] Huang S, Lin C, Zhou K, Yao Y, Lu H, Zhu F. Identifying physical-layer attacks for IoT security: An automatic modulation classification approach using multi-module fusion neural network. Physical Communication. 2020 Dec 1;43:101180.

[80] Vetrivel SC, Maheswari R, Saravanan TP. Industrial IOT: Security Threats and Counter Measures. InCommunication Technologies and Security Challenges in IoT: Present and Future 2024 Mar 26 (pp. 403-425). Singapore: Springer Nature Singapore.

[81] Bhardwaj A, Bharany S, Ibrahim AO, Almogren A, Rehman AU, Hamam H. Unmasking vulnerabilities by a pioneering approach to securing smart IoT cameras through threat surface analysis and dynamic metrics. Egyptian Informatics Journal. 2024 Sep 1;27:100513.

[82] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[83] Rafique SH, Abdallah A, Musa NS, Murugan T. Machine learning and deep learning techniques for internet of things network anomaly detection—current research trends. Sensors. 2024 Mar 20;24(6):1968.

[84] Sachintha S, Le-Khac NA, Scanlon M, Sayakkara AP. Data exfiltration through electromagnetic covert channel of wired industrial control systems. Applied Sciences. 2023 Feb 24;13(5):2928.

[85] Tsague HD, Twala B. Practical techniques for securing the Internet of Things (IoT) against side channel attacks. Internet of things and big data analytics toward next-generation intelligence. 2018:439-81.

[86] Polychronou NF, Thevenon PH, Puys M, Beroulle V. A comprehensive survey of attacks without physical access targeting hardware vulnerabilities in iot/iiot devices, and their detection mechanisms. ACM Transactions on Design Automation of Electronic Systems (TODAES). 2021 Sep 13;27(1):1-35.

[87] Baddi Y, Sebbar A, Zkik K, Maleh Y, Bensalah F, Boulmalf M. MSDN-IoT multicast group communication in IoT based on software defined networking. Journal of Reliable Intelligent Environments. 2024 Mar;10(1):93-104.

[88] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[89] Tyagi V, Saraswat A, Kumar A, Gambhir S. Securing IoT Devices Against MITM and DoS Attacks: An Analysis. Reshaping Intelligent Business and Industry: Convergence of AI and IoT at the Cutting Edge. 2024 Oct 15:237-49.

[90] Tyagi V, Saraswat A, Bansal S. An Analysis of Securing Internet of Things (IoT) Devices from Man-in-the-Middle (MIMA) and Denial of Service (DoS). InSmart Cities 2023 Nov 30 (pp. 337-357). CRC Press.

[91] Aoueileyine MO, Karmous N, Bouallegue R, Youssef N, Yazidi A. Detecting and Mitigating MitM Attack on IoT Devices Using SDN. InInternational Conference on Advanced Information Networking and Applications 2024 Apr 10 (pp. 320-330). Cham: Springer Nature Switzerland.

[92] Lazzaro S, De Angelis V, Mandalari AM, Buccafurri F. Is your kettle smarter than a hacker? a scalable tool for assessing replay attack vulnerabilities on consumer iot devices. In2024 IEEE International Conference on Pervasive Computing and Communications (PerCom) 2024 Mar 11 (pp. 114-124). IEEE.

[93] Sandosh S, Saxena R, Shah S, Rachiraju SS. State-of-the-Art of Voice Assistance Technology, Mitigating Replay Attacks: A Comprehensive Discussion. In2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) 2024 Mar 11 (pp. 594-601). IEEE.

[94] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[95] Shafiq M, Gu Z, Cheikhrouhou O, Alhakami W, Hamam H. The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks. Wireless Communications and Mobile Computing. 2022;2022(1):8669348.

[96] Keshary S, Venkatesan K, Padmapritha T, Srinivasan S, Seshadhri S. IoT Device Attacks, Security and Certification. In2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT) 2024 Aug 8 (Vol. 1, pp. 36-42). IEEE.

[97] Alazab A, Khraisat A, Singh S, Bevinakoppa S, Mahdi OA. Routing attacks detection in 6lowpan-based internet of things. Electronics. 2023 Mar 10;12(6):1320.

[98] Lounis K, Zulkernine M. Attacks and defenses in short-range wireless technologies for IoT. IEEE Access. 2020 May 11;8:88892-932.

[99] Ramadan R. Internet of things (iot) security vulnerabilities: A review. PLOMS AI. 2022;2(1).

