Journal of Computational and Experimental Science (JCES)
ISSN Print: 3136-0858 | ISSN Online: 3136-0866
Volume 1, Number 2, 2026, Pages 20–44
Journal Home Page: https://journals.airsd.org/index.php/jces

Review

A Comprehensive Review of Cybersecurity Threats, Vulnerabilities, and Mitigation Techniques in the Internet of Things (IoT)

Muhammad Sami Intizar[1], Maria Sikandar[2], Aqsa Siddique[3], Madiha Sikandar[4], Maria Farooq[3]
[1]Department of Computer Science, Muhammad Nawaz Sharif University of Engineering & Technology, Multan, Pakistan
[2]Department of Digital Forensics and Cyber Security, Hamdard University, Islamabad, Pakistan
[3]Department of Computer Science, Regional Institute of Allied Health Sciences, Mian Channu, Pakistan
[4]Department of Computer Sciences, University of Central Punjab Rawalpindi Campus, Rawalpindi, Pakistan

ARTICLE INFO

Article History:
Received: June 08, 2026
Revised: July 16, 2026
Accepted: July 27, 2026
Available Online: August 05, 2026

Keywords:
Artificial Intelligence, Blockchain, Cybersecurity, Edge Computing, Internet of Things, Network Security, Zero Trust Architecture

Corresponding Author:
Muhammad Sami Intizar
Email:
samiintizar888@gmail.com

ABSTRACT

Internet of Things (IoT) has become a new paradigm that combines physical devices with computing and networking features to form intelligent systems that can accomplish their tasks with minimal human interaction. It is estimated that by 2030, there will be more than 30 billion interconnected IoT devices, which will transfer more than 40 zettabytes of data each year. Nevertheless, this exponential increase has brought surprising cybersecurity issues, and recent evaluations show that over 70% of IoT devices are susceptible to hacking. This review examines the complex security environment of IoT ecosystems, evaluates vulnerabilities at each layer of architecture, explores new threat vectors, and assesses new defense solutions. This paper introduces a systematic review of IoT security issues based on a five-layer architecture and specifically focuses on the vulnerabilities of the network and application layers. It examines the ways in which artificial intelligence, blockchain technology, edge computing, and Zero Trust Architecture will transform IoT security paradigms. This review helps reveal long-standing issues such as resource limitations, device heterogeneity, and scaling challenges through the analysis of actual attack cases and defenses in the field of smart healthcare, industrial IoT, smart cities, and other vital infrastructures. Recommendations on future research directions are then given at the end of the paper with an emphasis on quantum-resistant cryptography, 6G network security, and standardized security frameworks required to construct resilient IoT ecosystems.

Introduction

The Internet of Things (IoT) is one of the most significant technological changes of the 21st century, which has contributed to a fundamental change in the way physical devices communicate with digital systems and human users. The IoT is a widespread system of networked devices, including simple environmental sensors and complicated industrial control systems that collect, process, and share data with minimal human interaction (Gubbi et al., 2013). This technology has entered practically all areas of contemporary society, such as healthcare, energy distribution, transportation, agriculture, and industrial and urban infrastructure (Da et al., 2014).

The development of IoT applications has been impressive. It is estimated that more than 30 billion interconnected IoT devices will be in operation worldwide by the end of 2030, and the amount of data that will be delivered in networks will be more than 40 zettabytes per year (Al-Fuqaha et al., 2015). These expansions have been facilitated by decreasing hardware prices, the ubiquitous nature of networks, further improvements in miniaturization, and the attractive value proposition of a data-based decision-making process in any industry (Wang et al., 2021).

However, the rapid development of IoT has raised serious cybersecurity concerns. According to recent evaluations, over 70% of IoT devices are vulnerable to different types of hacking, which can threaten personal privacy, company properties, and critical state infrastructure (HaddadPajouh et al., 2021). The innate features of IoT, which allow any device to access the Internet anytime and anywhere, can be enormous benefits that can become a serious liability in case of insufficient attention paid to privacy and security (Abomhara & Kokien, 2014).

The inherent nature of IoT systems is a further problem in the security challenge. IoT devices are usually faced with extreme resource limitations, for example, low processing power, limited memory capacity, and exhaustible energy sources (Alaba et al., 2017). These restrictions exclude the use of traditional security measures, which demand massive computing time. Moreover, the massive heterogeneity of IoT devices, communication procedures, and application requirements makes the development and deployment of standardized security solutions challenging (Sicari et al., 2015).

The extent of IoT security threats is highlighted with reference to historical evidence. The Mirai botnet attack in 2016 proved how compromised IoT devices can be used as weapons to create massive distributed denial-of-service attacks that can disrupt key Internet platforms and services (Antonakakis, 2017). Later attacks with Hajime, Reaper, BrickerBot, and VPNFilter have shown even more advanced exploitation schemes in the context of IoT ecosystems (Edwards & Profetis, 2016).

Although research in this area is extensive, there are still major gaps in the knowledge about the field of IoT security, in terms of the cumulative effect of the threat in multiple architectural layers, as well as the implementation of new defensive measures (Nguyen et al., 2025). This paper offers a systematic review of cybersecurity issues and opportunities in the IoT environment. The contributions of this study are as follows:

- This study provides a detailed five-layered IoT system architecture to improve knowledge about the security implications in various functional layers.
- This study also provides a specific analysis of vulnerability, attack vectors, and security measures, with particular emphasis on scientific decision-making, real-time monitoring, and query systems on the network and application layers.
- This study discusses how the new technologies of blockchain, artificial intelligence, software-defined networking (SDN), fog/edge computing, and zero trust architecture can be applied to increase IoT security by providing better context awareness, decentralized trust, and constant verification.
- This study uses real-life case studies of six important areas of IoT to explain how such vulnerabilities appear and how they can be addressed in real-world deployments.
- This study outlines the long-term research issues and suggests directions for developing resilient, scalable, and trustworthy IoT ecosystems in the future.

Methodology

This research utilized an integrative review approach to combine the available literature on the problems and opportunities of cybersecurity in IoT settings (Snyder, 2019). The methodology was developed to search, analyze, and summarize the relevant literature systematically while answering specific research questions.

- **RQ1:** What are the end-to-end vulnerabilities of the IoT architecture at the network and application layer systems?
- **RQ2:** What are the potential attacks on IoT systems, and how do the threats manifest in various application fields?
- **RQ3:** What are the solutions to reducing the threats to IoT security, and what is the effectiveness of these security measures in real-life applications?
- **RQ4:** What is the best approach to using emerging technologies to improve the security of IoT, and what are the difficulties with its implementation?

Search Strategy

Multiple academic databases, such as IEEE Xplore, Science Direct, ACM Digital Library, PubMed, Scopus, and arXiv e-Print Archive, were systematically searched to find the required articles (Snyder, 2019; Da et al., 2014). The search was limited to 2006 through early 2026, to both foundational research and recent advancements (Figure 1).

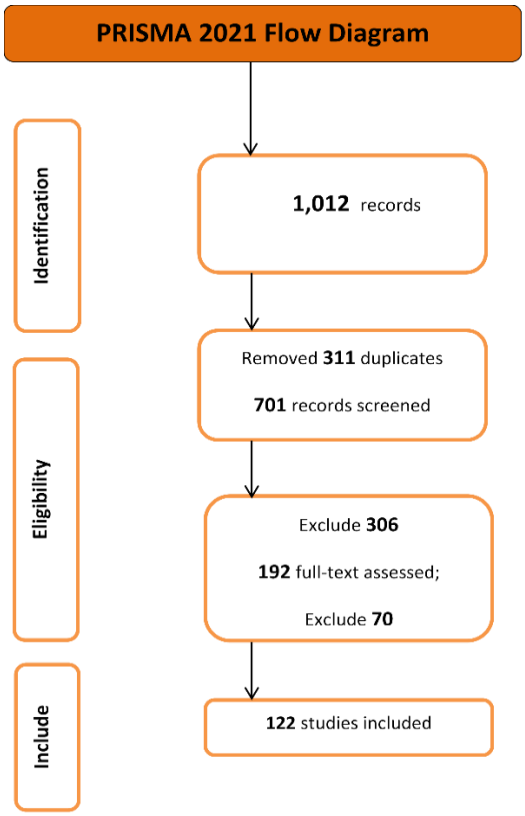

Figure 1. PRISMA Flow diagram

Inclusion Criteria

Studies were included if they (1) addressed IoT security challenges, threats, or countermeasures; (2) were published in peer-reviewed journals, conference proceedings, or reputable preprint servers; (3) provided empirical data, theoretical frameworks, or systematic reviews; and (4) were published in English.

Exclusion Criteria

Studies were excluded if they (1) focused exclusively on general network security without IoT specificity, (2) lacked methodological rigor or clear contributions, or (3) were duplicate publications of the same research.

