A Venture into the Realm of Security for the Industrial Internet of Things

Priya Jeejo Payyappilly*, Shweta Dour

School of Engineering & Technology, Navrachana University, Vasna-Bhayli, Vadodara-391410, Gujarat, India

Received: 1 June 2023 Revised: 15 December 2023 Accepted: 20 December 2023

Published: 30 December 2023

*Corresponding Author: 19721008@nuv.ac.in; priyajeejopayyappilly@gmail.com

https://doi.org/10.5281/zenodo.11470904

Abstract

Rapid growth of electronic and mobile technologies has given rise to smart devices that are capable of perceiving their surrounding environment and making associated decisions to accomplish simple or mission-critical tasks. This concept comes under the term Internet of Things. It is a confluence of electronics, mobile and internet technology which enables networked devices to link with each other and make cooperative decisions in order to cater to user experience by accomplishing pre-defined tasks. Industrial Internet of Things is an extension of the Internet of Things containing technology that is specifically directed towards implementation of concepts of Internet of Things for industrial applications. Ensuring security in the aforementioned applications is a topic of major concern among the engineering and scientific community alike. The concept of security is also paramount in ensuring a safe and effective experience for the end user of the technology. This paper is primarily a review paper attempting to furnish information on the Internet of Things, the Industrial Internet of Things and security implementations that have been proposed for the industrial internet of things. It also summarizes the various techniques and evaluating parameters that have been considered while designing security solutions for Industrial Internet of Things.

Keywords

Internet of Things, Industrial Internet of Things, Internet, network, protocol, technology, security, cyber security, information security, IoT security, IIoT security, cyber physical systems

Introduction

Around four decades ago, the concept of communication was limited primarily to first generation communication technology like analog telephones[1]. The advent of Internet[1] revolutionized the communications approach[1,2]. The worldwide interconnection of different networks, known as the Internet [1,2] has been around for more than three decades now. Since its inception, it has revolutionized the communication process happening around the world with increased efficiency and rapidity[3]. Its growth has been such through the years that it has become synonymous with ubiquity. It has progressed to include stationary and mobile devices in the interconnected web of information superhighway[3]. Any information is now just a click or a tap away. This revolution is also the result of enhancements in electrical, electronic and telecommunications technologies [3] and its interfacing with software, embedded systems, and even simple devices. Due to this, the devices have become 'smart'[4]. The term 'smart' implies that these devices are capable of a certain amount of decision making and can connect to the internet. The Internet is envisioned to include all types of devices alike so that a new concept called the Internet of Things[4] can be implemented. The next section underlines the contribution that the authors aim to offer through this article, followed by the organization of the paper.

Contribution of this paper:

The authors by means of this paper aim to:

- Introduce the concept of Internet of Things and Industrial Internet of Things

- Introduce the concept of Security for Industrial Internet of Things

- Present the analysis of different methods that have been proposed to increase security in Industrial Internet of Things.

Organization of this paper:

The rest of the paper is organized as follows:

The next section elucidates the concept of IoT, followed by the concept of IIoT and security for IIoT. After that, the section on Literature Survey explores the different studies that have been carried out in the field of security for IoT and IIoT [4]. Then, it is succeeded by the 'Results and Discussion' section. It focuses on bringing out the essence of these studies and also includes the author's observations towards the given studies including remarks and research opportunities. After that, the conclusion is presented and also the future scope of this study is added.

The Internet of Things

Incidentally, the internet was not envisioned as a forbearer of IoT. It was primarily thought of to connect computers around the world. By the late nineties, the concept of integrating physical things into the communication network was envisioned. Kevin Ashton[4] coined the term 'Internet of Things'[4, 5] to denote this kind of information exchange. Research work in the domain of IoT has gathered great momentum in the past decade. Rapid growth in electronics and communication technologies has given impetus to new technology of smart devices. These smart devices are capable of perceiving their environment and making decisions to provide services to the end-user. IoT embodies a heterogeneous connection between objects[5] where objects can be a device, a thing, a software, or a human being. IoT in essence is an amalgamation of myriad levels of protocols, communication technologies, data storage and management technologies and finally people along with processes to enable a seamless communication experience[5]. It is a global interconnection of devices which uses a standard internet protocol to provide services to users. The general representation of IoT as a layered structure can be summarized as shown in figure 1.

Starting from the bottom and progressing upward in Figure 1, the initial layer encompasses the essential components at the core of IoT, namely sensors and actuators[5]. These devices play a pivotal role by either sensing their surroundings or reacting to specific events. Commonly referred to as edge devices, mist devices, or fog devices, they are tasked with data acquisition and responding to events. Moving up, the subsequent layer is the network layer, where the facilitating technologies for communication between devices and across IoT networks are housed[7, 8]. This layer incorporates protocols that support short, medium, and long-range communications[8].

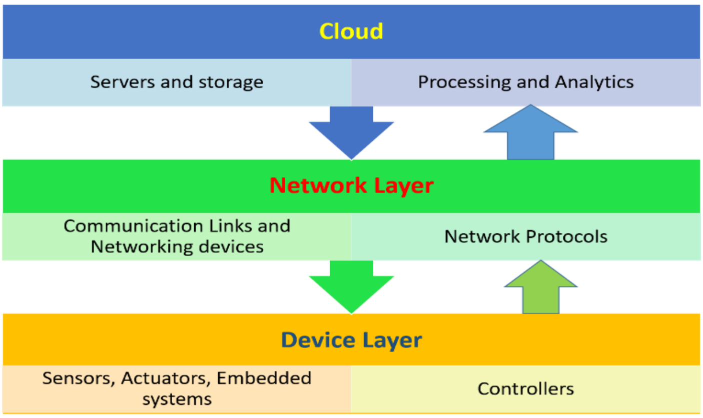


Fig. 1: IoT Layered Architecture

Proceeding to the subsequent layer, we encounter the data management layer, which assumes a crucial role in the conversion of data into various formats. This layer is responsible for structuring and analyzing data. The uppermost layer comprises tools and interfaces that facilitate user interaction with IoT devices, enabling them to access meaningful services. Security is a paramount consideration that must be addressed at each layer. The bidirectional flow of communication is denoted by the double-sided arrow in Figure 1, occurring at every layer. Figures 2 and 3 depict a rudimentary implementation[9] of the Internet of Things, emphasizing that the showcased implementation serves as a simplified representation for the purpose of clarity and comprehension, catering to readers from diverse backgrounds.

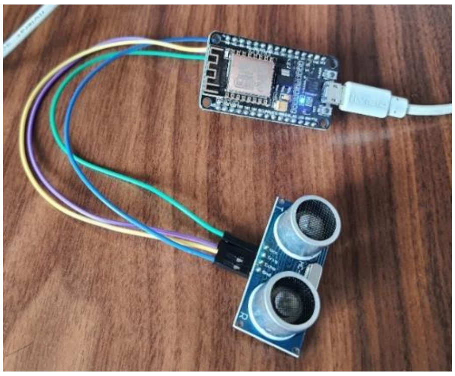
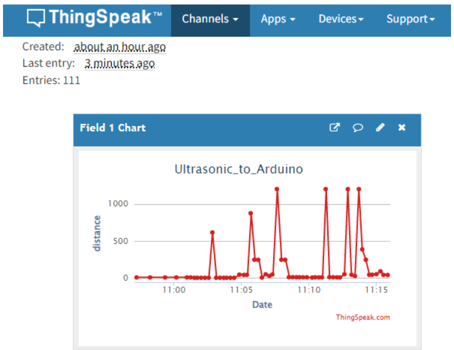


Fig. 2: Basic Implementation of Internet of Things: An ultrasonic Sensor connected to a microcontroller[9].