[100] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[101] Shanmugaraja P, Bhardwaj M, Mehbodniya A, VALI S, Reddy PC. An Efficient Clustered M-path Sinkhole Attack Detection (MSAD) Algorithm for Wireless Sensor Networks. Adhoc & Sensor Wireless Networks. 2023 Jan 1;55.

[102] Ravula PK, Uppalapati S, Karri GR. An early detection and prevention of wormhole attack using dynamic threshold value in VANET. International Journal of Vehicle Information and Communication Systems. 2024;9(2):201-25.

[103] Uddin R, Kumar SA, Chamola V. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks. 2024 Jan 1;152:103322.

[104] Alshahrani MM. A Secure and intelligent software-defined networking framework for future smart cities to prevent DDoS Attack. Applied Sciences. 2023 Aug 30;13(17):9822.

[105] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[106] Farraj A, Hammad E. A Physical-Layer Security Cooperative Framework for Mitigating Interference and Eavesdropping Attacks in Internet of Things Environments. Sensors. 2024;24(16):5171.

[107] Alaba FA, Madu IM, Musa H. Attacks, Challenges, and Countermeasures for an Integrated IoT Framework. Internet of Things and Cloud Computing. 2024 Aug;12(5):28-39.

[108] Cecílio J, Souto A. Security Issues in Industrial Internet-of-Things: Threats, Attacks and Solutions. In2024 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0 & IoT) 2024 May 29 (pp. 458-463). IEEE.

[109] Sudha KS, Jeyanthi N. A review on privacy requirements and application layer security in internet of things (IoT). Cybernetics and Information Technologies. 2021 Sep 1;21(3):50-72.

[110] Nebbione G, Calzarossa MC. Security of IoT application layer protocols: Challenges and findings. Future Internet. 2020 Mar 17;12(3):55.

[111] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[112] Noman HA, Abu-Sharkh OM. Code injection attacks in wireless-based Internet of Things (IoT): A comprehensive review and practical implementations. Sensors. 2023 Jun 30;23(13):6067.

[113] Akinmerese O, Fasanya S, Aderotoye D, Adingupu N, Ezeoke E, Muritala R, Lawal O, Akingbade B, Ifekandu C. Defence Against Command Injection Attacks in a Distributed Network Environment. Open Access Library Journal. 2024 May 9;11(5):1-4.

[114] Feng X, Zhu X, Han QL, Zhou W, Wen S, Xiang Y. Detecting vulnerability on IoT device firmware: A survey. IEEE/CAA Journal of Automatica Sinica. 2022 Sep 6;10(1):25-41.

[115] Nadir I, Mahmood H, Asadullah G. A taxonomy of IoT firmware security and principal firmware analysis techniques. International Journal of Critical Infrastructure Protection. 2022 Sep 1;38:100552.

[116] Yadav CS, Singh J, Yadav A, Pattanayak HS, Kumar R, Khan AA, Haq MA, Alhussen A, Alharby S. Malware analysis in IoT & android systems with defensive mechanism. Electronics. 2022 Jul 28;11(15):2354.

[117] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[118] Karim SS, Afzal M, Iqbal W, Al Abri D. Advanced Persistent Threat (APT) and intrusion detection evaluation dataset for linux systems 2024. Data in Brief. 2024 Jun 1;54:110290.

[119] Mallick MA, Nath R. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News. 2024;190(1):1-69.

[120] Jacob Rodrigues M, Postolache O, Cercas F. Physiological and behavior monitoring systems for smart healthcare environments: A review. Sensors. 2020 Apr 12;20(8):2186.

[121] Elmisery AM, Rho S, Aborizka M. A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. Cluster Computing. 2019 Jan 16;22:1611-38.

[122] Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE internet of things journal. 2017 Mar 15;4(5):1125-42.

[123] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[124] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems. 2018 May 1;82:395-411.

[125] Alam T. Cloud-based IoT applications and their roles in smart cities. Smart Cities. 2021 Sep 17;4(3):1196-219.

[126] Tikkinen-Piri C, Rohunen A, Markkula J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review. 2018 Feb 1;34(1):134-53.

[127] George AS. Digital Hoarding: The Rising Environmental and Personal Costs of Information Overload. Partners Universal Multidisciplinary Research Journal. 2024 Jul 25;1(2):51-67.

[128] Feng S, Setoodeh P, Haykin S. Smart home: Cognitive interactive people-centric Internet of Things. IEEE Communications Magazine. 2017 Feb 3;55(2):34-9.