Analysis Framework

The selected literature was reviewed using a systematic framework that identified the architectural layers of IoT that were addressed, the vulnerabilities or threats investigated, the suggested solutions or countermeasures, the evaluation strategies, and the limitations and research directions. This framework was able to perform a systematic synthesis of the results of diverse studies (Keele, 2007).

IoT Architecture and Security Fundamentals

The concept of IoT architecture is essential to understand the issues of security because network vulnerabilities vary at different levels of functionality, and layer-to-layer interactions provide intricate attack surfaces (Yaqoob et al., 2017).

IoT Architectural Models

Various architectural models have been suggested to conceptualize IoT systems, both simple three-layer models and multi-layered models (Khan et al., 2012).

Three-Layer Architecture

The foundational three-layer architecture comprises the perception, network, and application layers (Wu et al., 2010) (Figure 2).

Perception Layer

Perception Layer, also referred to as the device or sensing layer, includes RFID tags, physical sensors, smart devices, and actuators that are in direct contact with the environment (Al-Fuqaha et al., 2015). These sensors measure raw data humidity, temperature, pressure, motion, and position, and can perform initial processing prior to transmission. The perception layer has extreme constraints: restricted processing power, limited memory, and limited energy resources, which fundamentally reduce security (Ashraf & Habaebi, 2015). This layer has actuators that are commanded by the higher levels to carry out physical actions, which creates a possibility of physical-world effects of cyber-attacks.

Network Layer

This layer enables the transfer of data between the application services and perception devices (Miorandi et al., 2012). It has a wide variety of networking technologies, such as WiFi, LoRaWAN, Zigbee, 5G, cellular networks, and Bluetooth. The network layer performs routing, forwarding, and, possibly, preliminary aggregation of sensor data to processing units, cloud servers, or edge nodes (Whitmore et al., 2015). The key functions involved in congestion control, quality of service management, routing, and addressing. There are serious security issues at this layer owing to the heterogeneity of communication protocols and the resource-constrained nature of numerous IoT networks (Borgohain et al., 2015).

Application Layer

The application layer receives and processes IoT data and provides intelligent services in areas such as smart homes, industrial automation, healthcare, and smart cities (Lin et al., 2017). This layer incorporates cloud environments, data analytics engines, machine learning algorithms, and user interfaces to convert raw sensor data into actionable data (Ray, 2018). It deals with storage of data, intricate processing, decision-making logics, and presentation of information. Attacks at this level may affect not only individual devices but also the entire application ecosystem and sensitive information it carries (Razzaq et al., 2017).

Five-Layer Architecture

With more comprehensive models, the three-layer architecture is expanded to provide the complexity of modern IoT deployments. The five-layer architecture consists of five layers, namely, Perception, Network, Service Management, and Business layer (Edwards & Profetis, 2016) (Figure 2).

Service Management Layer

The Service Management Layer (also known as the middleware layer) interfaces between the network and application layers, which manage devices, process data, discover services, and store information (Chaqfeh & Mohamed, 2012). This layer applies middleware platforms that encapsulate the heterogeneity of networks and devices and offer uniform interfaces to application developers. It handles activities such as data filtering, initial analytics, protocol conversion, and quality-of-service management (Bandyopadhyay et al., 2011). With this special layer, the architecture facilitates better resource utilization, better scalability, and better security due to centralized management operations (Zhou, 2017).

Business Layer

The Business Layer lies on the top of the application layer and it is aware of the fact that IoT systems are business solutions and that they need to be in line with organizational goals and regulatory provisions (Atzori et al., 2010). This layer handles the entire IoT systems, which comprise revenue strategies, business models, decision-making processes, and user privacy. It uses application layer data to create business insights, regulatory compliance, and strategic planning (Perera et al., 2013). The business layer stipulates the security policies, privacy demands, and compliance models that are applied in the lower layers (Weber, 2010).

Fundamental Security Requirements

IoT systems are required to meet fundamental security goals that align with traditional core security requirements, including the consideration of IoT limitations and challenges (Pal et al., 2020) (Figure 3).

Confidentiality: In IoT systems, it is critical to ensure that data is available to authorized parties because devices can frequently gather sensitive personal, medical, or industrial data (Wang et al., 2020). There should be confidentiality in data storage on the devices, transmission through networks, and processing in cloud or edge platforms. The nature of IoT devices makes it difficult to establish a strong encryption mechanism owing to resource constraints (Granjal et al., 2015).

Integrity: Data integrity ensures that no information has been altered improperly either when transferred or stored (Neshenko et al., 2019). Integrity breaches in IoT devices may have drastic effects. Distorted sensor measurements in industrial control systems may cause negative physical reactions, and manipulated healthcare information may result in incorrect medical choices (Chui et al., 2023).

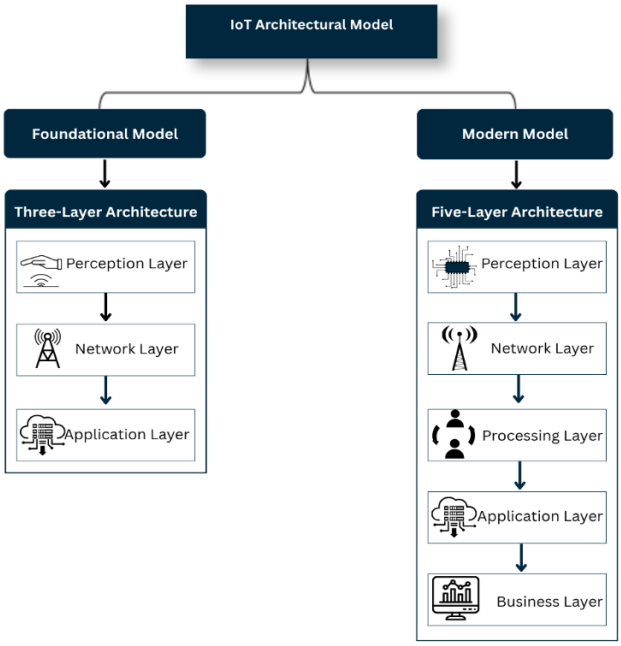

Figure 2. Three-layer and five-layer IoT architectural model

Availability: The availability of IoT services is important, especially in cases where real-time monitoring and control applications are involved (Yang et al., 2017). IoT devices or networks can be affected by a denial-of-service attack that disrupts key services, including home security systems and industrial production lines (Kolias et al., 2017).

Authentication: It is critical to identify the identity of devices, users, and services and authorize them to proceed in environments highly vulnerable to impersonation attacks, which are common in IoT ecosystems (El-Hajj et al., 2021). The authentication of devices is complex because of the sheer scale of IoT implementation and the necessity of lightweight protocols that can be adapted to constrained devices (Kouicem et al., 2018).

Authorization: After the authentication process, entities should be assigned relevant access rights and implemented on the IoT system (Gusmeroli et al., 2013). It is difficult to implement fine-grained access control in dynamic IoT systems because devices can join and leave or switch roles regularly (Lin et al., 2017).

Non-repudiation: It is significant because actions cannot be retracted once they have been performed to ensure accountability and forensic understanding (Yang et al., 2017). In IoT systems, this is especially demanding because of the spread of data generation and processing (Conti et al., 2018).

Privacy: In addition to confidentiality, IoT systems must be approached in terms of wider privacy, such as purpose limitation, data minimization, and control over personal information (Porambage et al., 2016). The data gathering nature of most IoT applications poses tremendous privacy threats that go beyond conventional security issues (Ziegeldorf et al., 2014).

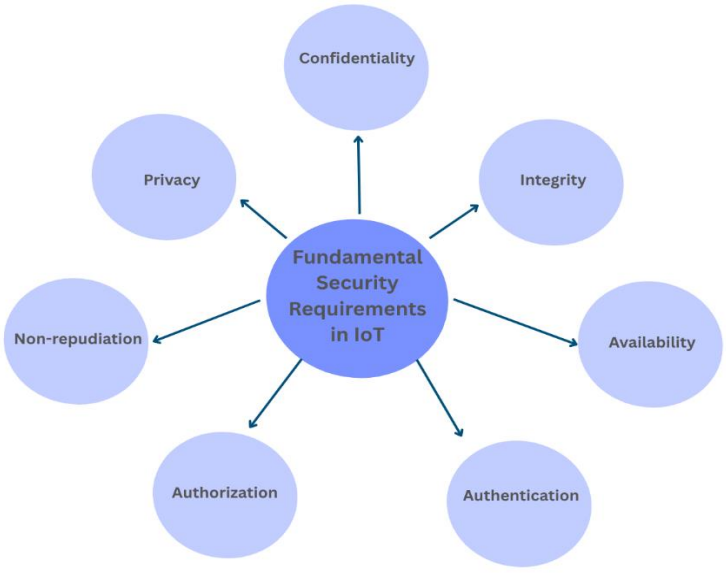

Figure 3. The fundamental security requirements in IoT

Unique IoT Security Challenges

IoT security is differentiated by several peculiar features that compound protection challenges compared to general IT security (Roman et al., 2013). The majority of IoT devices have limited processing capacity, memory usage, and power, which excludes the utilization of traditional security systems, which require substantial processing and memory resources. Lightweight cryptography and high-performance protocols are needed but frequently offer low security margins (Biryukov & Perrin, 2017). IoT devices, operating systems, and communication protocols, as well as application requirements, are extraordinarily diverse, which makes it difficult to develop and implement standardized security solutions. The security mechanisms should support devices that are simple, with an 8-bit microcontroller, to complex edge gateways (Yassein et al., 2017).