In Figure 2, an ultrasonic sensor is linked to a microcontroller known as NodeMCU. NodeMCU is an open-source platform that operates in conjunction with the ESP8266 Wi-Fi System on Chip (SoC) device. A microcontroller, often referred to as SoC due to its integration of basic computer system functions on a single chip, serves as the host for NodeMCU. The ultrasonic sensor is commonly employed to gauge the distance of an object from itself, making it an effective tool for obstacle detection. The sensor transmits distance information to the interfaced microcontroller. Subsequently, the microcontroller relays this information to the connected device or sends it to the cloud for further processing. In the cloud, the data can be visualized, offering insights, and revealing patterns within the dataset. Analyzing these data patterns over time empowers businesses to make informed decisions and anticipate changes based on the provided data. As shown in figure 3, the data is uploaded to the cloud platform called Thingspeak, the dashboard of Thingspeak shows the distribution of data over time by a line graph[7]. This application can be further extended to incorporate other sensors apart from ultrasonic sensors to get the data and store it in nodeMCU[9].



Created: about an hour ago
Last entry: 3 minutes ago
Entries: 111

Fig. 3: Basic Implementation of Internet of Things: Data uploaded to cloud[9].

The example cited above is just the tip of the iceberg, i.e. the varied potential that can be tapped from the implementation of Internet of Things. One such application area of the Internet of Things is in the domain of manufacturing for implementing the concept of Industry 4.0. This application area is called the Industrial Internet of Things which is explained in the next section.

Industrial Internet of Things

The extension of IoT towards industrial use is called Industrial Internet of Things[8] abbreviated as IIoT. It consists of various hardware, protocols and applications directed towards improving industrial processes[10]. It's a combination of Industrial automation systems and IoT systems [10, 11]. Processes occurring in an industry can be presented through figure 4. Industrial process generally consists of the steps that are mentioned in figure 4. The first step is manufacturing which implies the processes pertaining to designing and creation of product parts or whole product[12]. Following assembly, various components are brought together to form the complete product. Once the product is finalized, it undergoes packaging and may be either stored or transported to a central hub managing the inventory. This process may also involve conducting tests on the product.

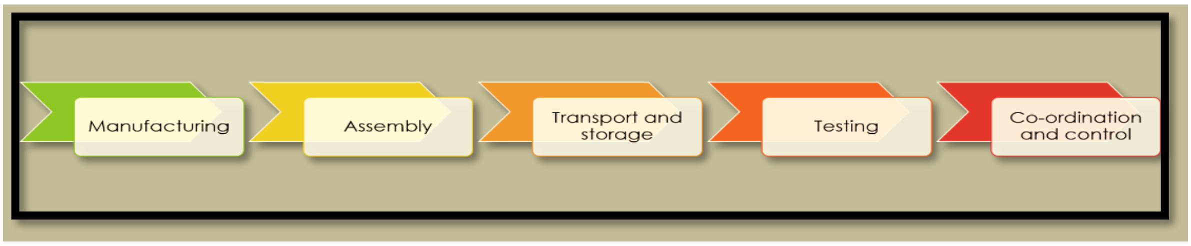


Fig. 4: Representation of Industrial processes

Testing may, at times, precede the transportation and storage phase. The Internet of Things (IoT) contributes to enhancing factory operations by offering services such as predictive maintenance[12] and streamlined processing. The fundamental architecture of an Industrial IoT implementation is illustrated in Figure 5. The initial layer comprises physical devices, typically end devices like sensors and actuators. The subsequent layer includes PLCs and controllers, making decisions based on received input. Following this is the OPC-UA server or SCADA systems, primarily serving as monitoring devices. This layer is succeeded by Edge gateway devices, acting as bridges between traditional networking architecture and Industrial IoT architecture.

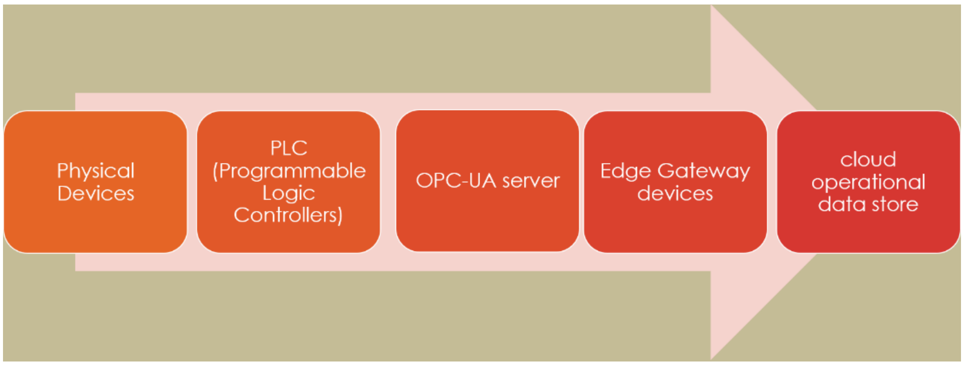

Physical Devices
PLC (Programmable Logic Controllers)
OPC-UA server
Edge Gateway devices
cloud operational data store

Fig. 5: Representation of IIoT Architecture

They relay information that is given by OPC-UA server to the cloud by mobilizing the data to travel on the network[13]. The data then reaches to the higher layer of architecture where it is stored for processing. This place is the cloud. The cloud is at a basic level and can be described as a data center consisting of myriad layers of hardware and software implementations. These data centers store data which can be then retrieved onto a dashboard as shown in figure 3 or given to different machine learning models to gain insights that may help businesses to grow and cater to their customer needs. Data travelling through the network and residing in the cloud is vulnerable to theft or loss in a public domain like the internet. Therefore, its security is of paramount importance. The successive section explains the concept of security for Industrial IoT.

Security in the context of Industrial IoT

IoT devices or IIoT devices for that matter, generally communicate using the internet using a wide variety of protocols making them vulnerable from a security point of view [13, 14]. Security is the ability of a system to safeguard against malicious entities that threaten the orderly working of a system. The Internet has been exposed to a lot of attacks since its commencement around four decades ago. These vulnerabilities are exploited by entities called malicious users/attackers[15,16.] These attackers can be a person or an external device[17]. Any application on the internet is susceptible to being attacked[18] on the following features as shown in figure 6. These features are collectively called the CIA triad[18]. The acronym can be expanded and explained as follows:

- Confidentiality[18]: implies that the message between communicating parties is private and not accessible to other entities apart from them. Confidentiality in a communications network is generally ensured by encrypting the data.
- Integrity[19]: The message transmitted should ensure the trustworthiness of the data, its accuracy and correctness. It generally implies that the data has not been modified in any way.

Fig. 6: The CIA triad

- Availability[19, 20]: The data will travel on the network and will be ultimately rendered to users through a web or mobile application. The availability criteria require to ensure that the data is available whenever the user requires it. It means ensuring uptime for websites and uninterrupted access to the system. In the field of cybersecurity, the CIA triad is the fundamental form of protection that has to be designed for a system.

There are also many other characteristics apart from the aforementioned triad, but the CIA triad forms the basis of most of the security descriptions. IIoT and IoT applications inherit the traits and vulnerabilities[20] of the traditional internet. Apart from that, they also have some vulnerabilities of their own. The vulnerabilities[21, 22] can be because the devices in IIoT are inherently smaller devices and so, they have memory constraints[23] and processing power constraints. As the security mechanisms[24] built for traditional applications connected to the internet require higher memory and processing power capability, the requirement is challenging to be fulfilled by IoT or IIoT applications. There are also times when security is not built into the system. These reasons make the applications susceptible to attacks[25]. A small description is provided in the next subsection as a means of understanding the practical implication of these kinds of attacks.

