


## Research Article

# An Extensive Examination on IOT and Industrial IOT: Attacks, Security, Detection Methods, Blockchain Solutions and Challenges

Karthik Kumar Vaigandla<sup>1,\*</sup>, <sup>1</sup> *Electronics and Communications Engineering, Balaji Institute of Technology and Science, Telangana, India.***ARTICLE INFO**

## Article History

Received 05 Jan 2025

Revised 29 Jan 2025

Accepted 20 Feb 2025

Published 10 Mar 2025

## Keywords

Attacks

Blockchain

Challenges

Internet of Things (IoT)

Industrial IoT

Privacy

Security

**ABSTRACT**

The Internet of Things (IoT) has consistently expanded in both the quantity of devices implemented and the variety of applications in which these devices are used. They exhibit significant variations in terms of their dimensions, processing capabilities, storage capacity, and energy consumption. The IoT has facilitated the ongoing digitization of society in several ways during the last decade. The IoT is an extensive network of interconnected smart gadgets that exchange data via web channels. The security aspect of IoT is of utmost importance due to its fast proliferation as a new technological paradigm, since it may include safety-critical operations and the digital storage of confidential information. Regrettably, the foremost obstacle that arises when using IoT technology is security. Consequently, enhancing the security of IoT devices is now the primary focus for manufacturers and researchers. There is a significant amount of literature that covers various challenges related to the topic and offers viable solutions. However, the majority of current research lacks a comprehensive viewpoint on assaults inside the IoT. Therefore, the purpose of this survey is to create a framework that will assist researchers in classifying attacks in a taxonomy based on different factors, including attack domains, threat types, execution methods, software surfaces, IoT protocols, device properties, adversary locations, and levels of information damage caused by the attacks.

**1. INTRODUCTION**

The IoT spans several application fields such as home automation, healthcare, manufacturing and supply chain management, agriculture, transportation, and municipal infrastructure. Physical equipment in various sectors are seeing a growing trend of interconnectivity with each other and the Internet [1]. The devices comprise an extensive array of technologies, which include connected cars, wearables, health-related devices such as pacemakers and glucose monitoring systems, industrial devices including RFID tags and manufacturing sensor networks, agricultural devices including greenhouse sensors and irrigation controllers, and city services including street lighting and water distribution systems [2]. An extensive range of technologies are integrated within these devices. The aforementioned items comprise smart door locks, thermostats, appliances, connected vehicles, wearable technology, glucose monitoring systems, pacemakers, RFID markers for supply chain management, manufacturing sensor networks, and irrigation controllers. Furthermore, city services and agricultural devices coexist. Examples of such devices include irrigation controllers and greenhouse sensors, while city services encompass water distribution systems and street illumination.

In the last ten years, the IoT has become very popular due to the availability of affordable and powerful devices such as sensors and RFIDs, as well as many connection methods. The IoT refers to a network of networked items, both stationary and mobile, that are equipped with communication, sensors, and actuator modules that are connected via the Internet. The IoT is expanding its scope as the quantity of interconnected devices extends to urban areas, facilitating the development of more intelligent systems [3]. These systems are created by combining our everyday things with small, clever gadgets to generate a completely automated and intelligent system that may decrease the need for human effort. For instance, many domestic appliances and technological gadgets may be interconnected on a network, enhancing the quality of human life by providing more intelligence and convenience. Ericsson's research predicts that the quantity of interconnected IoT devices will reach around 20 billion by 2023.

\*Corresponding author. Email: [vkvaigandla@gmail.com](mailto:vkvaigandla@gmail.com)

The IoT is a network of intelligent assets that are strategically placed in different areas. It is distinguished by its openness and inclusiveness. Specifically, it may use various sensing devices to achieve the immediate collection of a wide variety of monitored, networked, interacting entities and the accompanying essential data [4]. Thus, these devices integrate with the Internet to create a vast network. Moreover, the IoT has the capability to independently organize and distribute information resources based on environmental conditions. The gadgets are used for various tasks in a public network, improving user's ability to reach each device. However, a notable disadvantage of the IoT is its deficiency in security protocols that are equivalent to those found on servers, personal computers (PCs), and laptops. Many embedded devices may not have the processing capacity to effectively apply complex security rules and encryption algorithms [5]. Efforts have been undertaken in recent years to solve security vulnerabilities in the IoT paradigm. IoT security strategies may be categorized into two types: those that target specific layers to solve security problems, and those that aim to provide overall end-to-end security for IoT systems [6].

The IoT offers several advantages to people, organizations, and municipalities alike. Accessible and affordable devices that enhance convenience in domestic settings are readily accessible, while distant sensors may effectively monitor hard-to-reach regions [7]. Smart city IoT technology enables communities to monitor energy use and environmental conditions [8]. Medical IoT devices have the potential to enhance patient outcomes and minimize human mistakes in both hospital settings and distant care monitoring [9]. The widespread use of IoT devices across several fields has garnered attention from investors, businesses, and academics [10]. Threats present in specific layers of a security architecture framework may render those layers susceptible to attack. The physical, network, and application layers will be the subject of the security analysis presented in this article. Due to their inadequate security measures and resource constraints, physical layer IoT devices are susceptible to various forms of attacks, including physical destruction, manipulation, and forgery. The Network layer provides substantial support for data transmission between Internet of Things devices and application-layer processes. The availability of network services may be compromised by Denial of Service (DoS) attacks, which pose a danger to the network. Furthermore, security concerns are further amplified by weaknesses in wireless protocols. The Application layer, responsible for processing data from IoT devices and offering intelligent features to users, is susceptible to software flaws, gaps in application protocols, and permissions vulnerabilities [11-12].