IoT deployments may include thousands or millions of devices, which present enormous attack surfaces and make it impractical to manage security manually. Security mechanisms should be automated and scalable without being ineffective (Yan et al., 2014). Most IoT devices are installed in unprotected or hostile physical spaces where malicious parties have physical access. Real-world attacks may steal cryptographic keys, alter device firmware, or replace devices completely (Suo et al., 2012). IoT environments are very dynamic, and devices are constantly coming, going, and changing their location. Security controls should be able to accommodate changing topology as well as trust relationships without human intervention (Khan et al., 2018). IoT devices are frequently in service for many years or decades longer than their original security designs and support. The security of the long lifecycle requires update mechanisms and forward compatibility, which are unavailable to many devices (Bettayeb et al., 2019).

Taxonomy of Threats and Vulnerabilities

IoT systems face a diverse and evolving threat landscape, with attacks targeting different architectural layers, exploiting various vulnerabilities, and pursuing multiple adversarial objectives (Damghani et al., 2019) (Figure 4).

Vulnerabilities across IoT Layers

Perception Layer Vulnerabilities

Physical sensors and actuators make up the perception layer, which has special vulnerabilities owing to the direct exposure to the physical world and the limited resources of the sensing devices (Andrea et al., 2015). Sensors are also vulnerable to physical attacks or environmental factors. Attackers can either saturate sensors with inputs to blind them, spoof them with spoofed signals, or cause physical damage to sensors. The false data obtained by compromised sensors can spread throughout the whole IoT system in real-time monitoring systems, causing decision-making to be corrupted at higher levels (Sfar et al., 2018). Physical tampering of the devices that are used in uncontrolled environments can be physically attacked by removing components, extracting memory, side-channel analysis, and replacing the device. In contrast to traditional IT devices in secure data centers, IoT sensors can be connected to streetlights, fields, or building exteriors, where physical security is not possible (Sfar et al., 2018).

Hackers can reclaim the nodes of the IoT to obtain cryptographic keys or reverse engineer communication protocols or cause the re-programming of devices to do something malicious. After capturing, a device may serve as a beachhead against other network elements (Jing et al., 2014). The global supply chain of IoT components presents the risk of the hardware Trojan malicious modifications to integrated circuits that could leak information, reduce their performance, or create a backdoor. It is very hard to detect this type of Trojan, especially on the low cost commodity devices (Tehranipoor & Koushanfar, 2010).

Network Layer Vulnerabilities

The network layer is vulnerable to features of wireless communications, protocol design and heterogeneous network connectivity. A lot of IoT devices send data without encryption either because of the processing limits or design flaws known as encryption communication. Unsecured messages subject confidential information to eavesdropping and facilitate other types of interception attacks (Keoh et al., 2014). IoT communication procedures, such as Zigbee, Bluetooth Low Energy, LoRaWAN, and 6LoWPAN, have design and implementation vulnerabilities, which attackers can use. The Routing Protocol Low Power and Lossy Networks (RPL) are especially vulnerable to such attacks as routing table poisoning and selective forwarding (Mayzaud et al., 2016).

IoT networks are congested due to their limited bandwidth are vulnerable to flooding attacks that affect the normal flow of communication. DDoS attacks impact battery-powered gadgets in particular and make them stay active, drain power sources rapidly (Matheu et al., 2019). IoT data, once sent through the public networks or common infrastructure, is susceptible to interception and change. Traffic analysis can be used to expose sensitive data regarding device usage and user behaviors even when encrypted with payloads (Keoh et al., 2014).

Application Layer Vulnerabilities

The application layer that contains data processing and service provision exposes vulnerabilities to software complexity, data management, and user interaction (Jing et al., 2014). IoT applications are vulnerable to traditional software bugs such as buffer overflows, injection attacks, and insecure deserialization. Due to the poor testing and updating proficiencies of most IoT devices, the identified vulnerabilities are frequently not patched (Ammar et al., 2018). With cloud-based models, a number of IoT systems are based on cloud engineering, which exposes vulnerabilities to cloud API, web interfaces, and mobile apps. Numerous IoT deployments have been compromised by weak authentication, absent authorization verification, and exposure of data within cloud storage (Khan, 2016). IoT applications tend to store and analyze sensitive personal data from leakage, which poses a threat to privacy due to aggregation, inference, and exposure. Auxiliary information can usually re-identify even the anonymized

data (Christi, 2016). IoT devices and services that are configured improperly cause mass vulnerability. Such common vulnerabilities that attackers actively capitalize on include default credentials, unjustified open ports, and over-permeable access controls (Fagan et al., 2020).

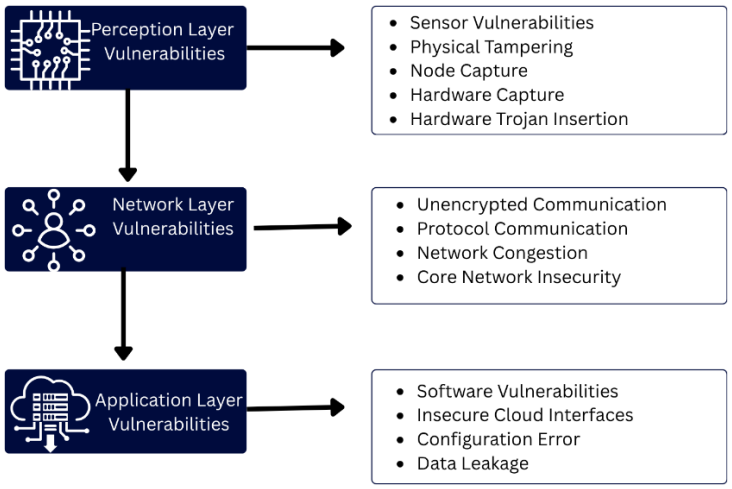

Figure 4. Schematic representation of vulnerabilities across IoT layers

Attack Taxonomy by Layer

Attacks on IoT systems can be categorized by the architectural layer they target, though sophisticated attacks often span multiple layers (Karie et al., 2020) (Figure 5).

Perception Layer Attacks

Direct physical attacks such as destruction of devices, component removal and side-channel analysis. Side-channel attacks steal cryptographic keys through the measurement of power usage, electromagnetic induction or processing time. Attackers tamper the nodes of physical devices to manipulate them either to change their behavior, steal secrets or to add malicious functionality. Compromised nodes might seem to be operating normally but they might secretly be leaking information or may be responding to unauthorized commands.

Jamming attacks that interfere with wireless communication by emitting radio frequency energy (RFE), which overpowers the signals of legitimate communication. Specific devices or communication channels can be targeted and jammed. Fabricated data is inserted into the system by attackers, either by directly attacking sensors or by hacking transmissions and altering them. False data may compromise the processes of making decisions and create a response that is not appropriate (Karie et al., 2020).

Network Layer Attacks

Denial of Service (DoS) is the floods of network resources to hinder the normal communication. DDoS attacks use hacked systems to amplify the amount of attacks. The Mirai botnet of 2016 revealed the potential of thousands of hacked IoT devices to produce new high-scale attacks on DDoS (Bertino & Islam, 2017). Eavesdropping can be defined as passive interception of network communications with the aim of capturing sensitive data. Even encrypted data can leak out information via traffic analysis of the information, which can tell what type of device is being used, the pattern of its activity, as well as the network topology.

Man-in-the-Middle (MitM) is the dynamic interception in which attackers set up their location between the communicating parties and intercept, alter, or inject messages. MitM attacks may impair authentication, steal credentials and maneuver data (Conti et al., 2016). Routing protocols are used to exploit reroute traffic, cause routing loops, or subnet networks. The sinkhole and wormhole attacks diverts traffic to a rogue node and constructs tunnels, respectively, which alter the network topology (Wallgren et al., 2013). In Sybil attacks, attackers generate numerous false identities to weaken reputation systems, voting process or distribution of resources. Sybil attacks may interfere with data aggregation, consensus mechanism, and trust management in the framework of IoT networks (Zhang et al., 2014).