[129] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[130] Sampaio S, Sousa PR, Martins C, Ferreira A, Antunes L, Cruz-Correia R. Collecting, processing and secondary using personal and (pseudo) anonymized data in smart cities. Applied Sciences. 2023 Mar 16;13(6):3830.

[131] Silva H, Basso T, Moraes R, Elia D, Fiore S. A re-identification risk-based anonymization framework for data analytics platforms. In2018 14th European Dependable Computing Conference (EDCC) 2018 Sep 10 (pp. 101-106). IEEE.

[132] Tawalbeh LA, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and security: Challenges and solutions. Applied Sciences. 2020 Jun 15;10(12):4102.

[133] Lekkala S, Gurijala P. Data Security in the Age of Connectivity. InSecurity and Privacy for Modern Networks: Strategies and Insights for Safeguarding Digital Infrastructures 2024 Oct 8 (pp. 87-97). Berkeley, CA: Apress.

[134] Alghofaili Y, Albattah A, Alrajeh N, Rassam MA, Al-Rimy BA. Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. Applied Sciences. 2021 Sep 27;11(19):9005.

[135] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[136] Karale A. The challenges of IoT addressing security, ethics, privacy, and laws. Internet of Things. 2021 Sep 1; 15:100420.

[137] Cheng L, Liu F, Yao D. Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2017 Sep;7(5):e1211.

[138] Kaur K, Kaur A, Gulzar Y, Gandhi V. Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies. Frontiers in Computer Science. 2024 Jun 26; 6:1420680.

[139] Chernyshev M, Zeadally S, Baig Z. Healthcare data breaches: Implications for digital forensic readiness. Journal of medical systems. 2019 Jan;43:1-2.

[140] Dian FJ, Vahidnia R, Rahmati A. Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A Survey. IEEE access. 2020 Apr 7; 8:69200-11.

[141] Nyangaresi VO, Abduljabbar ZA, Mutlaq KA, Bulbul SS, Ma J, Aldarwish AJ, Honi DG, Al Sibahee MA, Neamah HA. Smart city energy efficient data privacy preservation protocol based on biometrics and fuzzy commitment scheme. Scientific Reports. 2024 Jul 13;14(1):16223.

[142] Pour MS, Bou-Harb E, Varma K, Neshenko N, Pados DA, Choo KK. Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns. Digital Investigation. 2019 Apr 1;28:S40-9.

[143] Althobaiti A, Jindal A, Marnerides AK, Roedig U. Energy theft in smart grids: a survey on data-driven attack strategies and detection methods. IEEE access. 2021 Nov 29;9:159291-312.

[144] Singh N, Buyya R, Kim H. Securing Cloud-Based Internet of Things: Challenges and Mitigations. arXiv preprint arXiv:2402.00356. 2024 Feb 1.

[145] Sequeiros JB, Chimuco FT, Samaila MG, Freire MM, Inácio PR. Attack and system modeling applied to IoT, cloud, and mobile ecosystems: Embedding security by design. ACM Computing Surveys (CSUR). 2020 Mar 13;53(2):1-32.

[146] Hategekimana F, Whitaker TJ, Pantho MJ, Bobda C. IoT Device security through dynamic hardware isolation with cloud-Based update. Journal of Systems Architecture. 2020 Oct 1;109:101827.

[147] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[148] Stokes JW, England P, Kane K. Preventing machine learning poisoning attacks using authentication and provenance. InMILCOM 2021-2021 IEEE Military Communications Conference (MILCOM) 2021 Nov 29 (pp. 181-188). IEEE.

[149] Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. Computer networks. 2020 Mar 14;169:107094.

[150] Rajagopalan A, Swaminathan D, Bajaj M, Damaj I, Rathore RS, Singh AR, Blazek V, Prokop L. Empowering power distribution: Unleashing the synergy of IoT and cloud computing for sustainable and efficient energy systems. Results in Engineering. 2024 Feb 27:101949.

[151] Bittencourt L, Immich R, Sakellariou R, Fonseca N, Madeira E, Curado M, Villas L, DaSilva L, Lee C, Rana O. The internet of things, fog and cloud continuum: Integration and challenges. Internet of Things. 2018 Oct 1;3:134-55.

[152] Čolaković A, Hadžialić M. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer networks. 2018 Oct 24;144:17-39.

[153] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[154] Humayun M. Role of emerging IoT big data and cloud computing for real time application. International Journal of Advanced Computer Science and Applications. 2020;11(4).