## **2. INTERNET OF THINGS (IOT) OVERVIEW**

### **2.1. IoT**

The motivation to gather and acquire data, facilitate the transmission and dissemination of information effortlessly, from a distance, at all times, and without interruption, contributes to the advancement of the IoT. The IoT refers to a network of interconnected items or devices that are equipped with sensors to gather and transmit data. Currently, there is an abundance of networked devices that lack a standardized network or clearly defined limits. While IoT has great potential for many advantageous applications, there are significant issues regarding its security. These concerns mostly revolve on the absence of privacy, inadequate user authentication and authorization, and insufficient or non-existent data encryption [13-14]. In light of the emergence of IoT, it is crucial to promptly establish and adopt security standards to guarantee the safe design, connection, and accessibility of IoT devices. The IoT is poised to become the next major technological advancement in our digital era, following the successful integration of social networks in linking individuals [15]. The IoT will facilitate the interconnection of individuals and their surrounding gadgets, as well as the networking of interconnected objects.

The advantages of the IoT on our everyday activities are clear and obvious. However, during the first adoption of the IoT in the late 1960s [16], the significance of security concerns was not completely understood, and as a result, security was not prioritized in the design process. Currently, ensuring security is of utmost importance for the survival and widespread acceptance of IoT. The use of IoT apps and devices is becoming increasingly prevalent in every part of our everyday life. IoT, which encompasses Wireless Sensor Network (WSN) and Wireless Body Area Network (WBAN), has become a crucial element in various healthcare settings [17-20]. IoT devices have expanded into our living spaces in the home environment, allowing for home automation and the creation of intelligent, highly interconnected houses. Nowadays, household gadgets such as power outlets, light bulbs, thermostats, and others come with built-in networking capabilities, enabling wireless remote control. Almost any household appliance may be substituted with an automated and remotely operable equivalent. Figure 1 illustrates the pervasive presence of IoT devices and applications in several domains such as homes, automobiles, trains, streets, transportation, agriculture, and companies.

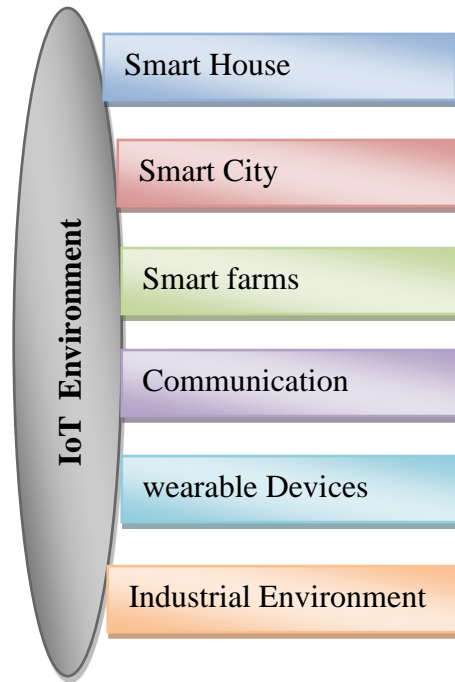


Fig. 1. IoT Environments

## 2.2 Security Attacks in IoT

The security attacks in the IoT may be categorized into four primary categories, as shown in Figure 2. This section provides a comprehensive analysis of these attacks, along by a thorough examination of the countermeasures implemented to address each of these attacks.

### 2.2.1 Physical Attacks

Physical assaults against the devices comprising a network or system are possible when an assailant is in close proximity to the apparatus [21]. The following are prevalent indicators of physical assaults: Physically modifying a communication connection or device is referred to as interference [22]. Malevolent code could be implanted through a physical device by an adversary, who could then utilize it to execute additional assaults. The term for this method is malicious code injection. Denial-of-service (DoS) attacks against RFID tags or sensor nodes can be carried out by an adversary through the generation and dissemination of disruptive signals using WSN or radio frequency (RF) signals. By installing a false node into the network, an adversary can manipulate the data transfer between two authentic nodes. The term for this method is "fake node injection." A slumber denial attack attempts to maintain the wakefulness of battery-powered machines by inputting erroneous data. As a result, their batteries deplete and they cease operation. In a side channel assault, the assailant extracts the encryption keys through the use of techniques such as power analysis, timing analysis, and hardware malfunction assaults. These keys allow it to encrypt and decrypt sensitive information. Permanent Denial of Service (PDoS) is a type of DoS attack in which the hardware of an IoT device is intentionally destroyed. It is possible for malicious software to corrupt the BIOS or delete the firmware, initiating the assault.

### 2.2.2 Network Attacks

With the intention of causing damage, network attacks utilize IoT network technology. It is possible to initiate the launch process even when not connected to the network. Following this, an examination of the most prevalent forms of network intrusions will ensue. An adversary can still obtain network information without physically penetrating the network by employing a traffic analysis attack, which consists of collecting sensitive information or other data travelling between devices. The intruder must first imitate an RFID signal in order to access the data contained on an RFID tag. By utilizing the authentic tag ID, the intruder can surreptitiously distribute its data. Inadequate authentication protocols permit unauthorized access to RFID by enabling an adversary to read, modify, or delete data stored on RFID nodes. Routing information attacks encompass direct assaults that manipulate or impersonate routing information with the intention of inducing disruption through means such as the generation of error messages or the establishment of cycles. Malicious nodes capable of selectively forwarding, modifying, or discarding messages have the potential to cause network

disruptions. As a result, the information gathered at the ultimate location lacks comprehensiveness. A sinkhole node refers to a compromised node that is deliberately positioned in close proximity to a sink. The objective of this attack is to induce other nodes within the network to route traffic towards the compromised node. A wormhole assault is initiated by an assailant who deliberately establishes a low-latency connection for the purpose of tunnelling communications between two distinct locations. A Sybil Attack involves the propagation of a single malicious node across a network by assuming the identities of multiple Sybil nodes. As a consequence, there is a notable disparity in the allocation of resources. A Man in the Middle (MiTM) attack could grant an assailant access to confidential information through the observation or recording of the transmission between two IoT devices. In replay attack an attacker is able to send a signed packet numerous times to the intended recipient. This keeps the network busy, resulting in a DoS attack. In contrast to DoS attacks, DDoS attacks occur when numerous hacked nodes flood a given target with information or requests for connections, causing the system server or network connection to fall down or completely fail.