Security Breach in an IIoT firm: A Description

Authors Berger et. al.[26] have presented a case study in which a German steel facility's security was compromised by intruders. They infiltrated the facility by exploiting the vulnerabilities in the system. Consequently, there was a great deal of harm was caused to the physical devices as their behavior became unregulated, which greatly impacted important process elements. The authors describe the infiltration in five steps as shown in figure 7.

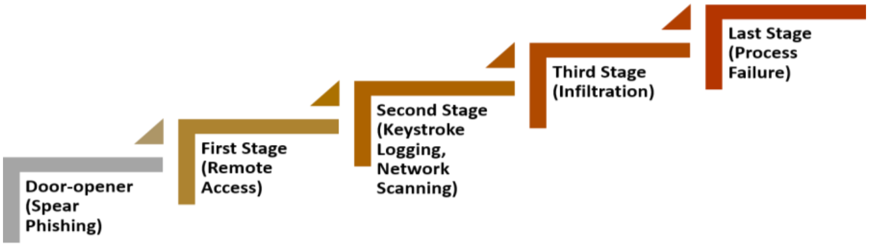

Door-opener (Spear Phishing)
First Stage (Remote Access)
Second Stage (Keystroke Logging, Network Scanning)
Third Stage (Infiltration)
Last Stage (Process Failure)

Fig. 7: Security breach stages for a German Steel Facility [26]

The attackers used spear-phishing emails with malicious malware to target the on-site operators in the facility. When the infected user opened the email, the malware took advantage of a glitch in one of the steel plant's applications. The attackers were able to enter the organization's network remotely using this exploit. The goal of the second phase was to compromise several workstations in order to gain access to the network and establish a base. To get into the network and obtain private data, the attackers used network scanning and keystroke logging. The attackers then made their way into the plant network. As of right now, it is unknown how this process was carried out. Once within the facility, the attackers used their knowledge of industrial control systems to cause several components to malfunction. This caused significant damage to property and monetary loss. From this, we can summarize that the attackers accessed confidential information, changed the controls, and made the whole network unavailable to the legitimate users thus attacking the CIA triad mentioned at the beginning of this section. This example is just the beginning point, various other attack scenarios are there wherein IIoT is in danger of being attacked using botnets, phishing, etc. making security of devices and network utmost importance.

The following section examines various studies that have been carried out in the realm of cybersecurity[26, 27] or information security[28] in an industrial setting and attempts to summarize the characteristics of security attacks that are launched on the devices [30, 31]. It also highlights the steps for mitigation that have been given by each of the studies.

Literature Survey

This section presents the literature survey of various techniques that have been proposed to increase security[28, 29] for the Industrial Internet of Things. At the end of the review, a compilation of comparisons between different techniques is proffered. Haseeb et al.[32] have proposed a deep learning model for malware detection in industrial IoT. Authors in this paper propose a model called ISEC which is the abbreviation for Intelligent and Secure Edge-Enabled Computing. This model primarily intends to develop a communication strategy for reducing the liability related to energy management and data security that is expended in data transportation. The area of attention for this model is mainly the smart city environment. Rehman et al.[33] put forward a model of security measures using the Green Internet of Things with Cloud Integrated Data Management (M-SMDM) for Smart Cities. It uses self-balancing trees for energy efficient communication. It also addresses the challenge of secret key distribution between peer nodes and attained trust for both limited and direct communication.

The parameters under observation are overheads and data latency which is optimized using the said approach. The analysis of this system is done using simulation environment ns3. Due to the broadcasting nature of wireless communication channels, there is a problem of eavesdropping that the Xingwang Li[34] have explored. To overcome this challenge, the authors propose C-AmBC, abbreviation for Cognitive Ambient Backscatter Communication. They investigate reliability and security of the proposed framework using the parameters of outage probability and intercept probability with analytical derivations. They have found trade-offs between signal to noise ratio, main to eavesdropper ratio and backscatter device. Kalyani et. al.[35] enlists the vulnerabilities of IoT systems and further states that homomorphic cryptosystems can be used to enhance the security of IoT devices. They go on to mention that there are three types of Homomorphic Encryption (HE): partial HE, somewhat HE and fully HE. They proposed preservation of data privacy in IoT systems through HE and SFF algorithm. The sensitive data is characterized by using the Deep Learning Neural Network then using combination of HE and SFF to secure the data and key. This algorithm is for improving IoT security and does not consider the energy aspect of the operations. Alzaharani et al.[36] design, construct, and assess a mandatory access control (MAC) system for the IoT. They further suggest a fine-grained context-aware access control mechanism that works over network flows which makes the solution transparent to IoT endpoints. They build the solution using standardized protocols without requiring any alteration. Abbas et al.[37] have proposed secure data management framework for Internet of Medical Things. Confidentiality and safety for patient data, scalability, and data accessibility are the most intricate IoT challenges. The authors aim to secure the medical data of the patient through blockchain technology. This method is a promising technique in data security for IoT devices. However, the energy dissipation expended for the security operations needs to be taken into consideration. Rampérez et al.[38] put forward a novel design of a context broker which relies internally on a context-aware content based publish-subscribe (CA-CBPS) middleware precisely designed to be elastic. Rahman et al.[39] propose blockchain based Software Defined Networking (SDN) for increasing the efficiency of trust in IoT nodes. The authors state that as SDN and blockchain are the latest technologies being incorporated in the internet realm, their inclusion in IoT study may yield significant improvement in security. They propose a model called Block-SDoTCloud which works on the aforementioned technologies. The lowest layer consists of perceptron in this model, the middle layer consists of blockchain, and the topmost layer consists of the cloud.