[155] Vítor G, Rito P, Sargento S, Pinto F. A scalable approach for smart city data platform: Support of real-time processing and data sharing. Computer Networks. 2022 Aug 4;213:109027.

[156] Makondo N, Kobo HI, Mathonsi TE, Du Plessis D. Implementing an Efficient Architecture for Latency Optimisation in Smart Farming. IEEE Access. 2024 Sep 24.

[157] Ma Z, Xiao M, Xiao Y, Pang Z, Poor HV, Vucetic B. High-reliability and low-latency wireless communication for internet of things: Challenges, fundamentals, and enabling technologies. IEEE Internet of Things Journal. 2019 Mar 25;6(5):7946-70.

[158] Nyangaresi VO, Al Sibahee MA, Abduljabbar ZA, Alhassani A, Abduljaleel IQ, Abood EW. Intelligent Target Cell Selection Algorithm for Low Latency 5G Networks. InAdvances in Computational Intelligence and Communication: Selected Papers from the 2nd EAI International Conference on Computational Intelligence and Communications (CICom 2021) 2022 Dec 14 (pp. 79-97). Cham: Springer International Publishing.

[159] Siow E, Tiropanis T, Hall W. Analytics for the internet of things: A survey. ACM computing surveys (CSUR). 2018 Jul 25;51(4):1-36.

[160] Bennis M, Debbah M, Poor HV. Ultrareliable and low-latency wireless communication: Tail, risk, and scale. Proceedings of the IEEE. 2018 Sep 26;106(10):1834-53.

[161] Chakour I, Daoui C, Baslam M, Sainz-de-Abajo B, Garcia-Zapirain B. Strategic Bandwidth Allocation for QoS in IoT Gateway: Predicting Future Needs Based on IoT Device Habits. IEEE Access. 2024 Jan 8.

[162] Pons M, Valenzuela E, Rodríguez B, Nolazco-Flores JA, Del-Valle-Soto C. Utilization of 5G technologies in IoT applications: Current limitations by interference and network optimization difficulties—A review. Sensors. 2023 Apr 11;23(8):3876.

[163] Bagade S, Kumar BA, Rao LK. Efficient data transmission over 5G Networks with improved accuracy using 802.11 p. Multimedia Tools and Applications. 2024 Apr;83(14):40377-92.

[164] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec;11(4):66.

[165] Wang W, Sobral VA, Billah MF, Saoda N, Nasir N, Campbell B. Low power but high energy: The looming costs of billions of smart devices. ACM SIGENERGY Energy Informatics Review. 2023 Oct 25;3(3):10-4.

[166] Yuksel ME, Fidan H. Energy-aware system design for batteryless LPWAN devices in IoT applications. Ad Hoc Networks. 2021 Nov 1;122:102625.

[167] Silva PV, Taconet C, Chabridon S, Conan D, Cavalcante E, Batista T. Energy awareness and energy efficiency in internet of things middleware: a systematic literature review. Annals of Telecommunications. 2023 Feb;78(1):115-31.

[168] Sheshashayee AV, Petrioli C, Basagni S. On the Impact of Overcoming Wake-up Radio Limitations on the Performance of Energy Aware Routing in Wireless Sensor Networks. In2024 33rd International Conference on Computer Communications and Networks (ICCCN) 2024 Jul 29 (pp. 1-9). IEEE.

[169] Aazam M, Zeadally S, Harras KA. Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities. Future Generation Computer Systems. 2018 Oct 1;87:278-89.

[170] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[171] Fan Q, Ansari N. Towards workload balancing in fog computing empowered IoT. IEEE Transactions on Network Science and Engineering. 2018 Jul 4;7(1):253-62.

[172] Neghabi AA, Navimipour NJ, Hosseinzadeh M, Rezaee A. Load balancing mechanisms in the software defined networks: a systematic and comprehensive review of the literature. IEEE access. 2018 Mar 5;6:14159-78.

[173] Berger C, Eichhammer P, Reiser HP, Domaschka J, Hauck FJ, Habiger G. A survey on resilience in the iot: Taxonomy, classification, and discussion of resilience mechanisms. ACM Computing Surveys (CSUR). 2021 Sep 17;54(7):1-39.

[174] Kirti M, Maurya AK, Yadav RS. Fault-tolerance approaches for distributed and cloud computing environments: A systematic review, taxonomy and future directions. Concurrency and Computation: Practice and Experience. 2024 Jun 10;36(13):e8081.

[175] Rehman Z, Gondal I, Ge M, Dong H, Gregory M, Tari Z. Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception. Computers & Security. 2024 Apr 1;139:103685.