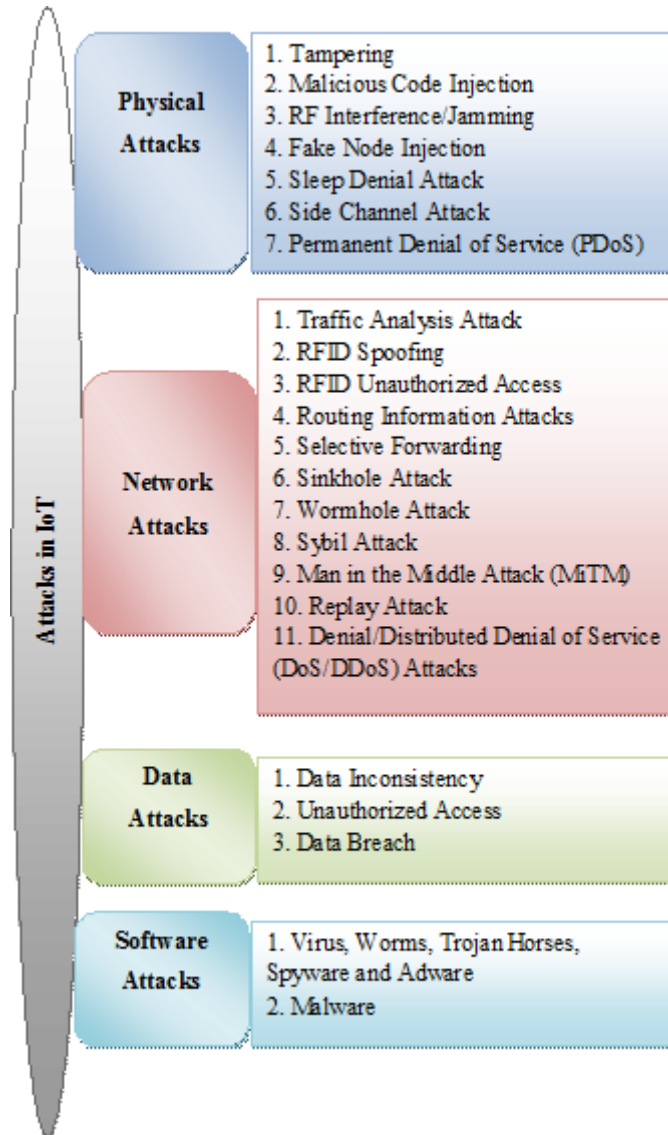


Fig. 2. Attacks in IoT

### 2.2.3 Software Attacks

An attacker can conduct software assaults on an IoT system by exploiting software or security flaws, which include the following:

- Virus, Worms, Trojan Horses, Spyware and Adware : Malicious software can infect systems, allowing adversaries to tamper with data, steal data, or conduct a DoS attack.
- Malware : Malware may infect data on IoT devices, contaminating cloud services or data centre networks.

#### 2.2.4 Data Attacks

The increasing use of IoT in factories is putting a demand on computer resources to support connectivity and data collecting. Cloud computing serves as the foundation for IoT's capabilities. Cloud computing simplifies the process of deploying virtual servers, databases, and data pipelines for IoT systems. Cloud technology can enhance data security through authentication processes, firmware and software updates, and other measures. This article covers the most common data threats in the IoT realm.

- Data Inconsistency : Data Inconsistency in IoT refers to an assault on data integrity that results in inaccuracy of data in transmission or information preserved in a centralized database.
- Unauthorized Access : Access control entails providing access to authorized users while limiting access to unauthorized ones. Malicious individuals can obtain data ownership or access critical information through unauthorized access.
- Data Breach : A data breach, also known as memory leakage, is the unauthorized revelation of individual, highly sensitive, or confidential information.

### 3. INDUSTRIAL INTERNET OF THINGS (IIOT)

Despite the arrival of the current industrial revolution (known as Industry 4.0), IIoT refers to the application of specialized IoT technologies and smart devices in an industrial setting to achieve industry-specific goals. Without human intervention, the IIoT system can watch, collect, analyze, and intelligently adjust behaviour or the environment. For almost two decades, industries have deployed Supervisory Control and Data Acquisition (SCADA) software and hardware. SCADA systems are made up of two parts: (a) the controlled or monitored process/machinery, and (b) a network of intelligent devices that control it. However, IIoT has evolved as a system constructed on top of SCADA, mostly due to the four areas listed below for improvement:

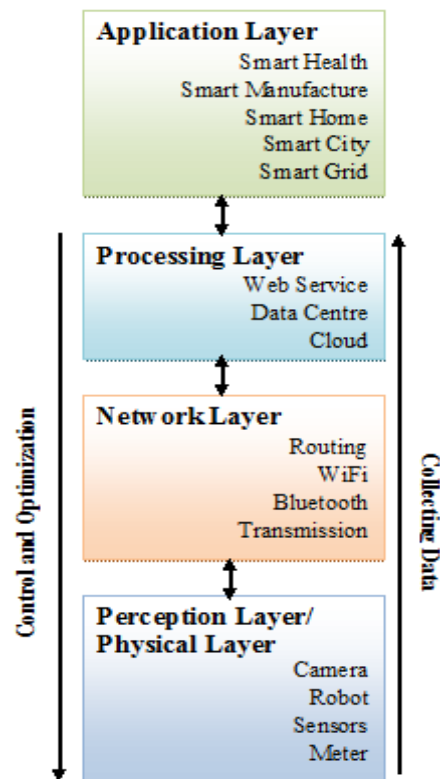


Fig. 3. Generalized IoT/ IIoT System Architecture

- Scalability: IIoT technology has the capacity to establish supplementary facilities by using cloud resources as required.
- Data Analytics: The IIoT requires the capability to store data for an extended duration. Substantial data processing and use of machine learning techniques may thereafter be employed to predict outcomes.
- Standardization: The goal of IIoT is to provide uniformity in sensor networks, data collecting, and consolidation in order to facilitate immediate and seamless communication inside industrial facilities.
- Interoperability: IIoT utilizes protocols like as MQTT to provide platforms that can be accessed and adapted on devices from many vendors.