The information travels through these layers and due to the enhanced security offered by these technologies, devastating effects of attacks like Distributed Denial of Service Attack are ameliorated to a great extent. The proposed method yields better throughput, quick response time and faster file transformation. This approach takes only CPU utilization into consideration as a parameter for implementation of Green IoT. Lee et al.[40] present a test bed for implementing cyber security in Industrial IoT systems. They use packet filtering firewall and intrusion detection system to examine anomalous packets. The scenario for which it is implemented is the cluster of SCADA systems used in the Industrial IoT setting. The testbed consists of five sites namely control plane, Energy Management System (EMS) site, control plane, SCADA planes namely SCADA site #1 and SCADA site #2, SA (Substation Automation), IDS (Intrusion Detection System) and Power plant site. The firewall is called a whitelist firewall that performs pattern-based packet filtering and there is a packet duplicator that replicates the packet received from the firewall and sends it to intrusion detection system. The IDS in turn does anomaly detection. The control plane performs audit and analysis of the packets so as to test the strength of the security system. SCADA site #1 performs the actual cyber-attack detection. The authors have mainly checked for unauthorized control commands, illegal device manipulation, undefined behavior, or crashes and buffer overflow. Pundir et al.[41] have focused on multimedia part of the Industrial IoT setting. They state that multimedia data generated by surveillance devices in an industrial IoT setting are mostly vulnerable to attacks such as man-in-the –middle, replay, malware injection, etc. The authors observe that such types of attacks can greatly affect the working of devices in an IIoT setting. The affected devices as a result of these attacks may not function properly or stop functioning altogether. Therefore, it is imperative to have a mechanism that detects these kinds of attacks and warns the users. The authors have taken help of different methods used by artificial intelligence namely, naïve-bayes, logistic regression, and Artificial Neural Networks (ANNs) to detect these attacks. Using the model, the authors were able to achieve 99.5% accuracy and 0.5% false positive rate was generated. The authors check the performance of their algorithm for various parameters like Throughput, packet arrival rate and file transfer operation. The performance of the proposed model remains persistent in the face of various challenges. The authors further plan to incorporate Artificial Intelligence into the proposed model so as to enhance it. Patel et. al.[42] presents an outline of the standard IIoT data chain and the challenges that limit the wide-range disposition of the IoT ecosystem, such as scalability, lack of standard architectures and protocols, energy efficiency, and security and privacy concerns. The study aims at securing communication in an IIoT scenario augmenting trusted authority and secure element with elliptic curve cryptography which has been a technique for encryption for a long time. The encryption scheme is called EBAKE-SE. The technique has four phases: System setup phase, Device registration phase, Device authentication phase, and Dynamic device addition phase. In the System setup phase, the trusted authority (TA) sets up the system and issues public parameters. In the Device registration phase, the TA generates a unique ID and keys for each device and loads them into device memory. In the Device authentication phase, two devices authenticate each other and set the session key. In the Dynamic device addition phase, the TA adds a new device or replaces a device. The Secure Element (SE) mentioned in this instance is a tamper proof microprocessor chip that the authors propose. It stores data and runs the applications. The scheme has two phases of working. The first phase is the system initialization phase and mutual authentication phase. In the former phase, the trusted authority generates credentials for itself and loads it into the SE. Then in the later phase, the devices perform mutual authentication and generate one – time session key for secure communication. Then the communication between devices begins. The authors have proven its efficient working under four attacks i.e. replay attacks, man in the middle attack, impersonation attack and information leakage attack. Rahman et. al.[43] proposes a distributed, secure block chain-based software-defined networking (SDN)-enabled control architecture for cloud computing. They begin with the literature survey that introduces the readers with varied concepts pertaining to emerging technologies like software defined networking, smart industrial Internet of Things, blockchain, etc. They discuss the possibility of improving existing SDN features. They go on to explain that Blockchain is a ledger that is decentralized and distributed. It uses hash data to maintain information that is communicated to the next block in the ledger connection. This ensures the security of the transmitted data. The architecture is proposed to enhance the confidentiality of transmitted data for cloud-based systems in IIoT. The framework consists of five layers in all namely: Data Extraction, SDN Environment, Distributed Secure Blockchain Methodology, Cloud Computing Management, and Services for smart IIoT applications. The authors have simulated the aforementioned model in mininet network emulator and used openstack as a cloud storage platform and openflow as a protocol for SDN applications. They evaluate it on the performance based on Constant Bit Rate (CBR) and Response to Request Time (RTR). The authors state that the proposed system outperforms the core model and remains intact, even when the attack rate is increased, proving its robustness against malevolent or intentional malicious activities. Altunay et. al.[44] explores the possibilities that IoT brings to the automation process in industry. They state that IoT ecosystem has expanded in the past years due to the increase in usage of internet and cloud-based technologies. Increase in the scale of IoT and number of devices and their connection to the internet has also increased the chances of having intruders, the entities that try to obtain unauthorized access to the system. The authors propose an intrusion detection system that ensures the protection of an IoT application. They use a hybrid Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) model. The model was able to achieve an accuracy of 93.21% for binary classification and 92.9% accuracy for multi-classification for 100 trials. Han et. al.[45] has created an air pollution monitoring system in an IIoT scenario using 5G and for security, they have used the blockchain technology to secure the data that is transferred during communication. The framework has five layers namely: the perception layer, data processing layer, data preservation layer, application layer and 5G network layer. These layers collectively work to store encrypted data. The method has been effectively implemented and shows promising results. Amoretti et. al.[45] proposes a communication framework on the basis of the MQTT (Message Queueing Telemetry Transport) protocol. They use the broker bridging concept to enhance security over information flows at the manufacturing stages. The authors describe a scenario in which there are one or more production sites having PLCs and SCADA systems interconnected to headquarters and external cloud system depending on the application. Further, they can be connected to third party companies or manufacturers for control and monitoring. The authors state that MQTT is becoming the de facto standard for industries now and it is of paramount importance that the machines using this protocol be secured. They state that these methods suffer from issues related to scalability security problems as there is only a single broker. The proposed solution is a multi-stage framework where there are different brokers in place to enable clients to access different devices across the infrastructure. There are two layers of brokers, one layer that connects to a second layer of brokers that are connected to a single manufacturing line each. There are some data aggregation functions associated with each broker for easy categorization of data. The categorization enables data of similar categories to be grouped together for publishing and subscribing. The authors have called this M2M (Machine to Machine) interaction for ease of understanding. They state that due to this multi-level segregation of devices and data, security is ensured because each machine interacts with a single broker so there is less chance of interference. It makes the application scalable as the brokers are managing less amount of data flow. The number of interactions at network level is reduced due to multi-level interaction of devices. The authors have tested different broker bridging conditions and obtained promising results. They aim to apply it in various IIoT scenarios and use it for predictive maintenance and cloud manufacturing. Sanjuan et. al.[46] highlights in their work that security is not by default inbuilt into the MQTT protocol and therefore they are aiming towards improving the security of the aforementioned protocol. The authors highlight that the standard of MQTT protocol strongly recommends implementing it over Transport Layer Security (TLS) instead of the conventional TCP (Transmission Control Protocol). However, this option is not possible in most lightweight devices that make up the bulk of IoT ecosystem. They propose a model of MQTT in which every publisher and subscriber is equipped with a security schema with a cryptographic smart card. It's hardware with minimum cost and can be easily integrated with the existing system to provide an additional layer of security providing mutual authentication. They present the results of experiments with the Java Card library. The execution time for the implementation has been included in the study and shows effective results. Cui et. al.[47] presents the fact that IIoT faces various threats to confidentiality and anonymity. They state that conventional security mechanisms consider cloud and edge servers as semi-trusted entities which affects the security mechanism. The authors propose to change the role of edge node to a semi-trusted entity so that the edge node can be better secured. They have implemented a scheme based on group digital signature. The scheme is based on five main phases namely: 1) Key Generation and Distribution, 2) Message Publishing, 3) Re-encryption, 4) Message Decryption and Verification, 5) Message Tracing. Key generation phase is for generating key for new node joining the network. The KDC (Key Distribution Center) distributes the key. In the publishing phase, the message that is published is encrypted which then is re-encrypted in the third phase. Then it is sent to the subscribers. Then the subscriber verifies the message and decrypts it. In the message tracing phase, if a node is found to be relaying incorrect message, the KDC can expose the identity of the subscriber and hence the malicious node is caught. The authors then compared the different parameters like time for encryption, group signature, transmission, re-encryption decryption, verification and sum. The results show that the model performs well. The authors state that as future scope, they will implement batch certification in order to scale the system for varied input and design a secure framework. Ali et. al.[48] describes physical layer security for IIoT and states that 5G networks are instrumental in improving the quality of communication by offering an increase in the data transmission rate in a multiple user scenario. They go on to state that although the performance is improved, it still lacks the reliability required for certain applications like autonomous driving and industrial process control. The authors go on to state that these kinds of applications are susceptible to attacks like eavesdropping, content modification, denial of service by jamming attacks, etc. The solution to the aforementioned attacks is suggested by the authors named as PLS (Physical Layer Security) and IRS (Intelligent Reflecting Surfaces). PLS is a technique that minimizes shared information that could be accessed by potential eavesdroppers by utilizing wireless transmission features, such as noise and channel circumstances, to achieve secure communication at the targeted receiver. Unlike traditional cryptographic methods, PLS avoids the delays involved in digital signature signing and verification and does not require security keys. The Intelligent Reflective Surface (IRS) comprises a large quantity of passive radio antennas, commonly referred to as reflective radio elements. Through the utilization of these reconfigurable IRS elements, an incoming electromagnetic wave can be redirected towards a specific desired direction. The authors consider a Multiple Input Single Output (MISO) system where each user has a single antenna. The eavesdroppers are cut out from the network using a phase shift in the Omni—directional IRS. The assignment problem for IRS is solved using an allocation methodology called Weighted Sum Secrecy Rate (WSSR). The authors by implementing this method show that the WSSR method increases the performance of machines by 40%. There is an improvement seen in the secrecy rate as compared to other methods, further making it a better solution. Rathee et. al. [49] state that a predominant and specific powerful use of the Internet of Things is for the applications used in Industrial Internet of Things (IIoT), which is transforming industrial growth by facilitating transparent communication across various entities such as logistic centers, production facilities, and packaging units. IIoT systems that are decentralized often lack the capacity for efficient data processing; however, this shortcoming can be addressed using data science and data analytics techniques. IIoT is at utmost risk from possible attackers and network anomalies from a security perspective. The authors discuss the security issue that undermines the effective working of an IIoT network and suggest a solution in their work. In order to keep malicious devices or software out of the network, a coordinator IoT device has been added. This device determines how trustworthy other IoT devices are in the network. The coordinator device is elected by all other nodes in the network and that device calculates the trust of the other devices in the network and then based on that, it allows or removes malicious nodes. Furthermore, they incorporate a blockchain based data model to guarantee data transparency. The authors have tested their work using MATLAB which gives a very good success rate of attack detection by having metrics such as attack strength, message alteration, and probability of false authentication. Soliman et. al.[50] highlights that within interconnected networks, predominantly, intrusion detection systems (IDS) are used to thwart cyberattacks. However, a number of current Industrial Internet of Things (IIoT) intrusion detection systems encounter difficulties, including restricted attack type coverage, excessive feature dimensionality, dependence on outdated datasets, and inadequate attention to imbalanced dataset problems. The authors describe an intelligent intrusion detection system made to recognize cyberattacks in Industrial IoT networks as a response to the challenge of recognizing the attack. In order to improve detection performance, their proposed model makes use of the singular value decomposition (SVD) technique to decrease data characteristics. The authors apply the synthetic minority over-sampling (SMOTE) technique to mitigate the risk of biased classification resulting from over-fitting or under-fitting of data samples in a cluster. Both binary and multi-class classification tasks are implemented using a variety of machine learning and deep learning algorithms. They assess their intelligent model's effectiveness with an available dataset. The outcomes show that their method performs remarkably well, with a 99.99% accuracy rate and a 0.001% error rate for binary classification. The model showed a reduced error rate of 0.016% and an accuracy rate of 99.98% for multi-class categorization and hence was instrumental in detecting intrusion related attack. Liu et. al. [51] state that The Internet of Things (IoT) has been widely adopted in smart cities, industrial settings, healthcare, and other fields in contemporary years, and it has been influential in transforming these industries. Due to its self-organizational characteristics, wireless sensor networks (WSNs) have become an essential technique in Internet of Things (IoT) systems, especially in industries. These networks are used to gather environmental data from edge devices. However, high Transmission Delay (TD) and excessive Battery Energy Consumption (EC) are among the major issues faced by IoT-enabled WSNs due to the gigantic volume of diverse data created by varied sensing devices. Recent years have seen a prevalent adoption of the Internet of Things (IoT), which has revolutionized a number of industries, including smart cities, manufacturing, healthcare, and others. Wireless sensor networks (WSNs) have emerged as a key technology in Internet of Things (IoT) systems, particularly in industries, due to their self-organizational characteristics. However, due to the aforementioned reasons of high quantity of data generation and complex environmental settings, high Transmission Delay (TD) and excessive Battery Energy Consumption (EC) are among the key problems faced by IoT-enabled WSNs. In order to improve efficiency of the current WSN scenario, the authors present their work entitled LEACH-D, a novel clustering-based data transmission algorithm for IIoT. LEACH-D guarantees constant battery energy consumption while simultaneously lengthening the transmission job. Its goal is to improve performance indicators, like the first node death (FND) average transmission time. The experimental results, which indicate notable reductions in average transmission time by percentages of 51.32%, 12.12%, 12.96%, and 5.42%, validate the efficacy of the proposed algorithm. These enhancements surpass the performance of contemporary algorithms that the authors have described namely, LEACH, EE-LEACH, ETH-LEACH, FREE_MODE, and LEACH. Garcés-Jiménez et. al. [52] assert that the transferal of industries towards the industry 4.0 paradigm requires solutions that involve machine-mounted devices that allow industrial equipment to be supervised and controlled. To assure the correct functioning of devices against many diverse and complex forms of attack, an effective monitoring mechanism is vital to the safety of the floor devices. The authors offer a method for identifying and categorizing common issues with these gadgets using machine learning approaches that take advantage of aspects like energy usage, data processing, and major application use. A dataset that was gathered from a testbed that was running a common equipment monitoring application was used to validate the suggested methodology. The aforementioned machine learning pipeline achieves 99.4% accuracy, 99.7% precision, 99.6% recall and 75.2% specificity by using a decision tree-based model for spotting and singling out a defect. For additional fault classification, a Semi-Supervised Graph-Based model is then used, and the results show 99.3% accuracy, 96.4% precision, 96.1% recall and 99.6% specificity. The results gathered highlight the important role that machine learning techniques which make use of available parameters play a significant role in mitigating common device defects and enhancing the overall resilience of industrial systems.