[176] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[177] Dudczyk P, Dunston J, Crosby GV. Blockchain Technology for Global Supply Chain Management: A Survey of Applications, Challenges, Opportunities & Implications (March 2024). IEEE Access. 2024 May 13.

[178] Zhang X, Huang P, Guo L, Fang Y. Social-aware energy-efficient data offloading with strong stability. IEEE/ACM Transactions on Networking. 2019 Jul 9;27(4):1515-28.

[179] Azad P, Navimipour NJ, Rahmani AM, Sharifi A. The role of structured and unstructured data managing mechanisms in the Internet of things. Cluster computing. 2020 Jun;23:1185-98.

[180] Hosen MS, Islam R, Naeem Z, Folorunso EO, Chu TS, Al Mamun MA, Orunbon NO. Data-Driven Decision Making: Advanced Database Systems for Business Intelligence. Nanotechnology Perceptions. 2024 May 12:687-704.

[181] Hazra A, Adhikari M, Amgoth T, Srirama SN. A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions. ACM Computing Surveys (CSUR). 2021 Nov 23;55(1):1-35.

[182] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[183] Givehchi O, Landsdorf K, Simoens P, Colombo AW. Interoperability for industrial cyber-physical systems: An approach for legacy systems. IEEE Transactions on Industrial Informatics. 2017 Aug 17;13(6):3370-8.

[184] Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the Internet of Healthcare Things. Digital health. 2023 May;9:20552076231177144.

[185] El-Hajj M, Beune P. Decentralized Zone-Based PKI: A Lightweight Security Framework for IoT Ecosystems. Information. 2024 May 24;15(6):304.

[186] Goworko M, Wytrębowicz J. A secure communication system for constrained IoT devices—experiences and recommendations. Sensors. 2021 Oct 18;21(20):6906.

[187] Edwards DJ. Internet of Things (IoT) Security. InMastering Cybersecurity: Strategies, Technologies, and Best Practices 2024 Jul 1 (pp. 281-328). Berkeley, CA: Apress.

[188] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[189] Canteaut A, Carpov S, Fontaine C, Fournier J, Lac B, Naya-Plasencia M, Sirdey R, Tria A. End-to-end data security for IoT: from a cloud of encryptions to encryption in the cloud. InCesar Conference 2017 Nov.

[190] Paris IL, Habaebi MH, Zyoud AM. Implementation of SSL/TLS security with MQTT protocol in IoT environment. Wireless Personal Communications. 2023 Sep;132(1):163-82.

[191] Yao J, Zimmer V. Building secure firmware. Apress: New York, NY, USA. 2020:18-48.

[192] El Jaouhari S, Bouvet E. Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions. Internet of Things. 2022 May 1;18:100508.

[193] Al-Omary A, Othman A, AlSabbagh HM, Al-Rizzo H. Survey of hardware-based security support for IoT/CPS systems. KnE Engineering. 2018 Oct 15:52-70.

[194] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[195] A Al-Ofeishat H, Alshorman R. Build a Secure Network using Segmentation and Micro-segmentation Techniques. International Journal of Computing and Digital Systems. 2023 Sep 20;16(1):1499-508.

[196] Azeez NA, Bada TM, Misra S, Adewumi A, Van der Vyver C, Ahuja R. Intrusion detection and prevention systems: an updated review. Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1. 2020:685-96.

[197] Sharp R. Network Security. InIntroduction to Cybersecurity: A Multidisciplinary Challenge 2023 Oct 13 (pp. 171-233). Cham: Springer Nature Switzerland.

[198] Canavese D, Mannella L, Regano L, Basile C. Security at the Edge for Resource-Limited IoT Devices. Sensors. 2024 Jan 17;24(2):590.

[199] Badgujar P. Implementing Data Masking Techniques for Privacy Protection. Journal of Technological Innovations. 2021 Dec 2;2(4).

[200] Ahmad AY, Alzubi J, James S, Nyangaresi VO, Kutralakani C, Krishnan A. Enhancing Human Action Recognition with Adaptive Hybrid Deep Attentive Networks and Archerfish Optimization. Computers, Materials & Continua. 2024 Sep 1;80(3).

[201] Janghyun K, Barry H, Tianzhen H. A review of preserving privacy in data collected from buildings with differential privacy. Journal of Building Engineering. 2022 Sep 15;56:104724.