#### 4. BLOCKCHAIN IN IOT AND IIOT

The exponential growth of the IIoT and the IoT has presented a formidable challenge in meeting Quality-of-Service (QoS) standards, due to the immense number of interconnected devices and data generated. In this context, Blockchain is advantageous due to the fact that it facilitates decentralized data storage and secure, anonymous transactions. Exciting is the possibility that blockchain technology could be utilized to oversee and control a network of billions of interconnected devices. It may also facilitate transaction processing, which could result in enormous cost savings for IoT industry manufacturers. By eradicating singular points of failure using this decentralized approach, a more resilient operating environment for devices would be established. Using the encryption algorithms of blockchain could provide a higher level of security for the personal information of customers [23-24]. A blockchain is a verifiable, decentralized, and immutable ledger system. Establishing a blockchain requires only a compilation of interconnected transactions contained within a solitary block. Subsequently, these blocks are interconnected such that any modifications made to a transaction in one block are automatically reflected in all subsequent blocks. Editing a transaction becomes a challenging task when multiple partners are utilizing the identical ledger. Acceptance or confirmation of a transaction by all peers on the blockchain is a prerequisite for its inclusion in a block. The block is subsequently appended to the Blockchain subsequent to its validation. This consensus can be attained through the implementation of consensus algorithms such as PoW, PoS, DPoS, PoA, and numerous others. Industry-wide, blockchain technology is exerting a significant influence that extends beyond the IoT setting. Scholars have recently focused on the integration of blockchain technology into the IoT ecosystem with the intention of providing it with distributed structure and security functionalities. In spite of this, prior to discussing how it is bringing about a substantial paradigm shift in the IoT, it is prudent to investigate a few of the chief attributes of blockchain. In order to facilitate direct transactions between two nodes, the decentralized character of blockchain technology precludes the need for an intermediary. Through this action, fault tolerance can be improved and the obstruction resulting from a singular point of failure can be eliminated. Decentralized consensus was employed by nodes to reach a unanimous agreement on all newly added entries to the blockchain. Every modification made to an entry in a block must be reflected in all subsequent blocks in all peers, by design. This ensures that alterations to blockchains are not possible. Through allowing peers to verify and authenticate any transaction, the auditability feature of blockchains fosters transparency. Each blockchain node maintains an immutable replica of each entry in the ledger. As a result, blockchain technology offers defect tolerance. This characteristic enhances both data confidentiality and network robustness.