Justification for the Current Study

IIoT is largely governed by IT (Information Technology) and OT (Operational Technology) with the addition of the Internet in the mix. This creates a myriad of opportunities and challenges as explained by the research company Gartner[53]. Authors Boyle et. al.[54], Moura et. al. [55] and numerous other researchers including all articles mentioned in the literature survey recognize the potential for IIoT leading the industrial revolution in the coming future. Hence a basic knowledge about this technology enables anyone pursuing a study in this field. This article therefore strives to facilitate that knowledge to the readers.

Observations and Discussion

Based on the literature survey, a classification based on layered architecture of IoT can be highlighted i.e., summary can be made based on what study targets which specific layer of the IoT/ IIoT architecture. The summary of the same is given below:

Sr. No.	**Paper Title**	**Layer of IIoT/IoT architecture for which security implementation is applicable**
1.	Intelligent and secure edge-enabled computing model for sustainable cities[32]	Edge (device layer)
2.	M-SMDM: A model of security measures using Green Internet of Things with Cloud Integrated Data Management for Smart Cities[33]	Cloud
3.	Physical Layer Security of Cognitive Ambient Backscatter Communications for Green Internet-of-Things[33]	Physical Layer (Device Layer) and Network Layer focusing on radio frequency
4.	An efficient approach for enhancing security in Internet of Things using the optimum authentication key[34]	Network layer encryption and key exchange
5.	Enhancing Internet of Things Security using Software-Defined Networking[35]	Network layer
6.	Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things[36]	Cloud layer and network layer
8.	An Innovative Approach to Improve Elasticity and Performance of Message Brokers for Green Smart Cities[37]	Cloud layer
11.	Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network[38]	Cloud layer
12.	Design and implementation of cybersecurity testbed for industrial IoT systems[39]	Physical layer and network layer implementation and testing
13.	MADP-IIME: malware attack detection protocol in IoT-enabled industrial	Device layer specifically focussing on malware infection

	multimedia environment using machine learning approach.[40]	
14.	EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element[41]	Network layer
15.	Towards a block chain-SDN-based secure architecture for cloud computing in smart industrial IoT[42]	Cloud layer and network layer
16.	A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks[43]	Network layer intrusion detection
17.	A Novel Architecture of Air Pollution Measurement Platform Using 5G and Blockchain for Industrial IoT Applications[44]	Network layer
18.	A Scalable and Secure Publish/Subscribe-Based Framework for Industrial IoT [45]	Oriented towards Network layer and application layer protocols
19.	Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach[46]	Device layer and application layer protocols
20.	Anonymous Message Authentication Scheme for Semi trusted Edge-Enabled IIoT[47]	Device layer
21.	IRS-Assisted Physical Layer Security for 5G Enabled Industrial Internet of Things[48]	Device layer
22	A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain[49]	Network layer
23	Deep learning-based intrusion detection approach for securing industrial Internet of Things[50]	Network layer and physical layer
24	A low-energy, low-delay data transmission method for industrial internet of things wireless sensors[51]	Network layer
25	Industrial Internet of Things embedded device's fault detection and classification. A case study[52]	Device layer