Application Layer Attacks

Attacking the authentication systems to obtain unauthorized access. They usually use default credentials, weak passwords, and broken authentication protocols as access points (Keoh et al., 2014). SQL Injection is a method of hacking into data inside a database by utilizing application interfaces. Decades of awareness have not helped many IoT web interfaces to resist injection attacks (Halfond et al., 2006). Cross-site Scripting (XSS) introducing the unsafe scripts into internet of things interfaces to steal session tokens, redirect clients, or damage interfaces (Wallgren et al., 2013).

Firmware attacks trying to exploit the weaknesses in device firmware or control over legitimate firmware and replacing it with a malicious one. Lax update systems allow malicious softwares to be installed on the systems (Halfond et al., 2006). Data breaches are the unauthorized access to sensitive data in stored in IoT applications or cloud backends. Verkada, another security camera breach of 2021, resulted in the exposure of live images of thousands of surveillance cameras using compromised administrative credentials (Nguyen et al., 2025).

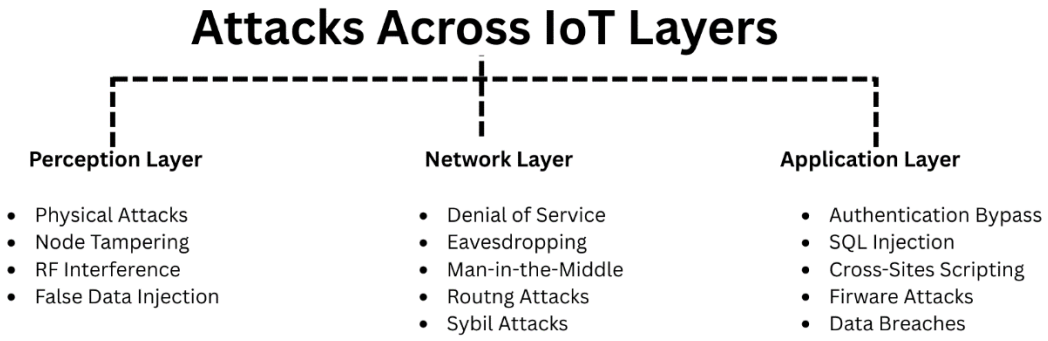

Figure 5. Categorization of attacks across IoT layers

Notable IoT Attack Incidents

Historical attacks provide concrete evidence of IoT vulnerabilities and their real-world impacts.

Mirai Botnet (2016) targeted hundreds of thousands of IoT devices (mainly routers and cameras) through inventing default passwords. These hacked systems were exploited to make huge DDoS attacks, such as to DNS provider Dyn, paralyzing access to major websites such as Twitter, Netflix, and PayPal. Mirai showed how insecure IoT devices may be a systemic risk (Kolias et al., 2017).

Hajime Botnet (2016) appeared together with Mirai, making use of more advanced peer-to-peer interaction and a more flexible structure. Hajime, in contrast to Mirai, seemed to enforce defensive capabilities that safeguarded infected devices, but its final objective is not entirely understood (Edwards & Profetis, 2016).

Emerging Threat Vectors

The threat level of IoT keeps changing as the new attack vectors use new technologies and deployment patterns. ML-based intrusion detection can be bypassed in the evasion of adversarial machine learning. Hackers apply generative AI to generate plausible phishing messages that attack IoT users or they use AI to automate vulnerability discovery (Goodfellow et al., 2014). Before deployment, hacking IoT devices using infected components, malware, or a modified software library. The IoT supply chain is globalized, which leaves a lot of points of intervention to advanced attackers (Rostami et al., 2014). Ransomware is becoming more and more popular with IoT targets, especially in industrial and healthcare environments where physical damage is instantly felt. Hackers also scramble the settings or information on devices, and require money to unscramble them (Zahra & Shah, 2017).

Next-generation networks bring novel attack surfaces due to software-defined networking, network slicing and integration of edge computing. The connectivity and capability of 5G/6G networks are likely to increase the effects of successful attacks (Ahmad et al., 2018). Future quantum computers have the potential to compromise existing cryptographic algorithms, and this puts the future security of IoT systems at risk. Quantum-resistant cryptography cannot be done on the processing capacity of many IoT devices (Bernstein, 2025).

Security Solutions and Defense Mechanisms

Addressing IoT security challenges requires multi-layered defense strategies that combine preventive, detective, and responsive controls adapted to IoT constraints.

Cryptographic Mechanisms

Cryptography offers basic security services but needs to be changed to IoT resource constraints. Specialized Lightweight Cryptographic algorithms are used in limited devices and are engineered to fit the device (Khan et al., 2025). Some of the lightweight algorithms such as ASCON an authenticated encryption have been standardized by National Institute of Standards and Technology (NIST). The security of these algorithms is acceptable at low processing, memory and energy costs (McKay et al., 2016). Trusted Execution Environments (TEE) and Hardware Security Modules (HSM) are secure key archives and cryptographic functions separated out of main processors. Cryptographic keys are still secured even in cases where the software of the device is breached (Sabt et al., 2015). Physical Unclonable Functions (PUFs) use natural differences in the manufacturing process to produce a unique identification of the devices and cryptography keys without any form of persistent storage. PUFs are also resistant to physical cloning and extraction attacks, making them useful in authentication of the IoT devices (Herder et al., 2014; Dritsas & Trigka, 2025).

Authentication and Access Control

Strong identity management is a necessity in the large scale IoT deployments. Mutual device infrastructure-network authentication eliminates impersonation and unauthorized access. Lightweight protocols in symmetric cryptography or PUFs, address the device constraints and offer strong assurance (Mahalle et al., 2012). Public key infrastructure (PKI) can be scaled to millions of devices with automated certificate enrollment and renewal procedures such as the Enrollment over Secure Transport (EST). Nevertheless, the overhead of certificate management is still troublesome to the devices with limited resources (Keoh et al., 2014). Distributed ledger technology is a decentralized identity management

technology, where there are no central authorities. Smart contracts have the potential to automate the process of device registration, authentication, and revocation and keep tamper-evident records (Lin et al., 2019). Both Capability-Based Access Control (CapBAC) and Attribute-Based Access Control (ABAC) offer flexible access control policy to be adjusted to evolving IoT contexts. Policies are able to include device features, circumstances and instantaneous situations (Gusmeroli et al., 2013).

Network Security Mechanisms

IoT communications need to be adapted to typical network security controls in order to be secure. IoT-optimized security protocols such as DTLS, CoAP over DTLS, and MQTT with TLS offer encryption and authentication of limited networks. Protocol profiles need to attain the stability between security and overhead (Raza et al., 2015). SDN is a centralized control of the network, which permits dynamically implementing security policies and responding quickly to threats. SDN can isolate compromised devices, reroute traffic around attacks, and micro-segmentation in an IoT environment (Bizanis and Kuipers, 2016). A network-based Intrusion Detection System (IDS) displays network traffic (Zarpelão et al., 2017). Signature and anomaly based detection are used to detect recognized attacks and detection of deviation respectively. Machine learning improves the detection precision but should be tailored to IoT traffic characteristics (Zarpelão et al., 2017). Distributed ledger technology may be used in securing the operations of the IoT networks by decentralized trust. Routing protocols based on the blockchain are resistant to manipulation, and smart contracts achieve security responses in an automated manner (Khan & Salah, 2018).

Machine Learning and Artificial Intelligence

The concept of ML and AI has become the revolution in IoT security, allowing automated threat detection and scale reaction (Xiao et al., 2018; Bello et al., 2025). ML models are trained to understand the normal device and network behavior, and can perform an anomaly detection. Unsupervised learning detects new attacks without having to be trained on labeled attacks (Khan et al., 2019; Alangari, 2025). Autoencoders and recurrent neural networks are deep learning models that extract complex time-dependent patterns of IoT data streams (Chalapathy and Chawla, 2019). Federated ML learns using multiple devices without accessing sensitive information. Federated learning does not violate privacy and allows sharing of threat intelligence. Nevertheless, it also brings about new security threats such as model poisoning attacks (Bagdasaryan et al., 2020). ML-based security systems themselves have to be defended against adversarial examples inputs that are made to avoid detection. Adversarial training, input sanitization, and ensemble are some of the defensive techniques (Madry et al., 2017). Due to influence of ML systems in making security decisions, explainability becomes a must in the context of trust and accountability. Explainable AI methods aid security experts to comprehend the reasons why certain detections were made and confirm automated reaction (Arrieta et al., 2022; Li & Saxena, 2025).