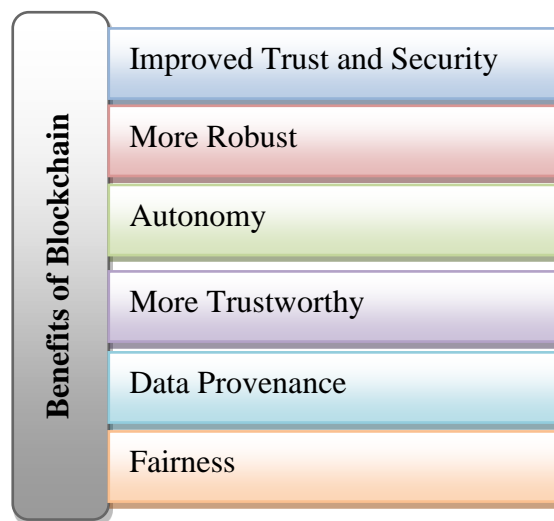


Fig. 4. Benefits



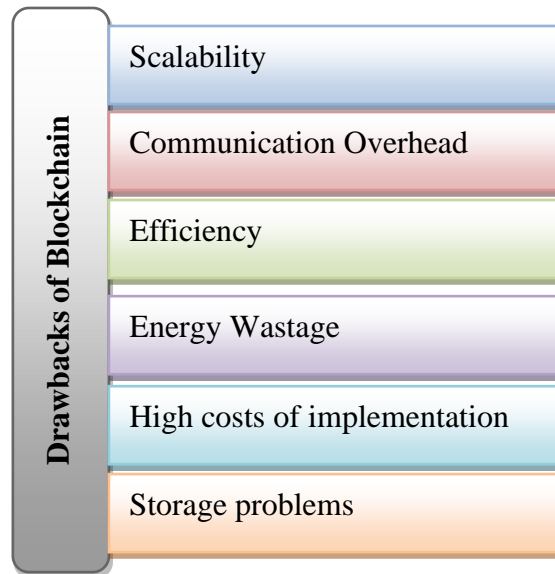


Fig. 5. Drawbacks

#### 4.1. Blockchain Solutions for IoT

Capitalizing on the advantages of integrating blockchain with IoT, researchers investigated ways to address critical issues including security of IoT devices, processing large amounts of data, protecting user privacy, and guaranteeing trust, secrecy, and integrity, among many others. Consequently, we will examine many significant studies that have dealt with the challenges outlined above and offered solutions based on blockchain technology in [25-28]. A blockchain connected gateway for IoT devices supported by Bluetooth Low Energy (BLE) that safeguards and adjusts user privacy settings was created by the authors [25]. The gateway ensures that sensitive user data cannot be accessed without the user's consent, therefore protecting their privacy. To further facilitate authentication and provide strong privacy protection, a digital signature mechanism based on bilinear pairing is also included. By encrypting and storing user preferences on the network, the blockchain network addresses privacy issues between IoT application providers and their customers. Another study [26] offered the idea of a Blockchain of Things (BoT) to address problems with hacking into IoT devices. By using colour spectrum chain blockchain technology, their suggested approach tackles security issues in sensor multi-platforms. This approach assesses Thin Plate Spline's (TPS) security features using a multiple-agreement methodology. In addition, the authors of the study [27] suggested and executed a system for automated door locking that used blockchain technology and mobile fingerprint verification. The blockchain technology that supports biometric authentication ensures that the system is secure by prohibiting unauthorized parties from tampering with, stealing, or otherwise compromising the user's fingerprint data. Nevertheless, as shown in the paper [28] proof of work and agreement would be very challenging for mobile devices with limited resources to accomplish because of the substantial resource requirements. It follows that they provide a model for edge computing where mobile devices execute complicated proof-of-work procedures using their capabilities. In order to address the demands of citizens, patients, healthcare providers, policymakers, and medical informatics experts, e-healthcare is expanding into new areas of focus [29-30]. Due to its ability to streamline the transfer of important data, blockchain technology is revolutionizing the healthcare industry. Electronic medical records may be accessed more swiftly, safely, and simply by important parties like as patients, physicians, clinical researchers, and chemists [31]. The Vehicular Ad-Hoc Network (VANET) is used by [32] to describe a system of wireless communication that allows vehicles with radio interfaces to share information and facilitate safe and efficient transportation. As a means of managing event alerts, ensuring the integrity of nodes, and safely and precisely transporting data, VANET networks are using blockchain technology.

#### 4.2. Blockchain Solutions for IIoT

Combining blockchain technology with IIoT systems has shown to be quite advantageous. It has significantly contributed to the continued strengthening of industrial systems by providing benefits such as safe data exchange, secure data aggregation, data secrecy, and so on. As a result, we will begin by reviewing a few important publications [33-35] that have successfully addressed these problems. Untrustworthy or malevolent service providers, as well as dishonest clients, may purposefully reject service offerings in order to profit themselves. In order to avoid harmful repudiation, by employing a blockchain-based non-repudiation network, [33] present a computational strategy for IIoT scenarios.

Blockchain may serve as a surrogate for publishing services and a repository of evidence with this information; the required service programme is divided into two non-executable components. Each of these components is transmitted via its own on-chain and off-chain channels, accompanied by the appropriate proof submissions, in order to guarantee non-repudiation. BSeIn for Industry 4.0, which [34] presented, also employs blockchain technology to ensure secure remote mutual authentication and precise access control. In order to ensure the secure authentication of end user terminals, the proposed methodology employs attribute signatures and blockchain technology. In order to verify gateways, Message Authentication Codes (MACs) are implemented. In order to enhance the level of privacy assurance for authorized users, BSeIn implements a multi-receiver encryption method [36]. Scalability and demand management are accomplished through the implementation of smart contracts.

## 5. IOT ATTACKS DETECTION METHODS

Identifying and mitigating threats is crucial for the security of IoT networks. Various methods to identify attacks have been developed to address these difficulties. The following strategies are used to identify attacks in the IoT domain.

### 5.1 Anomaly Detection

A singular data point that deviates from the anticipated behaviour of a simulated system constitutes an anomaly. Anomalies refer to rare incidents or observations that exhibit substantial deviation from established norms or patterns, whether they occur within a particular data point, contextual environment, time interval, or across the entire dataset. The majority of anomalies are brought about by external factors, including sensor failure or external attack. The principal objective of a detection algorithm is to identify an anomaly and its corresponding categories, or to ascertain its root cause [37]. Anomaly identification, which is also referred to as event detection or outlier identification, is the process of analyzing data to identify unusual occurrences within a system. Algorithms for anomaly detection oversee incoming traffic across multiple tiers, ranging from the IoT network to the data centre. Anomaly detection is critical for identifying and analyzing abnormalities in IoT data. These abnormalities, while uncommon, can give useful insights and actionable information in a variety of areas, including healthcare, manufacturing, finance, transportation, and energy. The betting and gaming business uses anomaly detection in the IoT to identify cases of insider trading by analyzing trade activity trends.