Table 1. Classification of security implementations with respect to layered architecture of IIoT

It can be inferred from the contents in table 1 all studies that have been targeted towards one or the other layer of the IoT layered architecture mentioned in figure 1. It can be seen that most of the security solutions are either applied to the network layer or the cloud layer, the device layer has been explored less. Next table enlists the observations from an implementation point of view and checks whether the solution has been implanted for IIoT or not.

It can be inferred from the observations enlisted in table 2 that effective security mechanisms have been realized for the Industrial Internet of Things. Diverse branches of Artificial Intelligence also play a significant role in implementation of operative protection mechanisms for the Industrial Internet of Things. The observations by the authors have been summarized in table 1.

Sr. No.	**Paper Name**	**Technology/Framework/ Protocol**	**Security**	**Incorporated for IIoT**	**Observation**
1.	Intelligent and secure edge-enabled computing model for sustainable cities[32]	Deep learning	√	X	Model mainly implemented for smart city environment so it is not clear if it can be implemented for other applications.
2.	M-SMDM: A model of security measures using Green Internet of Things with Cloud Integrated Data Management for Smart Cities[33]	Cloud	√	X	Overhead and latency optimized. Implemented as a simulation on ns3 platform.
3.	Physical Layer Security of Cognitive Ambient Backscatter Communications for Green Internet-of-Things[33]	Cognitive Ambient Backscatter Communication	√	X	Protects against eavesdropping, other kinds of attacks are not considered.
4.	An efficient approach for enhancing security in Internet of Things using the optimum authentication key[34]	Deep Learning Neural Network	√	X	Encryption is done to ensure confidentiality.
5.	Enhancing Internet of Things Security using Software-Defined Networking[35]	Software Defined Networking	√	√	The security is built on existing OpenFlow protocol
6.	Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things[36]	Blockchain	√	X	Security is covered but the existing protocols are taken not much change has been made
8.	An Innovative Approach to Improve Elasticity and Performance of Message Brokers for Green Smart Cities[37]	Publish-subscribe model	√	X	QoS parameters like throughput and delay

11.	Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network[38]	Software Defined Networking and Blockchain	√	X	Primarily for DDoS attack
12.	Design and implementation of cybersecurity testbed for industrial IoT systems[39]	IDS and whitelist firewall	√	√	For getting information about anomalous behavior in devices
13.	MADP-IIME: malware attack detection protocol in IoT-enabled industrial multimedia environment using machine learning approach.[40]	Machine Learning	√	√	For malwares spread at communication layer
14.	EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element[41]	Elliptic Curve Cryptography key exchange, Secure Element (tamper resistant microprocessor chip)	√	√	Safeguards against passive attacks like replay and man-in the middle
15.	Towards a block chain-SDN-based secure architecture for cloud computing in smart industrial IoT[42]	Blockchain	√	√	Emulator based study
16.	A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks[43]	Intrusion Detection System CNN and LSTM	√	√	Detecting unauthorized access
17.	A Novel Architecture of Air Pollution Measurement Platform Using 5G and Blockchain for Industrial IoT Applications[44]	5G and blockchain	√	√	Encryption of data at rest
18.	A Scalable and Secure Publish/Subscribe-Based Framework for Industrial IoT [45]	MQTT	√	√	Multi-level broker architecture
19.	Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach[46]	Smart card	√	√	Low-cost hardware addition to the existing device.
20.	Anonymous Message Authentication Scheme for Semi trusted Edge-Enabled IIoT[47]	Encryption	√	√	Directed towards assuring confidentiality and anonymity
21.	IRS-Assisted Physical Layer Security for 5G Enabled Industrial Internet of Things[48]	Physical layer security, Intelligent Reflective Surfaces	√	√	Confidentiality and Service availability

22	A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain[49]	Trust computation, blockchain based data model	√	√	Trust, attack strength, message alteration, false authentication probability
23	Deep learning-based intrusion detection approach for securing industrial Internet of Things[50]	Intelligent Intrusion Detection System, Singular Value Decomposition Technique and synthetic minority oversampling	√	√	Classification result, error in classification
24	A low-energy, low-delay data transmission method for industrial internet of things wireless sensors[51]	LEACH-D for lower battery power consumption	X	√	Average transmission time and performance
25	Industrial Internet of Things embedded device's fault detection and classification. A case study[52]	Decision tree-based model in machine learning	√	√	Accuracy, precision, recall, specificity

Table 2. Summary of Security Implemented for Industrial Internet of Things

As shown in table 1, there are various techniques implemented to incorporate security in the Industrial internet of Things. However, it is important to note that there is still scope of better implementations for the same. The shortcomings of the articles in the literature survey can be stated as given in the next subsection.

Research gaps or Opportunities

The solutions implemented are not necessarily implemented for IIoT. Some have been implemented for other scenarios like smart cities, Internet of Medical Things, etc.

The proposed solutions are different for different types of cyber-attacks, there does not exist a framework which takes into consideration all types of cyber-attacks or a majority of cyber-attacks.

Machine learning is the primary method in which Artificial Intelligence is used to detect attacks. Other deep learning approaches can also be considered for attack detection and mitigation. So, it is evident that there is still scope for improvement in this domain.

Implication of Current Research Review

The present study offers an insight into the various terminologies associated with IoT, IIoT and IIoT security. Readers through this article will be able to:

- Understand and define Internet of Things and Industrial Internet of Things
- Describe basic terminologies related to Industrial Internet of Things
- Describe characteristics for security for IIoT devices
- Understand different work that has been carried out in IoT/ IIoT security domain and the parameters that have been taken into account by different authors.

Conclusion and Future Scope

The authors by means of this article attempted to proffer information about the concept of Internet of Things, the Industrial Internet of Things and the concept of security in the current scenario for improving communication safety in the Industrial Internet of Things domain. The authors were able to explore various security methods proposed and pinpoint the characteristics of each method. The study can be extended towards implementing security mechanisms for different types of cyber-attacks for different protocols used in the Industrial Internet of Things.