Blockchain Technology

Blockchain offers decentralized trust that handles the security challenges in IoT such as data integrity, identity and secure transactions. With a Blockchain, it is possible to have a self-sovereign identity in which devices have control over their identifiers and credentials. Identity management removes the single points of failure in distributed ledger technology (Ali et al., 2017; Khan et al., 2025). Blockchain will give evidence of device actions, data provenance, and security transactions. The immutable logs facilitate compliance with regulations and analysis of the forensic nature (Maesa et al., 2019). Smart contract security policy that is embedded in smart contracts, represented as automated policies, controls access control, data sharing policies and security responses without having human involvement. Smart contracts should be created with a high level of care that remove vulnerabilities (Christidis & Devetsikiotis, 2016) (Figure 6).

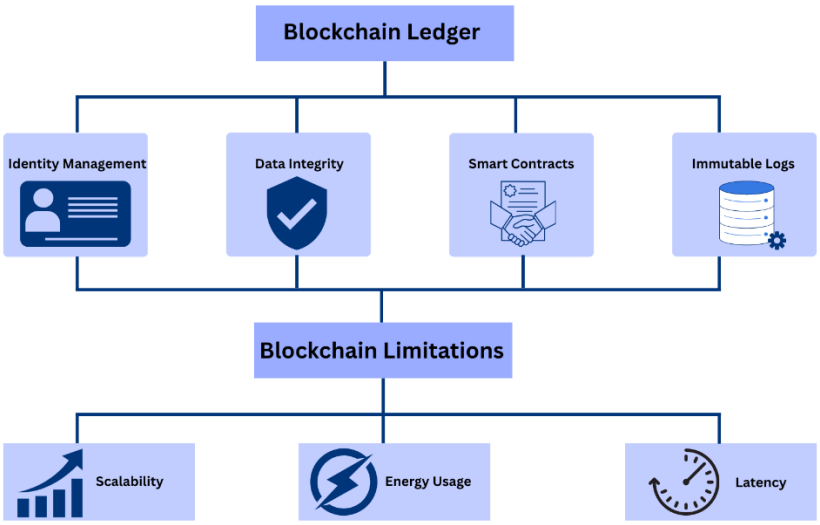

Figure 6. Blockchain technology application and limitation

Blockchain limitations includes scalability, energy usage, and latency are some of the major limitations of blockchain usage in resource-constrained IoT systems. Some of the limitations are resolved by hybrid solutions that involve on- and off-chain processing. Studies suggest that blockchain applications can lessen the number of unauthenticated access in a controlled deployment by up to 90% (Yli-Huumo et al., 2017) (Figure 6).

Edge and Fog Computing

The distributed computing architecture moves processing nearer to the IoT devices, responding to security threats swiftly (Shi et al., 2016). Edge nodes have the ability to scan immediate devices and network areas, identifying and reacting to hazards without being linked to the cloud. Edge analysis is also possible in real-time, allowing the fast containment of compromised devices. Edge gateways have firewall rules and access controls which defend downstream devices. Micro-isolation at the edge boundaries prevents sideways motion by attackers (Guan e al., 2018). Edge computing minimizes exposure to the cloud-based risks and facilitates privacy preservation laws. Minimization of data and local anonymization are done prior to transmission. Edge nodes can also be limited sources with a low security capacity and be targeted. The provision of the edge infrastructure must be designed and maintained closely (Hu et al., 2017).

Zero Trust Architecture

Zero Trust Architecture (ZTA) is an IoT security paradigm shift that no longer depends on the fights with the perimeter but performs consistent verification of every entity and transaction (Rose et al., 2020; Sadaf et al., 2025). ZTA does not give implicit trust depending on the location of the network or ownership of the device. All access requests should be authenticated, authorized and encrypted irrespective of the source. ZTA will constantly check the actions of devices, network traffic and user actions to identify signs of compromise. Abnormalities lead to the immediate loss of access or further validation (Rose et al., 2020; Zanasi et al., 2024). Network segmentation at fine details curtails the terrorist range of successful attacks. Hacked machines cannot be used to access resources that are not within their sections of authority. To achieve ZTA in IoT applications, it is necessary to use lightweight continuous authentication, behavioral profiling and automated policy enforcement. Policy control points the constrained devices commonly have

edge nodes where policy is enforced. Case studies show that ZTA can be used in healthcare, industrial IoT, and smart agriculture implementation (Nguyen et al., 2025).

Security Risk Assessment Frameworks

Systematic risk assessment helps organizations to make security investments priorities and to keep the levels of risk within acceptable parameters (Waqdan et al., 2025). The conventional risk assessment frameworks have to be adjusted to the IoT traits such as scale, heterogeneity, and the physical safety considerations. IoT frameworks have been extended to OCTAVE and FAIR (Alberts et al., 2003). Organization of taxonomies of IoT assets, threats, and vulnerabilities enable the identification of risks in a holistic way. The relationships between vulnerabilities, attack vectors, and potential impacts allow conducting a systematic analysis (Waqdan et al., 2025). Quantitative risk assessment tries to place monetary amounts on IoT risks to support cost-benefit analysis of security controls. Gordon-Loeb model has been used in the case of IoT investment decisions (Gordon et al., 2020). The nature of dynamic IoT environments necessitates constant re-evaluation of risks as new devices enter the environment as well as threats and vulnerabilities increase. Risk visibility is achieved by using automated assessment tools that are coupled with security monitoring (Høj et al., 2002) (Figure 7).

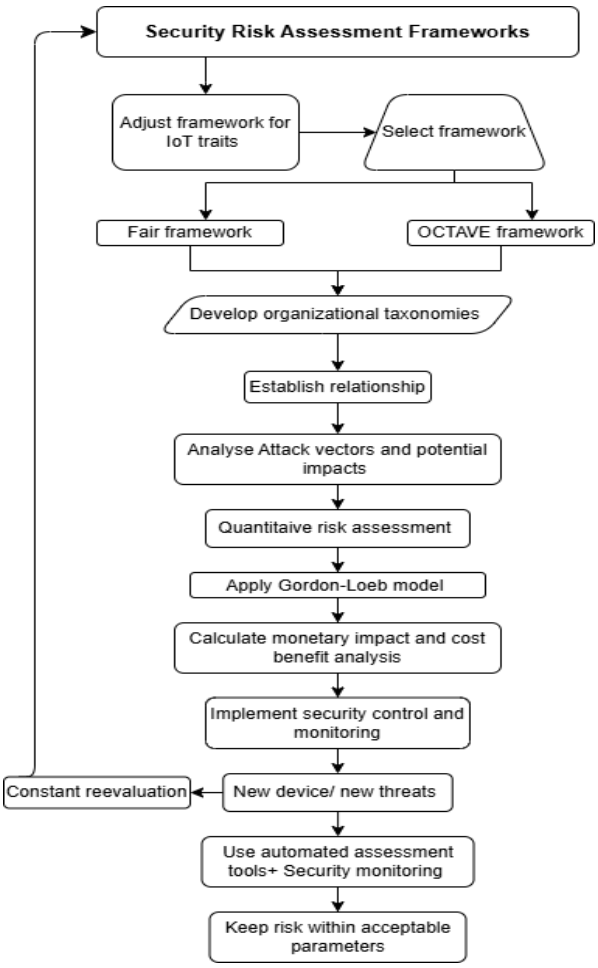

Figure 7. Flow chart of security risk assessment frameworks

Domain-Specific Applications of IoT

IoT security challenges and solutions manifest differently across application domains, each presenting unique requirements, constraints, and threat models (Figure 8).

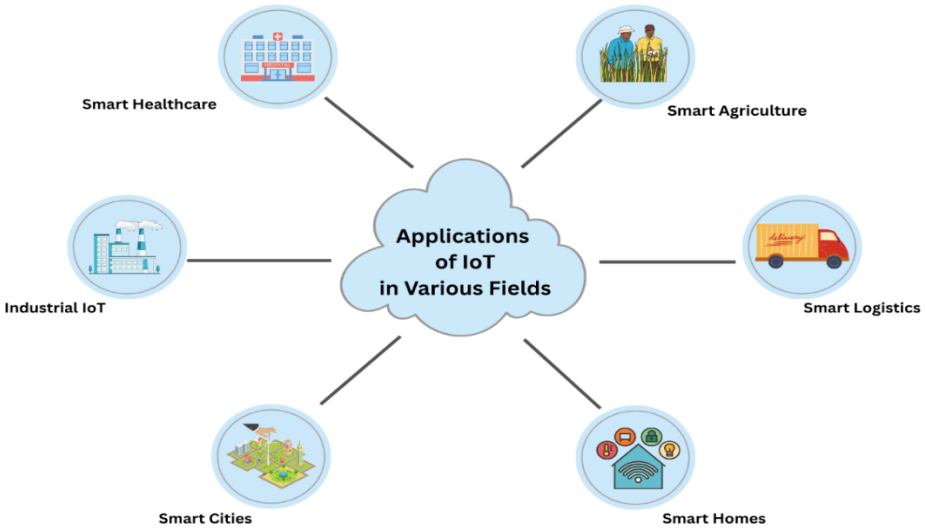

Figure 8. Applications of IoT in various fields

Smart Healthcare

Healthcare IoT (HIoT) encompasses medical devices, patient monitoring systems, and hospital infrastructure, where security failures can directly impact patient safety (Baker et al., 2017). Healthcare IoT prioritizes data confidentiality (protected health information), integrity (accurate medical data), and availability (continuous monitoring). Regulatory requirements including HIPAA and GDPR impose additional obligations. Medical devices often lack basic security features, run outdated software, and cannot be easily patched due to regulatory constraints. Wireless communication between sensors and monitoring stations may be unencrypted. The Verkada breach demonstrated how compromised cameras in healthcare settings expose patient privacy. Network segmentation isolates medical devices from general IT systems. Blockchain ensures tamper-evident storage of electronic health records (Baker et al., 2017).