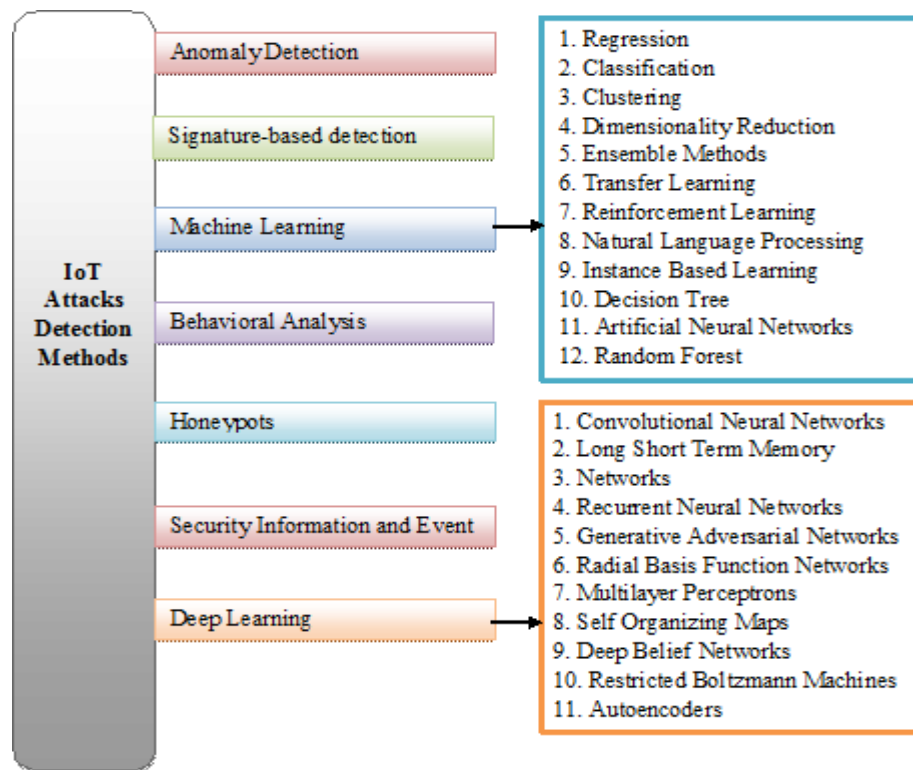


Fig. 6. IoT Attack Detection Methods



## 5.2 Signature-based detection (SGD)

SGD requires security experts to create established rules or signatures in advance to recognize known attack patterns. This method is very useful at identifying known assaults with signatures already in the database. Without signatures, the database cannot identify unknown assaults. The SGD algorithm outperforms other approaches in terms of computing efficiency. However, it has limitations in terms of properly detecting and classifying novel attack types that have not previously been experienced or included in its training data. Signature-based methods possess a notable advantage over anomaly-based approaches due to their intrinsic simplicity and ability to function in real-time online environments. Abuse detection is another name for signature-based detection. Abuse detection is a method that examines network activity in order to identify established threats; it frequently employs string-searching algorithms [38]. Signature detection is an algorithm that employs a set of predetermined criteria. The system compares observed occurrences with these criteria, which may include identified patterns of detrimental instructions utilized by malware or specific byte patterns in network traffic. An alert is generated the moment a suspect event is identified. The effectiveness of this Intrusion Detection System (IDS) in detecting and mitigating known threats is exceptional. It is incapable, however, of identifying zero-day assaults that were previously unknown and lacked defined signatures. SGD is widely utilized in the field of cyber security solutions due to its ease of implementation and efficacy in identifying known attacks. A research study on network intrusion detection for IoT security identifies this approach as one that minimizes false alarms while maximizing detection rates through the application of learning techniques [39].

## 5.3. Behavioral Analysis

Debugging potentially hazardous software in both physical and virtual environments requires dynamic code analysis. A variety of test inputs are executed against the program's source code in order to detect security vulnerabilities that may arise during interactions with other applications or systems. An instrument utilized to examine IoT attack behaviours is dynamic analysis [40]. There are numerous benefits to identifying IoT threats through behaviour analysis as opposed to static analysis. Through pattern recognition of attack activity, dynamic analysis can identify both known and unknown threats. Sandbox tools, including dynamic analysis platforms like Cuckoo Sandbox and CWS and Box, enable the real-time observation of malware activities.

A malware executable file's behaviour after being executed on the victim's host system is examined in the dynamic analysis behavioural report. The malware-infested files were downloaded from the Internet, the operating system was exploited to execute malicious operations, files were deleted and new ones created, sensitive data was collected through remote access, resources were denied to users, and the network's performance was intentionally hampered. Furthermore, the behaviour of assaults on the IoT may be investigated via memory analysis. To do memory analysis, it is necessary to take snapshots of the system's RAM while it is running in order to access its physical storage.

## 5.4. Honeypots

The purpose of a honeypot in cyber security is to lure would-be attackers by creating the illusion of a genuine and lucrative network. The network in which it runs is completely separate and unconnected. The system discussed before might be seen as a computer programme that mimics a genuine system in order to trick would-be attackers into interacting with it. By using this method, it is possible to keep tabs on the communications between intruders and their infected machines. Since honeypots are so useful for identifying threats and creating deception tools, information security experts have focused a lot of attention on them. A honeypot is a special kind of computer resource that is specifically designed to be manipulated in order to gather information about possible dangers. A honeypot's principal function is to deceive would-be attackers into thinking they're focusing on the wrong target or into giving up useful information about their attack tendencies [41]. The effectiveness of a honeypot may also be tested by subjecting it to malicious assaults. In order to lure would-be hackers into compromising a system, honeypots create a virtual environment that seems very similar to the real thing. If the hackers were to successfully breach the system, they would most likely be able to access this portion of the network and steal important data. The basic idea behind a honeypot is to keep an eye on incoming data and record it so that you may use it to stop similar cyber attacks in the future.

## 5.5 Security Information and Event Management

With the assistance of Security Information and Event Management (SIEM), a security system that aids in the detection and resolution of security threats and vulnerabilities, organizations can avert operational disruptions. SIEM systems function as vital auxiliary components of corporate security teams by enabling the detection of atypical user behaviour. Furthermore, these systems employ artificial intelligence to streamline and automate procedural stages, including incident management and threat detection [42]. Security information management (SIM) and security information management

(SEM) systems, which were initially designed to manage logs, have since expanded their capabilities to encompass a vast array of tasks. In addition to facilitating auditing processes and enabling the recording and tracking of security data to ensure compliance, these technologies enabled the real-time monitoring and analysis of security-related occurrences. SIEM systems are responsible for gathering event data from various sources throughout the entire IT infrastructure of an organization, including both on-premises and cloud-based systems. It is necessary to acquire, correlate, and analyze event log data from a variety of sources, including users, endpoints, applications, data sources, cloud workloads, and networks, in order to conduct real-time analysis. Information collected by hardware and software security measures, such as antivirus or firewall software, is also incorporated into this process. Security information and event management systems have the capability to incorporate threat intelligence reports obtained externally. This relationship enables the linking of threat signatures and profiles that have been previously developed to internal security data. With the assistance of real-time threat feeds, teams can identify and prevent new attack signatures more effectively.

## 6. RESEARCH CHALLENGES AND SECURITY RESEARCH IN IOT/IIOT

This section presents a taxonomy of security research for IoT and IIoT. Authentication methods verify persons, devices, or data during transit. Device authentication is achieved by the combination of simple cryptographic processes. Various approaches, including biometrics, chaotic maps, and blockchain-based fingerprint verification, are commonly utilized for user identification. Data authentication may be performed by establishing appropriate signature systems for various purposes. The blockchain architecture incorporates specialised smart contracts to facilitate efficient authorization mechanisms. In particular, indexing frameworks for intelligent objects are a common method of obtaining authorization in IIoT systems. IoT systems are susceptible to attack, with industrial IoT systems taking on especially severe damage. Additionally, preventive measures are IIoT-specific and employ fundamental cryptographic algorithms or other multi-level mitigation frameworks. User privacy and data protection are the two most important requirements for an IoT/IIoT system. In this domain, numerous blockchain-based solutions have been suggested. In recent times, the academic community has put forth a number of blockchain-based data aggregation strategies that are intended to facilitate privacy protection. Scholars have extended their attention to secure data management as well as safeguarding data privacy. In this domain, numerous blockchain-specific solutions, such as SDN have also been examined. One traditional approach to safeguarding data is through the implementation of multi-key aggregate keyword searchable encryption. Figure illustrates the security research breakthroughs in the IoT and IIoT sectors. This graphic and accompanying comments provide insight into the areas of focus and potential solutions by scholars. This enables future investigation and identifies open research areas for both IoT and IIoT.