[202] Hassan MU, Rehmani MH, Chen J. Differential privacy techniques for cyber physical systems: A survey. IEEE Communications Surveys & Tutorials. 2019 Oct 1;22(1):746-89.

[203] Yakubu BM, Ali SM, Khan MI, Bhattarakosol P. PatCen: A blockchain-based patient-centric mechanism for the granular access control of infectious disease-related test records. PloS one. 2024 Sep 18;19(9):e0310407.

[204] Khan JA. Role-Based access Control (RBAC) and Attribute-Based Access Control (ABAC). InImproving Security, Privacy, and Trust in Cloud Computing 2024 (pp. 113-126). IGI Global.

[205] Malek MA. Bigger Is Always Not Better; less Is More, Sometimes: The Concept of Data Minimization in the Context of Big Data. Eur. J. Privacy L. & Tech.. 2021:212.

[206] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[207] Merlec MM, Lee YK, Hong SP, In HP. A smart contract-based dynamic consent management system for personal data usage under GDPR. Sensors. 2021 Nov 30;21(23):7994.

[208] Pathmabandu C, Grundy J, Chhetri MB, Baig Z. Privacy for IoT: informed consent management in smart buildings. Future Generation Computer Systems. 2023 Aug 1;145:367-83.

[209] Lipford HR, Tabassum M, Bahirat P, Yao Y, Knijnenburg BP. Privacy and the Internet of Things. Modern Socio-Technical Perspectives on Privacy. 2022;233.

[210] Seth B, Dalal S, Jaglan V, Le DN, Mohan S, Srivastava G. Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies. 2022 Apr;33(4):e4108.

[211] Singh S, Sharma PK, Moon SY, Park JH. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing. 2024 Feb:1-8.

[212] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[213] Bakare SS, Adeniyi AO, Akpuokwe CU, Eneh NE. Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations. Computer Science & IT Research Journal. 2024 Mar 9;5(3):528-43.

[214] Papamartzivanos D, Menesidou SA, Gouvas P, Giannetsos T. A perfect match: Converging and automating privacy and security impact assessment on-the-fly. Future Internet. 2021 Jan 27;13(2):30.

[215] Georgiadis G, Poels G. Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. Computer Law & Security Review. 2022 Apr 1;44:105640.

[216] Pawar AB, Ghumbre SU, Jogdand RM. Privacy preserving model-based authentication and data security in cloud computing. International Journal of Pervasive Computing and Communications. 2023 Feb 28;19(2):173-90.

[217] Zhang J, Chen B, Zhao Y, Cheng X, Hu F. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE access. 2018 Mar 28;6:18209-37.

[218] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[219] Wójcicki K, Biegańska M, Paliwoda B, Górna J. Internet of things in industry: Research profiling, application, challenges and opportunities—a review. Energies. 2022 Feb 28;15(5):1806.

[220] Schiller E, Aidoo A, Fuhrer J, Stahl J, Ziörjen M, Stiller B. Landscape of IoT security. Computer Science Review. 2022 May 1;44:100467.

[221] Maddireddy BR, Maddireddy BR. Evolutionary Algorithms in AI-Driven Cybersecurity Solutions for Adaptive Threat Mitigation. International Journal of Advanced Engineering Technologies and Innovations. 2021 Aug 16;1(2):17-43.

[222] Mahboubi A, Luong K, Aboutorab H, Bui HT, Jarrad G, Bahutair M, Camtepe S, Pogrebna G, Ahmed E, Barry B, Gately H. Evolving techniques in cyber threat hunting: A systematic review. Journal of Network and Computer Applications. 2024 Aug 23:104004.

[223] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[224] Rozlomii I, Yarmilko A, Naumenko S. Data security of IoT devices with limited resources: challenges and potential solutions. Indoors 2024 Apr 5 (pp. 85-96).

[225] Kumar S, Kumar D, Dangi R, Choudhary G, Dragoni N, You I. A Review of Lightweight Security and Privacy for Resource-Constrained IoT Devices. Computers, Materials and Continua. 2024;78(1):31-63.

[226] Pandey S, Bhushan B. Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks. Wireless Networks. 2024 May;30(4):2987-3026.

[227] Qasem MA, Thabit F, Can O, Naji E, Alkhzaimi HA, Patil PR, Thorat SB. Cryptography algorithms for improving the security of cloud-based internet of things. Security and Privacy. 2024 Jul;7(4):e378.

[228] Ding X, Wang X, Xie Y, Li F. A lightweight anonymous authentication protocol for resource-constrained devices in Internet of Things. IEEE Internet of Things Journal. 2021 Jun 11;9(3):1818-29.