Industrial IoT (IIoT)

Industrial IoT connects sensors, controllers, and actuators in manufacturing, energy, and critical infrastructure, where cyber-attacks can cause physical damage and safety incidents. IIoT prioritizes availability and integrity above confidentiality, as production processes cannot tolerate interruption. Safety systems must remain operational even during cyber-attacks. Legacy industrial control systems were designed for isolated networks and lack modern security features. Convergence with IT networks exposes industrial systems to general internet threats (Boyes et al., 2018). The Stuxnet attack demonstrated how sophisticated adversaries can compromise industrial systems to cause physical destruction. Deep packet inspection of industrial protocols identifies malicious commands. Anomaly detection learns normal process behavior and alerts on deviations. Zero Trust principles segment industrial networks and continuously verify device identities (Zolanvari et al., 2019).

Smart Cities

Smart city IoT integrates diverse systems including energy, transportation, waste management, water and public safety, creating complex interdependencies (Zanella et al., 2014). Smart city systems must maintain availability of critical services while protecting citizen privacy. Interconnected systems require coordinated security across municipal departments and private partners. Massive scale creates extensive attack surfaces. Heterogeneous systems with varying security postures create weak links (Zanella et al., 2014). Publicly accessible sensors and controllers invite physical tampering. Encryption protects sensitive

citizen data during transmission and storage. Privacy-preserving methods including differential privacy enable data analytics without exposing individual information. Blockchain supports secure identity management across city services (Andrade et al., 2022).

Smart Homes

Consumer IoT devices in homes present unique challenges due to limited user expertise, diverse device ownership, and privacy expectations. User privacy is paramount, with devices collecting intimate details of daily life. Usability is essential, as consumers cannot manage complex security configurations (Apthorpe et al., 2017). Default credentials, unpatched vulnerabilities, and insecure mobile apps are widespread. Voice assistants always listening create privacy concerns (Sivaraman et al., 2016). Compromised smart home devices have been used for surveillance and as botnet members. Router-level security can protect multiple devices simultaneously. Automated updates reduce the window of vulnerability. User education and transparent privacy practices build trust (Sivaraman et al., 2016).

Smart Logistics

IoT in logistics tracks goods through supply chains, monitoring location, condition, and handling. Integrity of tracking data prevents theft and diversion. Authentication ensures only authorized parties can modify shipment status. RFID tags used for tracking can be cloned or spoofed. GPS receivers are susceptible to jamming and spoofing (Lehtonen et al., 2007). Centralized tracking platforms create single points of failure. Blockchain provides tamper-evident supply chain records. Multi-factor authentication for shipment release prevents unauthorized access. Encryption protects sensitive shipment data (Humphreys, 2012).

Smart Agriculture

Agricultural IoT monitors soil conditions, crop health, livestock, and equipment, optimizing resource use and increasing yields (Elijah et al., 2018). Availability during critical planting and harvest seasons is essential. Location data and yield information have competitive value requiring protection (Elijah et al., 2018). Remote deployments with limited physical security invite tampering. Cellular and satellite communications may have limited bandwidth for security protocols. Farm management platforms in the cloud concentrate data from multiple operations. Lightweight protocols accommodate limited connectivity. Physical security measures protect field-deployed sensors. Data aggregation techniques minimize sensitive information exposure (Vasisht et al., 2017).

Challenges and Future Directions

Despite significant advances in IoT security, persistent challenges remain, and emerging technologies present both opportunities and new risks (Rachit & Ragiri, 2021).

Persistent Challenges

The fundamental limitation of constrained devices continues to restrict security options. Progress in lightweight cryptography addresses some concerns but cannot fully compensate for severe limitations. Energy-efficient security remains challenging for battery-powered devices expected to operate for years. Security solutions must accommodate devices ranging from simple sensors to powerful gateways while maintaining interoperability. Industry fragmentation slows the adoption of consistent security practices. IoT devices often remain in service for years or decades, outlasting their security support (Bakhshi et al., 2024). Update mechanisms are frequently inadequate, leaving devices vulnerable after discovery of flaws (Bettayeb et al., 2019). Secure decommissioning and data sanitization receive insufficient attention. Users routinely fail to change default credentials, apply updates, or recognize IoT security risks. Consumer IoT devices prioritize ease of use over security, often hiding configuration options that would enable

protection. Security indicators that effectively communicate risk to non-expert users remain elusive (Weber, 2010). Divergent security requirements across jurisdictions complicate compliance for global IoT deployments. The absence of harmonized standards forces manufacturers to navigate conflicting requirements. Regulatory enforcement lags behind technological change (Fagan et al., 2020).

Emerging Research Directions

The eventual arrival of quantum computers threatens current cryptographic algorithms. Developing and standardizing post-quantum cryptography appropriate for constrained IoT devices is urgent. NIST's ongoing standardization process will produce algorithms but implementation challenges remain (Bernstein, 2025).

Next-generation networks will enable new IoT capabilities while introducing novel security challenges. Network slicing isolation, distributed trust models, and AI-native security architectures require research attention. The massive scale and ultra-low latency of 6G will demand automated, predictive security (Ahmad et al., 2018).

As AI becomes central to IoT security, protecting AI systems from manipulation becomes critical. Adversarial examples, model poisoning, and inference attacks against ML models require robust defenses. Research on certified robustness and verifiable neural networks offers promising directions (Papernot et al., 2016).

Distributed ML across IoT devices introduces new attack surfaces. Secure aggregation protocols, differential privacy guarantees, and robustness to poisoning attacks require further development. Incentive mechanisms for device participation in federated learning need exploration (Blanchard et al., 2017).

Permissioned blockchains and layer-2 solutions address scalability concerns but introduce centralization risks. Research on lightweight consensus protocols suitable for IoT environments continues. Integration of blockchain with edge computing offers promising hybrid architectures (Yang et al., 2019).

The scale of IoT deployments demands automated security response. Security Orchestration, Automation, and Response (SOAR) platforms adapted for IoT can coordinate detection and response across distributed environments. Machine learning for automated incident classification and prioritization shows promise (Yang et al., 2019; Dwork et al., 2014).

Conclusion

The Internet of Things marks a transformative era where digital intelligence pervades the physical world, spanning healthcare, industry, cities, and homes. This integration brings immense opportunities but equally profound cybersecurity challenges, with over 30 billion devices expected by 2030. More than 70% of these devices may be vulnerable, transmitting over 40 zettabytes of data annually across an increasingly complex attack surface. Resource constraints, physical exposure, and long device lifecycles further compound the difficulty of securing IoT systems. Despite these risks, promising solutions are emerging AI enables scalable threat detection, blockchain ensures trust, and edge computing supports rapid response. Zero Trust Architecture offers a robust security model by continuously verifying all entities and transactions. Real-world attacks like Mirai and Verkada show that IoT failures have serious consequences, but successes across domains prove security is achievable. Effective protection relies on layered defenses, smart technology choices, and consistent risk management. Moving forward, progress depends on advancing lightweight cryptography, harmonized standards, smart regulation, and user education. The future of IoT and the safety of the systems society depends on hangs in the balance.

Funding: Funding is inappropriate for this research study.

Data availability: The statistics supporting the outcomes of this research are accessible upon reasonable request from the first author.

Declarations

Ethical approval: Not applicable

Consent to participate: Not applicable

Consent to publish: All authors have given consent to publish.

Competing interest: The authors have no competing interests to declare.