References

1. Kleinrock, L. (2010). An early history of the internet [History of Communications]. *IEEE Communications Magazine*, 48(8), 26–36. https://doi.org/10.1109/mcom.2010.5534584
2. Bonastre, O.M. and Veà, A. (2019), Origins of the Domain Name System, *IEEE Annals of the History of Computing*, 41(2), 48-60. https://doi.org/10.1109/MAHC.2019.2913116
3. Martikainen, O. "Internet Revolution in Telecom," IEEE John Vincent Atanasoff. (2006). *International Symposium on Modern Computing (JVA'06)*, Sofia, Bulgaria, 58-62. https://doi.org/10.1109/JVA.2006.31
4. Collin, J., Pellikka, J., & Penttinen, J. T. J. (2024). *Digital Disruption of Industries. 5G Innovations for Industry Transformation: Data-Driven Use Cases*, 1-18. https://doi.org/10.1002/9781394181513.ch1

5. Minoli, D., & Occhiogrosso, B. (2024). Current and Evolving Applications to IoT and Applications to Smart Buildings and Energy Management. *In AI Applications to Communications and Information Technologies: The Role of Ultra Deep Neural Networks, IEEE,* 257-346. https://doi.org/10.1002/9781394190034.ch5
6. Rezaee, N., Zanjirchi, S. M., Jalilian, N., & Bamakan, S. M. H. (2023). Internet of things empowering operations management; A systematic review based on bibliometric and content analysis. Telematics and Informatics Reports, 11. https://doi.org/10.1016/j.teler.2023.100096
7. Goyal, P., Sahoo, A. K., & Sharma, T. K. (2021). Internet of things: Architecture and enabling technologies. *Materials Today: Proceedings*, *34,* 719–735. https://doi.org/10.1016/j.matpr.2020.04.678
8. Yu, X. and Sun, F. A (2022). Study on Telecommunication Network, Internet, and Internet of Things, *10th International Conference on Information Systems and Computing Technology (ISCTech), Guilin, China*, 673-680. https://doi.org/10.1109/ISCTech58360.2022.00111
9. Payyappilly, P.J., Dour, S. (2023). IoT Communication to Capture and Store Data to Thingspeak Cloud Using NodeMCU and Ultrasonic Sensor. In: Hemanth, J., Pelusi, D., Chen, J.IZ. (eds) *Intelligent Cyber Physical Systems and Internet of Things*. ICoICI 2022. *Engineering Cyber-Physical Systems and Critical Infrastructures*, vol 3. Springer, Cham. https://doi.org/10.1007/978-3-031-18497-0_10
10. Abbas, S.G., Hashmat, F. and Shah, G.A., (2020). A Multi-layer Industrial-IoT Attack Taxonomy: Layers, Dimensions, Techniques and Application, *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1820-1825. https://doi.org/10.1109/TrustCom50675.2020.00249

11. Kraeling, M., Brogioli, M.C., (2019). In: Editor(s): Robert Oshana, Mark Kraeling, *Software Engineering for Embedded Systems* (Second Edition), Newnes, 465-499. https://doi.org/10.1016/B978-0-12-809448-8.00013-8
12. Soori, M., Arezoo, B., Dastres, R., (2023) Internet of things for smart factories in industry 4.0, a review, *Internet of Things and Cyber-Physical Systems*, 3, 192-204. https://doi.org/10.1016/j.iotcps.2023.04.006
13. Hazra, A., Amgoth, T. (2022) CeCO: Cost-Efficient Computation Offloading of IoT Applications in Green Industrial Fog Networks, *IEEE Transactions on Industrial Informatics*, (9), 6255-6263. https://doi.org/10.1109/TII.2021.3130255
14. Lalos, A.S., Vlachos, E., Berberidis, K., Fournaris, A.P. and Koulamas, C., (2020). Privacy Preservation in Industrial IoT via Fast Adaptive Correlation Matrix Completion, *IEEE Transactions on Industrial Informatics,* 16(12), 7765-7773. https://doi.org/10.1109/TII.2019.2960275
15. Piccialli, F., Bessis, N., Cambria, E., (2021) Guest Editorial: Industrial Internet of Things: Where Are We and What Is Next?, *IEEE Transactions on Industrial Informatics*, 17(11), 7700-7703. https://doi.org/10.1109/TII.2021.3086771
16. Serpanos, D., (2024) Industrial Internet of Things: Trends and Challenges, *Computer*, 57(1), 124-128. https://doi.org/10.1109/MC.2023.3331552
17. Yu, P., Long, Y., Yan, H., Chen, H., Geng, X., (2022)., Design of Security Protection Based on Industrial Internet of Things Technology, *14th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, 515-518. https://doi.org/10.1109/ICMTMA54903.2022.00109

18. Al-Sada, B., Sadighian, A., Oligeri, G. (2024) Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database, *IEEE Access*, 12, 1217-1234. https://doi.org//10.1109/ACCESS.2023.3344680
19. Malik, P.K., Sharma, R., Singh, R., Gehlot, A., Satapathy, S.C., Alnumay, W.S., Pelusi, D., Ghosh, U., Nayak, J., (2021) Industrial Internet of Things and its Applications in Industry 4.0: State of The Art, *Computer Communications*, 166, 125-139. https://doi.org/10.1016/j.comcom.2020.11.016
20. Saqib,M., Moon, A.H., (2023). A Systematic Security Assessment and Review of Internet of Things in the Context of Authentication, *Computers & Security*, 125. https://doi.org/10.1016/j.cose.2022.103053
21. Liu, C., (2020). Research on the Gradual Intelligence of Industrial Internet of Things, *International Conference on Computer Communication and Network Security (CCNS)*, 113-116. https://doi.org/10.1109/CCNS50731.2020.00032
22. Rakas, S.B., Timčenko, V., Kabović, M., Kabović, A., (2021). Industrial Internet: Architecture, characteristics and implementation challenges, *20th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 1-4. https://doi.org/10.1109/INFOTEH51037.2021.9400694
23. Chen, H., Han, X., Zhang, Y., (2024). Endogenous Security Formal Definition, Innovation Mechanisms, and Experiment Research in Industrial Internet, *Tsinghua Science and Technology*, 29(2), 492-505, https://doi.org/10.26599/TST.2023.9010034
24. Bansal, M., Nanda, M., Husain, M.N., (2021), Security and privacy Aspects for Internet of Things (IoT), *6th International Conference on Inventive Computation Technologies (ICICT)*, 199-204. https://doi.org//10.1109/ICICT50816.2021.9358665
25. Corallo, A., Lazoi, M., Lezzi, M., (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts, *Computers in Industry*, Volume 114. https://doi.org/10.1016/j.compind.2019.103165
26. Berger, S., Bürger, O., Röglinger, M., (2020). Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy, *Computers & Security*, 93. https://doi.org/10.1016/j.cose.2020.101790
27. Chaudhary, S., Mishra, P.K., (2023). DDoS attacks in Industrial IoT: A survey, *Computer Networks*, Volume 236. https://doi.org/10.1016/j.comnet.2023.110015

28. Chen, H., Hu, M., Yan, H., P. Yu, (2019) Research on Industrial Internet of Things Security Architecture and Protection Strategy, *International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, 365-368. https://doi.org/10.1109/ICVRIS.2019.00095
29. Milić, S.D, Đurović, Z., Stojanović, M.D., (2023), Data science and machine learning in the IIoT concepts of power plants, *International Journal of Electrical Power & Energy Systems*, 145. https://doi.org/10.1016/j.ijepes.2022.108711
30. Shojafar, M., Mukherjee, M., Piuri, V., Abawajy, J., (2022). Guest Editorial: Security and Privacy of Federated Learning Solutions for Industrial IoT Applications, *IEEE Transactions on Industrial Informatics*, 18(5), 3519-3521. https://doi.org/10.1109/TII.2021.3128972
31. Haseeb, K., Din, I.U., Almogren, A., Ahmed, I., Guizani, M., (2021) Intelligent and secure edge-enabled computing model for sustainable cities using green internet of things, Sustainable Cities and Society, 68. https://doi.org/10.1016/j.scs.2021.102779
32. Rehman, A., Haseeb, K., Saba, T., Kolivand, H., (2021), M-SMDM: A model of security measures using Green Internet of Things with Cloud Integrated Data Management for Smart Cities, *Environmental Technology & Innovation*, 24. https://doi.org/10.1016/j.eti.2021.101802
33. Li, X., Zheng, Y., Khan, W.U., Zeng, M., Li, D., Ragesh, G.K., Li, L., (2021), Physical Layer Security of Cognitive Ambient Backscatter Communications for Green Internet-of-Things, *IEEE Transactions on Green Communications and Networking*, 5(3), 1066-1076. https://doi.org/10.1109/TGCN.2021.3062060
34. Kalyani, G., Chaudhari, S., (2019), An efficient approach for enhancing security in Internet of Things using the optimum authentication key, *International Journal of Computers and Applications*, 306-314. https://doi.org/10.1080/1206212X.2019.1619277
35. Alzahrani, B., Fotiou, N., (2020), Enhancing Internet of Things Security using Software-Defined Networking, *Journal of Systems Architecture*, Volume 110. https://doi.org/10.1016/j.sysarc.2020.101779
36. Abbas, A., Alroobaea, R., Krichen, M., (2021), Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical

Things, *Personal and Ubiquitous Computing*. https://doi.org/10.1007/s00779-021-01583-8ID

37. Rampérez, V., Soriano, J., Lizcano, D., Lara. J.A., (2018). An Innovative Approach to Improve Elasticity and Performance of Message Brokers for Green Smart Cities. In *Proceedings of the Fourth International Conference on Engineering & MIS 2018 (ICEMIS '18). Association for Computing Machinery*, Article 34, 1–5. https://doi.org/10.1145/3234698.3234732
38. Rahman, A., Islam, M.J., Khan, M.S. I., Kabir, S., Pritom, A.I., Karim, M.R., (2020). Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network," *2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, 1-6. https://doi.org/10.1109/STI50764.2020.9350419
39. Lee, S., Yoo, H. (2018), Design and implementation of cybersecurity testbed for industrial IoT systems., *J Supercomput*, 74, 4506–4520. https://doi.org/10.1007/s11227-017-2219-z
40. Pundir, S., Obaidat, M.S., Wazid, M. (2021). MADP-IIME: malware attack detection protocol in IoT-enabled industrial multimedia environment using machine learning approach, *Multimedia Systems*. https://doi.org/10.1007/s00530-020-00743-9
41. Patel, C., Bashir, A.K., AlZubi, A. A., Jhaveri, R., (2022), EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element, *Digital Communications and Networks*. https://doi.org/10.1016/j.dcan.2022.11.001
42. Rahman, A., Islam, M., J., Band, S. S., Hasan, G. M.K., Tiwari, P., (2022) Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT, *Digital Communications and Networks*. https://doi.org/10.1016/j.dcan.2022.11.003
43. Altunay, H.C. Albayrak, Z., (2023). A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks, *Engineering Science and Technology, an International Journal*, 38. https://doi.org/10.1016/j.jestch.2022.101322
44. Han, Y., Park, B., Jeong, J., (2019). A Novel Architecture of Air Pollution Measurement Platform Using 5G and Blockchain for Industrial IoT Applications, *Procedia Computer Science*, 155, 728-733. https://doi.org/10.1016/j.procs.2019.08.105

45. Amoretti, M., Pecori, R., Protskaya, Y., Veltri, L., Zanichelli, F., (2021). A Scalable and Secure Publish/Subscribe-Based Framework for Industrial IoT, *IEEE Transactions on Industrial Informatics*, 17(6), 3815-3825. https://doi.org/10.1109/TII.2020.3017227
46. Sanjuan, E.B., Cardiel, I. A., Cerrada, J. A., Cerrada, C., (2020), Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach, *IEEE Access*, 8, 115051-115062. https://doi.org/10.1109/ACCESS.2020.3003998
47. Cui, J., Wang, F., Zhang, Q., Xu, Y., Zhong, H. (2021), Anonymous Message Authentication Scheme for Semi trusted Edge-Enabled IIoT, *IEEE Transactions on Industrial Electronics*, 68(12), 12921-12929. https://doi.org/10.1109/TIE.2020.3039227
48. Ali, B., Mirza, J., Alvi, S. H., Khan, M. Z., Javed, M. A., Noorwali, A., (2023), IRS-Assisted Physical Layer Security for 5G Enabled Industrial Internet of Things, *IEEE Access*, 11, 21354-21363. https://doi.org/10.1109/ACCESS.2023.3250251
49. Rathee, G., Ahmad, F., Jaglan, N., Konstantinou, C. (2023), A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain, *IEEE Transactions on Industrial Informatics*, 19(2), 1894-1902. https://doi.org/10.1109/TII.2022.3182121
50. Soliman, S., Oudah, W., Aljuhani, A., (2023), Deep learning-based intrusion detection approach for securing industrial Internet of Things, *Alexandria Engineering Journal*, 81, 371-383. https://doi.org/10.1016/j.aej.2023.09.023
51. Liu, D., Liang, C., Mo, H., Chen, X., Kong, D., Chen, P., (2024), LEACH-D: A low-energy, low-delay data transmission method for industrial internet of things wireless sensors, *Internet of Things and Cyber-Physical Systems*, 4, 129-137. https://doi.org/10.1016/j.iotcps.2023.10.001
52. Garcés-Jiménez, A., Rodrigues, A., Gómez-Pulido, J. M., Raposo, D., Gómez-Pulido, J.A., Silva, J.S., Boavida, F., (2024), Industrial Internet of Things embedded device’s fault detection and classification. A case study, *Internet of Things*, 25. https://doi.org/10.1016/j.iot.2023.101042
53. Predicts 2017: IT and OT Convergence Will Create New Challenges and Opportunities. (n.d.). Gartner. https://www.gartner.com/en/documents/3531817
54. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018, October). 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

55. Moura, R., Ceotto, L., Gonzalez, A., & Toledo, R. (2018, December). Industrial Internet of Things (IIoT) Platforms - An Evaluation Model. *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*. https://doi.org/10.1109/csci46756.2018.00194

Glossary

Internet of Things – A network of physical devices, vehicles, appliances and other physical objects called ‘things’ that are embedded with sensors, software and network connectivity that allows them to collect and share data.

Industrial Internet of Things - An ecosystem of devices, sensors, applications, and associated networking equipment that work together to collect, monitor, and analyze data from industrial operations.

Microcontroller - An integrated circuit that contains a microprocessor along with memory and associated circuits and those controls some or all of the functions of an electronic device or system.

Microprocessor - A part of a computer that controls its primary operations.

Sensor - A device that reacts to a physical stimulus (such as heat, light, sound, pressure, magnetism, or a particular type of motion) and transmits a resulting impulse (as for measurement or operating a control).

Actuator - A mechanical device for moving or controlling a machinery part or a part of a system.

Cloud Computing - The practice of storing regularly used computer data on multiple servers that can be accessed through the Internet.

Cloud – A set of servers that store data and are interconnected through the internet.

Protocol – A set of rules that govern data communication.

Architecture – A framework with a set of protocols to facilitate the working of any application.

Security – The protection designed for a system against external attacks.

Cybersecurity - Cybersecurity is the practice of protecting computer systems, networks, and programs from digital attacks.

SCADA – Abbreviation for supervisory control and data acquisition. It is a category of software applications for controlling industrial processes, which is the gathering of data in Real Time from remote locations in order to control equipment and conditions. SCADA provides organizations with the tools needed to make and deploy data-driven decisions regarding their industrial processes.

Real Time - Relating to a system in which input data is processed within milliseconds so that it is available virtually immediately as feedback to the process from which it is coming, e.g. alerts in a self-driving car.