[229] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;1 5:100210.

[230] Azrour M, Mabrouki J, Guezzaz A, Kanwal A. Internet of things security: challenges and key issues. Security and Communication Networks. 2021;2021(1):5533843.

[231] Mamdouh M, Awad AI, Khalaf AA, Hamed HF. Authentication and identity management of IoHT devices: achievements, challenges, and future directions. Computers & Security. 2021 Dec 1; 111:102491.

[232] Lee E, Seo YD, Oh SR, Kim YG. A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials. 2021 Mar 19;23(2):1020-47.

[233] Karie NM, Sahri NM, Yang W, Valli C, Kebande VR. A review of security standards and frameworks for IoT-based smart environments. IEEE Access. 2021 Sep 3;9:121975-95.

[234] Jiang X, Lora M, Chattopadhyay S. An experimental analysis of security vulnerabilities in industrial IoT devices. ACM Transactions on Internet Technology (TOIT). 2020 May 12;20(2):1-24.

[235] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[236] Gadotti A, Rocher L, Houssiau F, Creţu AM, de Montjoye YA. Anonymization: The imperfect science of using data while preserving privacy. Science Advances. 2024 Jul 17;10(29):eadn7053.

[237] Majeed A, Khan S, Hwang SO. Toward privacy preservation using clustering based anonymization: recent advances and future research outlook. IEEE Access. 2022 May 16;10:53066-97.

[238] Alhajri M, Rudolph C, Shahraki AS. A blockchain-based consent mechanism for access to fitness data in the healthcare context. IEEE Access. 2022 Feb 24;10:22960-79.

[239] Chanal PM, Kakkasageri MS. Security and privacy in IoT: a survey. Wireless Personal Communications. 2020 Nov;115(2):1667-93.

[240] Kreso I, Kapo A, Turulja L. Data mining privacy preserving: Research agenda. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2021 Jan;11(1):e1392.

[241] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[242] Fakeyede OO, Okeleke PA, Hassan AO, Iwuanyanwu U, Adaramodu OR. Navigating data privacy through IT audits: GDPR, CCPA, and beyond. International Journal of Research in Engineering and Science. 2023;11(11).

[243] Aly M, Khomh F, Haoues M, Quintero A, Yacout S. Enforcing security in Internet of Things frameworks: A systematic literature review. Internet of Things. 2019 Jun 1;6:100050.

[244] Beierle F, Tran VT, Allemand M, Neff P, Schlee W, Probst T, Pryss R, Zimmermann J. Context data categories and privacy model for mobile data collection apps. Procedia computer science. 2018 Jan 1;134:18-25.

[245] Singh M, Bhardwaj P, Bhardwaj R, Narayan S. Advancing Scalability and Efficiency in Distributed Network Computing Through Innovative Resource Allocation and Load Balancing Strategies. InInternational Conference on Intelligent and Fuzzy Systems 2024 Jul 16 (pp. 722-740). Cham: Springer Nature Switzerland.

[246] Mutlag AA, Abd Ghani MK, Arunkumar NA, Mohammed MA, Mohd O. Enabling technologies for fog computing in healthcare IoT systems. Future generation computer systems. 2019 Jan 1;90:62-78.

[247] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[248] Callebaut G, Leenders G, Van Mulders J, Ottoy G, De Strycker L, Van der Perre L. The art of designing remote iot devices—technologies and strategies for a long battery life. Sensors. 2021 Jan 29;21(3):913.

[249] Selvi M, Thangaramya K, Ganapathy S, Kulothungan K, Khannah Nehemiah H, Kannan A. An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications. 2019 Apr 30;105:1475-90.

[250] Dièn B, Rodrigues JJ, Diallo O, Ndoye EH, Korotaev VV. Data management techniques for Internet of Things. Mechanical Systems and Signal Processing. 2020 Apr 1;138:106564.

[251] Kaya M, Yildirim E. Strategic Optimization of High-Volume Data Management: Advanced Techniques for Enhancing Scalability, Efficiency, and Reliability in Large-Scale Distributed Systems. Journal of Intelligent Connectivity and Emerging Technologies. 2024 Sep 6;9(9):16-44.

[252] Asad M, Basit A, Qaisar S, Ali M. Beyond 5G: Hybrid end-to-end quality of service provisioning in heterogeneous IoT networks. IEEE Access. 2020 Oct 21;8:192320-38.