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2444095
2. Ashraf, Q. M., & Habaebi, M. H. (2015, April). Introducing autonomy in internet of things. In *14th International Conference on Applied Computer & Applied Computational Science*.
3. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., & Zhou, Y. (2017). Understanding the mirai botnet. In *26th USENIX Security Symposium (USENIX Security 17)*, 1093-1110.
4. Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In *2014 International Conference on Privacy & Security in Mobile Systems,* 1-8. https://doi.org/10.1109/PRISMS.2014.6970594
5. Alangari, S. (2025). An unsupervised machine learning algorithm for attack and anomaly detection in IoT sensors. *Wireless Personal Communications*, *144*(1-2), 1-25. https://doi.org/10.1007/s11277-023-10811-8
6. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network & Computer Applications*, *88*, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002
7. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, *54*(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010
8. Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In *2015 IEEE Symposium on Computers & Communication,* 180-187. https://doi.org/10.1109/ISCC.2015.7405513
9. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012
10. Ali, M. S., Dolui, K., & Antonelli, F. (2017, October). IoT data privacy via blockchains and IPFS. In *Proceedings of the Seventh International Conference on the Internet of Things*, 1-7. https://doi.org/10.1145/3131542.3131563
11. Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE approach. https://doi.org/10.21236/ADA634134
12. Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. (2020). A comprehensive study of the IoT cybersecurity in smart cities. *IEEE Access*, *8*, 228922-228941. https://doi.org/10.1109/ACCESS.2020.3046442

13. Apthorpe, N., Reisman, D., & Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805*. https://doi.org/10.48550/arXiv.1705.06805
14. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G security challenges and solutions. *IEEE Communications Standards Magazine*, *2*(1), 36-43. https://doi.org/10.1109/MCOMSTD.2018.1700063
15. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security & Applications*, *38*, 8-27. https://doi.org/10.1016/j.jisa.2017.11.002
16. Blanchard, P., El Mhamdi, E. M., Guerraoui, R., & Stainer, J. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent. *Advances in Neural Information Processing Systems*, *30*.
17. Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access*, *5*, 26521-26544. https://doi.org/10.1109/ACCESS.2017.2775180
18. Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A review of IoT firmware vulnerabilities and auditing techniques. *Sensors*, *24*(2), 708. https://doi.org/10.3390/s24020708
19. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1-12. https://doi.org/10.1016/j.compind.2018.04.015
20. Bettayeb, M., Nasir, Q., & Talib, M. A. (2019, March). Firmware update attacks and security for IoT devices: Survey. In *Proceedings of the ArabWIC 6th Annual International Conference Research Track*, 1-6. https://doi.org/10.1145/3333165.3333169
21. Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer*, *50*(2), 76-79. https://doi.org/ 10.1109/MC.2017.62
22. Bello, A. B., Ogundipe, A. O., George, A. A., & Anifowose, O. (2025). The role of AI and machine learning in cybersecurity: Advancements in threat detection, anomaly detection and automated response. International *Journal of Science and Research Archive, 14*(2), 1587-1597. https://doi.org/10.30574/ijsra.2025.14.2.0542
23. Biryukov, A., & Perrin, L. (2017). State of the art in lightweight symmetric cryptography. *Cryptology ePrint Archive*.
24. Bizanis, N., & Kuipers, F. A. (2016). SDN and virtualization solutions for the Internet of Things: A survey. *IEEE Access*, *4*, 5591-5606. https://doi.org/10.1109/ACCESS.2016.2607786
25. Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. *arXiv preprint arXiv:1501.02211*. https://doi.org/10.48550/arXiv.1501.02211
26. Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020, June). How to backdoor federated learning. In *International Conference on Artificial Intelligence & Statistics*, 2938-2948.
27. Bernstein, D. J. (2025). Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1846-1847). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-71522-9_386
28. Bandyopadhyay, S., Sengupta, M., Maiti, S., & Dutta, S. (2011). Role of middleware for internet of things: A study. *International Journal of Computer Science & Engineering Survey*, *2*(3), 94-105.
29. Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. *arXiv preprint arXiv:1901.03407*. https://doi.org/10.48550/arXiv.1901.03407
30. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, *4*, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

31. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, *78*, 544-546. https://doi.org/10.1016/j.future.2017.07.060
32. Chaqfeh, M. A., & Mohamed, N. (2012, May). Challenges in middleware solutions for the internet of things. In *2012 International Conference on Collaboration Technologies & Systems,* 21-26. https://doi.org/ 10.1109/CTS.2012.6261022
33. Chui, K. T., Gupta, B. B., Liu, J., Arya, V., Nedjah, N., Almomani, A., & Chaurasia, P. (2023). A survey of internet of things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions. *Information*, *14*(7), 388. https://doi.org/10.3390/info14070388
34. Christin, D. (2016). Privacy in mobile participatory sensing: Current trends and future challenges. *Journal of Systems & Software*, *116*, 57-68. https://doi.org/10.1016/j.jss.2015.03.067
35. Dritsas, E., & Trigka, M. (2025). A survey on cybersecurity in IoT. *Future Internet*, *17*(1), 30. https://doi.org/10.3390/fi17010030
36. Damghani, H., Damghani, L., Hosseinian, H., & Sharifi, R. (2019, November). Classification of attacks on IoT. In *4th International Conference on Combinatorics, Cryptography, Computer Science & Computation*, 245-255.
37. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations & Trends® in Theoretical Computer Science*, *9*(3-4), 211-487. https://doi.org/10.1561/0400000042
38. Da X, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, *10*(4), 2233-2243. https://doi.org/10.1109/TII.2014.2300753
39. Dao, T., Nguyen, M., Do, S., & Tran, H. (2026). Cyberscurity threats and defense mechanisms in IoT network. *arXiv preprint arXiv:2601.00556*. https://doi.org/10.48550/arXiv.2601.00556
40. Edwards, S., & Profetis, I. (2016). Hajime: Analysis of a decentralized internet worm for IoT devices. *Rapidity Networks*, *16*, 1-18.
41. Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of Things Journal*, *5*(5), 3758-3773. https://doi.org/ 10.1109/JIOT.2018.2844296
42. El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. *Sensors*, *19*(5), 1141. https://doi.org/10.3390/s19051141
43. Fagan, M., Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020, May). *IoT Device Cybersecurity Capability Core Baseline*. https://doi.org/10.6028/NIST.IR.8259A
44. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010
45. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa005
46. Görmüş, S., Aydın, H., & Ulutaş, G. (2018). Security for the internet of things: a survey of existing mechanisms, protocols and open research issues. *Journal of the Faculty of Engineering & Architecture of Gazi University*, *33*(4), 1247-1272. https://doi.org/10.17341/gazimmfd.416406
47. Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the internet of things. *Mathematical & Computer Modelling*, *58*(5-6), 1189-1205. https://doi.org/10.1016/j.mcm.2013.02.006
48. Guan, Y., Shao, J., Wei, G., & Xie, M. (2018). Data security and privacy in fog computing. *IEEE Network*, *32*(5), 106-111. https://doi.org/10.1109/MNET.2018.1700250
49. Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*. https://doi.org/10.48550/arXiv.1412.6572

50. Humphreys, T. (2012). Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing. *University of Texas at Austin (July 18, 2012)*, 1-16.
51. Herder, C., Yu, M. D., Koushanfar, F., & Devadas, S. (2014). Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, *102*(8), 1126-1141. https://doi.org/10.1109/JPROC.2014.2320516
52. Halfond, W. G., Viegas, J., & Orso, A. (2006). A classification of SQL injection attacks and countermeasures.
53. Høj, N. P., & Kröger, W. (2002). Risk analyses of transportation on road and railway from a European Perspective. *Safety Science*, *40*(1-4), 337-357. https://doi.org/10.1016/S0925-7535(01)00053-4
54. HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, 100129. https://doi.org/10.1016/j.iot.2019.100129
55. Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of Network & Computer Applications*, *98*, 27-42. https://doi.org/10.1016/j.jnca.2017.09.002
56. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501. https://doi.org/10.1007/s11276-014-0761-7
57. Khan, I. U., Khan, F. M., Haider, Z. A., & Alturise, F. (2025). Integrating AI, blockchain, and edge computing for zero-trust IoT security: A comprehensive review of advanced cybersecurity framework. *Computers, Materials & Continua*, *85*(3), 4307-4344. https://doi.org/10.32604/cmc.2025.070189
58. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411. https://doi.org/10.1016/j.future.2017.11.022
59. Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. *IEEE Internet of Things Journal*, *1*(3), 265-275. https://doi.org/10.1109/JIOT.2014.2323395
60. Khan, M. A. (2016). A survey of security issues for cloud computing. *Journal of Network & Computer Applications*, *71*, 11-29. https://doi.org/10.1016/j.jnca.2016.05.010
61. Karie, N. M., Sahri, N. M., & Haskell-Dowland, P. (2020, April). IoT threat detection advances, challenges and future directions. In *2020 Workshop on Emerging Technologies for Security in IoT,* 22-29. https://doi.org/10.1109/ETSecIoT50046.2020.00009
62. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80-84. https://doi.org/10.1109/MC.2017.201
63. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221. https://doi.org/10.1016/j.comnet.2018.03.012
64. Khan, F. A., Gumaei, A., Derhab, A., & Hussain, A. (2019). A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access*, *7*, 30373-30385. https://doi.org/10.1109/ACCESS.2019.2899721
65. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: the internet of things architecture, possible applications and key challenges. In *10th IEEE International Conference on Frontiers of Information Technology*, 257-260. https://doi.org/10.1109/FIT.2012.53
66. Khan, S., Ferreira Lopes martins, P. A., Sousa, B., & Pereira, V. (2025). A comprehensive review on lightweight cryptographic mechanisms for industrial internet of things systems. *ACM Computing Surveys, 58*(1), 1-37. https://doi.org/10.1145/3757734
67. Keele, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (Vol. 5). Technical report, ver. 2.3 ebse technical report. ebse.

68. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125-1142. https://doi.org/10.1109/JIOT.2017.2683200
69. Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., & Choo, K. K. R. (2019). HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal*, *7*(2), 818-829. https://doi.org/10.1109/JIOT.2019.2944400
70. Li, S., & Saxena, N. (2025). Explainable AI-based intrusion detection in IoT systems. *Internet of Things*, *31*, 101589. https://doi.org/10.1016/j.iot.2025.101589
71. Lehtonen, M. O., Michahelles, F., & Fleisch, E. (2007). Trust and security in RFID-based product authentication systems. *IEEE Systems Journal*, *1*(2), 129-144. https://doi.org/10.1109/JSYST.2007.909820
72. Mayzaud, A., Badonnel, R., & Chrisment, I. (2016). A Taxonomy of attacks in RPL-based internet of things. *International Journal of Network Security*, *18*(3), 459-473. https://doi.org/10.6633/IJNS.201605.18(3).07
73. Matheu, S. N., Hernandez-Ramos, J. L., & Skarmeta, A. F. (2019). Toward a cybersecurity certification framework for the Internet of Things. *IEEE Security & Privacy*, *17*(3), 66-76. https://doi.org/10.1109/MSEC.2019.2904475
74. Madry, A., Makelov, A., Schmidt, L., Tsipras, D., & Vladu, A. (2017). Towards deep learning models resistant to adversarial attacks. *arXiv preprint arXiv:1706.06083*. https://doi.org/10.48550/arXiv.1706.06083
75. Maesa, D. D. F., Mori, P., & Ricci, L. (2019). A blockchain based approach for the definition of auditable access control systems. *Computers & Security*, *84*, 93-119. https://doi.org/10.1016/j.cose.2019.03.016
76. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497-1516. https://doi.org/10.1016/j.adhoc.2012.02.016
77. Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2012). Identity authentication and capability based access control (iacac) for the internet of things. *Journal of Cyber Security & Mobility*, *1*(4), 309-348.
78. McKay, K., Bassham, L., Sönmez Turan, M., & Mouha, N. (2016). *Report on lightweight cryptography* (No. NIST Internal or Interagency Report (NISTIR) 8114 (Draft)). National Institute of Standards and Technology.
79. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, *21*(3), 2702-2733. https://doi.org/10.1109/COMST.2019.2910750
80. Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security requirements for the internet of things: A systematic approach. *Sensors*, *20*(20), 5897. https://doi.org/10.3390/s20205897
81. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials*, *16*(1), 414-454. https://doi.org/10.1109/SURV.2013.042313.00197
82. Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The quest for privacy in the internet of things. *IEEE Cloud Computing*, *3*(2), 36-45. https://doi.org/10.1109/MCC.2016.28
83. Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z. B., & Swami, A. (2016, March). The limitations of deep learning in adversarial settings. In *2016 IEEE European Symposium on Security & Privacy,* 372-387. https://doi.org/10.1109/EuroSP.2016.36

84. Rachit, Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. *SN Applied Sciences*, *3*(1), 121. https://doi.org/10.1007/s42452-021-04156-9
85. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST Special Publication*, *800*(207), 1-52. https://doi.org/10.6028/NIST.SP.800-207
86. Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the internet of things. *IEEE Sensors Journal*, *13*(10), 3711-3720. https://doi.org/10.1109/JSEN.2013.2277656
87. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018
88. Rostami, M., Koushanfar, F., & Karri, R. (2014). A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, *102*(8), 1283-1295. https://doi.org/10.1109/JPROC.2014.2335155
89. Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer & Information Sciences*, *30*(3), 291-319. https://doi.org/10.1016/j.jksuci.2016.10.003
90. Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. *International Journal of Advanced Computer Science & Applications*, *8*(6), 383.
91. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications & Networks*, *4*(2), 118-137. https://doi.org/10.1016/j.dcan.2017.04.003
92. Sabt, M., Achemlal, M., & Bouabdallah, A. (2015, August). Trusted execution environment: What it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/Ispa*, 1, 57-64. https://doi.org/10.1109/Trustcom.2015.357
93. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, *3*(5), 637-646. https://doi.org/10.1109/JIOT.2016.2579198
94. Sivaraman, V., Chan, D., Earl, D., & Boreli, R. (2016, July). Smart-phones attacking smart-homes. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless & Mobile Networks*, 195-200. https://doi.org/10.1145/2939918.2939925
95. Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *2012 International Conference on Computer Science & Electronics Engineering*, 3, 648-651. https://doi.org/10.1109/ICCSEE.2012.373
96. Sadaf, M., Muhammad, M., & Mujahid, M. M. (2025). A systematic literature review on the implementation and challenges of zero trust architecture across domains. *Sensors*, *25*(19), 6118. https://doi.org/10.3390/s25196118
97. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008
98. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039
99. Tehranipoor, M., & Koushanfar, F. (2010). A survey of hardware trojan taxonomy and detection. *IEEE Design & Test of Computers*, *27*(1), 10-25. https://doi.org/10.1109/MDT.2010.7
100. Vasisht, D., Kapetanovic, Z., Won, J., Jin, X., Chandra, R., Sinha, S., & Stratman, S. (2017). {FarmBeats}: an {IoT} platform for {Data-Driven} agriculture. In *14th USENIX Symposium on Networked Systems Design & Implementation,* 515-529.
101. Wang, J., Lim, M. K., Wang, C., & Tseng, M. L. (2021). The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering*, *155*, 107174. https://doi.org/10.1016/j.cie.2021.107174

102. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory & Engineering,* 5, 484. https://doi.org/10.1109/ICACTE.2010.5579493
103. Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261-274. https://doi.org/10.1007/s10796-014-9489-2
104. Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008
105. Wang, C., Wang, D., Tu, Y., Xu, G., & Wang, H. (2020). Understanding node capture attacks in user authentication schemes for wireless sensor networks. *IEEE Transactions on Dependable & Secure Computing*, *19*(1), 507-523. https://doi.org/10.1109/TDSC.2020.2974220
106. Wallgren, L., Raza, S., & Voigt, T. (2013). Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks*, *9*(8), 794326. https://doi.org/10.1155/2013/794326
107. Waqdan, M., Louafi, H., & Mouhoub, M. (2025). Security risk assessment in IoT environments: A taxonomy and survey. *Computers & Security*, *154*, 104456. https://doi.org/10.1016/j.cose.2025.104456
108. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. *IEEE Signal Processing Magazine*, *35*(5), 41-49. https://doi.org/10.1109/MSP.2018.2825478
109. Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE Wireless Communications*, *24*(3), 10-16. https://doi.org/10.1109/MWC.2017.1600421
110. Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019). Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(2), 1508-1532. https://doi.org/10.1109/COMST.2019.2894727
111. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250-1258. https://doi.org/10.1109/JIOT.2017.2694844
112. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS One*, *11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477
113. Yassein, M. B., Aljawarneh, S., & Masa'deh, E. A. (2017). A new elastic trickle timer algorithm for Internet of Things. *Journal of Network & Computer Applications*, *89*, 38-47. https://doi.org/10.1016/j.jnca.2017.01.024
114. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network & Computer Applications*, *42*, 120-134. https://doi.org/10.1016/j.jnca.2014.01.014
115. Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, *1*(5), 372-383. https://doi.org/10.1109/JIOT.2014.2344013
116. Zahra, A., & Shah, M. A. (2017, September). IoT based ransomware growth rate evaluation and detection using command and control blacklisting. In *2017 23rd International Conference on Automation & Computing,* 1-6. https://doi.org/10.23919/IConAC.2017.8082013
117. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & De Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network & Computer Applications*, *84*, 25-37. https://doi.org/10.1016/j.jnca.2017.02.009
118. Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., & Jain, R. (2019). Machine learning-based network vulnerability analysis of industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(4), 6822-6834. https://doi.org/10.1109/JIOT.2019.2912022

119. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, *1*(1), 22-32. https://doi.org/10.1109/JIOT.2014.2306328
120. Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security & Communication Networks*, *7*(12), 2728-2742. https://doi.org/10.1002/sec.795
121. Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine*, *55*(1), 26-33. https://doi.org/10.1109/MCOM.2017.1600363CM
122. Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, *156*, 103414. https://doi.org/10.1016/j.adhoc.2024.103414