However additional studies may not be addressed, this research gives a full review of IoT security, including IoT layers, threats, solutions, restrictions, and countermeasure studies from the literature. There are still numerous concerns to be investigated and resolved in future study. IoT devices have restricted processing capabilities, memory, and storage, thus they must function at minimal power. Security approaches that need strong encryption are unsuitable for restricted devices owing to the number and complexity of the decryption and encryption processes required to deliver data fast and securely. Thus, lightweight encryption techniques are required for limited devices such as actuators and sensors. The exchange of information between these devices must be safeguarded with hash functions and AES to ensure integrity and secrecy. The use of IDS in IoT networks introduces additional issues since it creates a huge number of false warnings. Providing real-time IoT-IDSs is challenging, as it requires extending the range of attack detection while also considering the influence on IoT device performance (overhead, energy consumption, accuracy). The new age of Industry 4.0 and industrial IoT necessitates developing a revolutionary intrusion detection approach to ensure the security of linked systems and services. Prevention measures for particular assaults on the IIoT environment, such as smart grids, transportation, and smart industries, require further research. Creating a lightweight security method for smart grid applications based on a less computation technique that is appropriate for restricted devices.

## 7. CONCLUSIONS

The IoT is transforming our daily lives by linking various technologies, devices, and apps to improve efficiency, provide infinite services, enhance quality of life, and give convenience. The proliferation of IoT devices poses significant security and privacy vulnerabilities. The new IoT technology enables physical network connectivity and the processing capabilities of sensors and control systems to create, exchange, and consume data with minimum human intervention. This survey showed several security concerns at different IoT levels, as well as security issues and solutions for the whole IoT environment. The article addresses security concerns at the network, middleware, communication, and application layers. Furthermore, it has conducted a critical examination of existing IoT solutions based on various security measures, such as encryption and IDSs. The current status of IoT security was also examined, along with possible future research initiatives to improve IoT security standards. This survey is designed to serve as a roadmap for

improving security in IoT industrial applications. Finally, we explore various current research difficulties related with the IoT ecosystem that require more study and analysis before IoT can be completely accepted, given the widespread application of IoT/IIoT, there is an urgent need to proactively address newly emerging dangers, as well as build effective security solutions leveraging cutting-edge technologies such as Blockchain. Thus, this study identifies potential open research topics on security challenges in IoT/IIoT, both for traditional and blockchain-based solutions, that have received little attention.

### Conflicts of Interest

The paper states that there are no personal, financial, or professional conflicts of interest.

### Funding

The absence of any funding statements or disclosures in the paper suggests that the author had no institutional or sponsor backing.

### Acknowledgment

The author extends appreciation to the kut university college for their unwavering support and encouragement during the course of this research.

### References

- [1] K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, "On security challenges and open issues in Internet of Things," *Future Gener. Comput. Syst.*, vol. 83, pp. 326–337, 2018.
- [2] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, "Challenges of securing Internet of Things devices: A survey," *Secur. Priv.*, vol. 1, p. e20, 2018.
- [3] K. K. Vaigandla, M. K. Vanteru, and M. Siluveru, "An Extensive Examination of the IoT and Blockchain Technologies in Relation to their Applications in the Healthcare Industry," *Mesopotamian J. Comput. Sci.*, pp. 1–14, 2024. [Online]. Available: <https://doi.org/10.58496/MJCSC/2024/001>
- [4] K. K. Vaigandla, R. K. Karne, and A. S. Rao, "A Study on IoT Technologies, Standards and Protocols," *IBM RD's J. Manag. Res.*, vol. 10, no. 2, Sep. 2021. DOI: 10.17697/ibmrd/2021/v10i2/166798
- [5] W. Ma, L. Ma, K. Li, and J. Guo, "Few-shot IoT attack detection based on SSDSAE and adaptive loss weighted meta residual network," *Inf. Fusion*, vol. 98, p. 101853, 2023. DOI: 10.1016/j.inffus.2023.101853
- [6] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, p. 102481, 2020. DOI: 10.1016/j.jnca.2019.102481
- [7] B. E. El-Shweky et al., "Internet of Things: A comparative study," in *Proc. 2018 IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2018, pp. 622–631.
- [8] A. M. Hassan and A. I. Awad, "Urban Transition in the Era of the Internet of Things: Social Implications and Privacy Challenges," *IEEE Access*, vol. 6, pp. 36428–36440, 2018.
- [9] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113–131, 2019.
- [10] C. Ramakrishna et al., "A Smart System for Future Generation based on the Internet of Things Employing Machine Learning, Deep Learning, and Artificial Intelligence: Comprehensive Survey," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 9, pp. 1798–1815, 2023. DOI: 10.17762/ijritcc.v11i9.9167.
- [11] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, vol. 4, pp. 1125–1142, 2017.
- [12] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," *J. Hardw. Syst. Secur.*, vol. 2, pp. 97–110, 2018.
- [13] J. Lee, S. Yu, K. Park, Y. Park, and Y. Park, "Secure Three-Factor Authentication Protocol for Multi-Gateway IoT Environments," *Sensors*, vol. 19, p. 2358, 2019.
- [14] K. K. Vaigandla, N. Azmi, and R. K. Karne, "Investigation on Intrusion Detection Systems (IDSs) in IoT," *Int. J. Emerg. Trends Eng. Res.*, vol. 10, no. 3, Mar. 2022. DOI: 10.30534/ijeter/2022/041032022
- [15] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN)," *Comput.*, vol. 9, p. 8, 2020.
- [16] "The History and Future of the Internet of Things." Available: <https://www.itransition.com/blog/iothistory>
- [17] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "A Novel Security Protocol for Wireless Sensor Networks with Cooperative Communication," *Comput.*, vol. 9, p. 4, 2020.
- [18] T. Hayajneh, K. Griggs, and M. Imran, "Secure and Efficient Data Delivery for Fog-Assisted Wireless Body Area Networks," *Peer-to-Peer Netw. Appl.*, vol. 12, pp. 1289–1307, 2019.
- [19] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare," *IEEE Internet Things J.*, vol. 6, pp. 410–420, 2019.