[253] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[254] Emmann PS. Leveraging Artificial Intelligence and Machine Learning for Threat Detection in Hybrid Cloud Systems. International Journal of Artificial Intelligence & Machine Learning (IJAIML). 2024 May 1;3(01):75-84.

[255] Lad S. Harnessing Machine Learning for Advanced Threat Detection in Cybersecurity. Innovative Computer Sciences Journal. 2024 Aug 6;10(1).

[256] Dalal A, Abdul S, Mahjabeen F, Kothamali PR. Leveraging Artificial Intelligence and Machine Learning for Enhanced Application Security. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 2019 Mar 31;10(1):82-99.

[257] Rodriguez P, Costa I. Artificial Intelligence and Machine Learning for Predictive Threat Intelligence in Government Networks. Advances in Computer Sciences. 2024 Apr 17;7(1):1-0.

[258] Xu X, Patibandla RL, Arora A, Al-Razgan M, Awwad EM, Nyangaresi VO. An Adaptive Hybrid (1D-2D) Convolution-based ShuffleNetV2 Mechanism for Irrigation Levels Prediction in Agricultural Fields with Smart IoTs. IEEE Access. 2024 Apr 3.

[259] Khan AA, Laghari AA, Shaikh ZA, Dacko-Pikiewicz Z, Kot S. Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. IEEE Access. 2022 Nov 18;10:122679-95.

[260] Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors. 2022 Jan 25;22(3):927.

[261] Sharma G, Joshi AM, Mohanty SP. Fortified-grid: Fortifying smart grids through the integration of the trusted platform module in internet of things devices. Information. 2023 Sep 6;14(9):491.

[262] Gunn LJ, Asokan N, Ekberg JE, Liljestrand H, Nayani V, Nyman T. Hardware platform security for mobile devices. Foundations and Trends® in Privacy and Security. 2022 Jun 6;3(3-4):214-394.

[263] Fernandez-Carames TM, Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access. 2020 Jan 23;8:21091-116.

[264] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[265] Cavoukian A. Privacy by design: The seven foundational principles. IAPP Resource Center, https://iapp. org/resources/article/privacy-by-design-the-7-foundational-principles. 2021.

[266] Cha SC, Hsu TY, Xiang Y, Yeh KH. Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. IEEE Internet of Things Journal. 2018 Oct 30;6(2):2159-87.

[267] Alhirabi N, Rana O, Perera C. Security and privacy requirements for the internet of things: A survey. ACM Transactions on Internet of Things. 2021 Feb 1;2(1):1-37.

[268] Sylla T, Chalouf MA, Krief F, Samaké K. Towards a context-aware security and privacy as a service in the internet of things. InInformation Security Theory and Practice: 13th IFIP WG 11.2 International Conference, WISTP 2019, Paris, France, December 11–12, 2019, Proceedings 13 2020 (pp. 240-252). Springer International Publishing.

[269] Jain A, Lopez-Aguilera E, Demirkol I. Are mobility management solutions ready for 5G and beyond?. Computer Communications. 2020 Sep 1;161:50-75.

[270] Gill SS. A manifesto for modern fog and edge computing: Vision, new paradigms, opportunities, and future directions. InOperationalizing Multi-Cloud Environments: Technologies, Tools and Use Cases 2021 Sep 18 (pp. 237-253). Cham: Springer International Publishing.

[271] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[272] Sawitri D. Big Data Challenges And Opportunities In The Development Of Digital Technology. Jurnal Info Sains: Informatika dan Sains. 2024 Jun 24;14(02):215-24.

[273] Badawy MM, Ali ZH, Ali HA. QoS provisioning framework for service-oriented internet of things (IoT). Cluster Computing. 2020 Jun;23(2):575-91.

[274] Said O. Design and performance evaluation of QoE/QoS-oriented scheme for reliable data transmission in Internet of Things environments. Computer Communications. 2022 May 1;189:158-74.

[275] Brotsis S, Limniotis K, Bendiab G, Kolokotronis N, Shiaeles S. On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. Computer Networks. 2021 May 22;191:108005.

[276] Samaila MG, Sequeiros JB, Simoes T, Freire MM, Inacio PR. IoT-HarPSecA: a framework and roadmap for secure design and development of devices and applications in the IoT space. IEEE Access. 2020 Jan 13;8:16462-94.

[277] Abid MA, Afaqui N, Khan MA, Akhtar MW, Malik AW, Munir A, Ahmad J, Shabir B. Evolution towards smart and software-defined internet of things. AI. 2022 Feb 21;3(1):100-23.