- [20] K. K. Vaigandla, "Communication Technologies and Challenges on 6G Networks for the Internet: Internet of Things (IoT) Based Analysis," in 2022 2nd Int. Conf. Innov. Pract. Technol. Manag. (ICIPTM), 2022, pp. 27–31. DOI: 10.1109/ICIPTM54933.2022.9753990.
- [21] M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT Security: A Layered Approach for Attacks and Defenses," in 2017 Int. Conf. Commun. Technol. (ComTech), 2017, pp. 104–110.
- [22] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security Vulnerabilities and Challenges," in 2015 IEEE Symp. Comput. Commun. (ISCC), 2015, pp. 180–187.
- [23] R. Yadav, Ritambhara, K. K. Vaigandla, G. S. P. Ghantasala, R. Singh, and D. Gangodkar, "The Blockchain Technology to Protect Data Access Using Intelligent Contracts Mechanism Security Framework for 5G Networks," in 2022 5th Int. Conf. Contemp. Comput. Inform. (IC3I), Uttar Pradesh, India, 2022, pp. 108–112. DOI: 10.1109/IC3I56241.2022.10072740.
- [24] K. K. Vaigandla, R. Karne, M. Siluveru, and M. Kesoju, "Review on Blockchain Technology: Architecture, Characteristics, Benefits, Algorithms, Challenges and Applications," *Mesopotamian J. CyberSecurity*, 2023, pp. 73–85. DOI: 10.58496/MJCS/2023/012.
- [25] S. Cha, J. Chen, C. Su, and K. Yeh, "A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.
- [26] S.-K. Kim, U.-M. Kim, and H. J. Huh, "A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security," *Energies*, vol. 12, p. 402, 2017.
- [27] J.-H. Huh and K. Seo, "Blockchain-Based Mobile Fingerprint Verification and Automatic Log-in Platform for Future Computing," *J. Supercomput.*, vol. 75, no. 6, pp. 3123–3139, 2019. DOI: 10.1007/s11227-018-2496-1.
- [28] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When Mobile Blockchain Meets Edge Computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, 2018.
- [29] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain-Based Searchable Encryption for Electronic Health Record Sharing," *Future Gener. Comput. Syst.*, vol. 95, pp. 420–429, 2019. Available: <http://www.sciencedirect.com/science/article/pii/S0167739X18314134>.
- [30] N. Venu, A. ArunKumar, and K. K. Vaigandla, "Investigation on Internet of Things (IoT): Technologies, Challenges and Applications in Healthcare," *Int. J. Res.*, vol. XI, no. II, pp. 143–153, Feb. 2022.
- [31] Forbes, "Blockchain in Healthcare: How it Could Make Digital Healthcare Safer and More Innovative," 2019.
- [32] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, 2019.
- [33] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A Blockchain-Based Non-Repudiation Network Computing Service Scheme for Industrial IoT," *IEEE Trans. Ind. Inf.*, 2019.
- [34] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSEIN: A Blockchain-Based Secure Mutual Authentication with Fine-Grained Access Control System for Industry 4.0," *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, 2018. Available: <http://www.sciencedirect.com/science/article/pii/S1084804518301619>.
- [35] R. Karne, S. Mounika, and K. K. Vaigandla, "Applications of IoT on Intrusion Detection System With Deep Learning Analysis," *Int. J. Innov. Eng. Manag. Res.*, vol. 11, SPL ISSUE 06, pp. 203–208, 2022. DOI: 10.48047/IJEMR/V11/SPL ISSUE 06/37.
- [36] S. H. Islam, M. K. Khan, and A. M. Al-Khouri, "Anonymous and Provably Secure Certificateless Multireceiver Encryption Without Bilinear Pairing," *Secur. Commun. Netw.*, vol. 8, no. 13, pp. 2214–2231, 2015.
- [37] A. Chatterjee and B. S. Ahmed, "IoT Anomaly Detection Methods and Applications: A Survey," *Internet Things*, vol. 19, 2022, p. 100568. DOI: 10.1016/j.iot.2022.100568.
- [38] N. U. Sheikh, H. Rahman, S. Vikram, and H. AlQahtani, "A Lightweight Signature-Based IDS for IoT Environment," 2018. arXiv:1811.04582.
- [39] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 3, pp. 2671–2701, 2019. DOI: 10.1109/COMST.2019.2896380.
- [40] P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, "A Study on Malicious Software Behaviour Analysis and Detection Techniques: Taxonomy, Current Trends and Challenges," *Future Gener. Comput. Syst.*, vol. 130, pp. 1–18, 2022. DOI: 10.1016/j.future.2021.11.030.
- [41] M. F. Razali, M. N. Razali, F. Z. Mansor, G. Muruti, and N. Jamil, "IoT Honeypot: A Review from Researcher's Perspective," in 2018 IEEE Conf. Appl. Inf. Netw. Secur. (AINS), 2018, pp. 93–98. DOI: 10.1109/AINS.2018.8631494.
- [42] Farhan et al., "Implementation of Security Information & Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System," *Intelmatix*, 2024. DOI: 10.25105/itm.v4i1.18529.