Review

Securing the Sustainable Future of Manufacturing: Analysis of IoT Retrofit Challenges and Solutions

Seyedmostafa Safavi , Zarina Shukur , Muhammad Ehsan Rana * , Umi Asma Mokhtar , Khairul Azmi Abu Bakar , Nizmar b. Mohd Nazar , Farzana Iasmin Rumpa

Posted Date: 25 October 2024

doi: 10.20944/preprints202410.2045.v1

Keywords: Internet of Things; Retrofitting; Manufacturing Environment; IoT framework; Literature Review

 doi:10.20944/preprints202410.2045.v1

Review

Securing the Sustainable Future of Manufacturing: Analysis of IoT Retrofit Challenges and Solutions

Seyedmostafa Safavi [1], Zarina Shukur [2], Muhammad Ehsan Rana [1,*], Umi Asma Mokhtar [2], Khairul Azmi Abu Bakar [2] and Nizmar b.Mohd Nazar [3] nad Farzana Iasmin Rumpa [2]

[1] School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
[2] Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 4300 Bangi, Malaysia
[3] Malaysia Automotive Robotics and IoT Institute, 63000 Cyberjaya, Selangor; nizmar@marii.my
* Correspondence: muhd_ehsanrana@apu.edu.my

Abstract: The Internet of Things (IoT) is revolutionizing manufacturing, serving as a digital makeover tool that collects essential production data. The transition to IoT generates vast data volumes, requiring robust storage and system architecture. Cloud computing steps in here, accommodating these needs with ease. In this setup, a network of sensors across a manufacturing unit captures valuable data, which is transmitted to the cloud. Specialized software then transforms this data into operational performance insights. This digital integration can elevate a manufacturing business, coalescing with existing systems to deliver remarkable results. As the IoT gains popularity, digital manufacturing is poised to soar. However, security has become a paramount concern, especially for retrofitted IoT devices operating with limited human intervention. Researchers have proposed various solutions for IoT security issues. In this study, we conduct a literature review (LR) to identify the security requirements for retrofitting IoT devices in manufacturing. Our goal is to provide a straightforward roadmap for industry stakeholders, highlighting the most suitable security solutions for their retrofitted IoT systems. Our review focuses on scientific papers from the past four years, specifically addressing the security and simplicity of retrofitted IoT architecture in manufacturing. The overarching aim is to define the security needs for IoT retrofitted devices in manufacturing, facilitating the smooth integration of process data into cloud platforms.

Keywords: Internet of Things; retrofitting; manufacturing environment; IoT framework; Literature review

1. Introduction

The natural and virtual worlds are increasing and closely rising to build the Internet of Things (IoT). In truth, the IoT inspired factories and governments to begin an evolutionary journey to Industry 4.0, the fourth industrial revolution [1]. IoT equipment is powered by low-cost chips provided by semiconductor manufacturers such as Renessa, STMicroelectronics, NXP, Silicon Labs, etc. As the manufacturing system is growing, it isn't easy to fulfil all the requirements of the manufacturing control system. The success of manufacturing depends on the power-efficient, cost-effective analysis, collection, and secure exchange of quality data. To improve productivity, manufacturing by embedded IoT devices is becoming popular. However, attempts to retrofit IoT devices in the existing system make it hard to ensure the security system of embedded devices due to the ignorance of cyber threats. IoT manufacturing systems developed IoT without security to produce more IoT devices; as a result, it introduces vulnerabilities to other manufacturing systems due to inadequate protection and policies.

In the last ten years, both challenges and solutions in IoT security have significantly matured. Previous works traditionally focused on securing IoT systems using a perimeter-based security approach, which provided protection to devices from isolated threats. However, with the increased technological advancement and the application of IoT into complex manufacturing systems, a more layered and integrated approach toward security has become highly necessary. Present-day research emphasizes data encryption, multi-factor authentication, and advanced monitoring systems that can

 doi:10.20944/preprints202410.2045.v1

take care of threats as they come along and is pointing toward more proactive and adaptive security solutions. By reviewing the evolution of these methodologies, this paper aims to deliver an in-depth insight into the ways in which IoT retrofitting security has changed over time to meet the expanding needs of Industry 4.0. Through all network connections, attackers can launch attacks on manufacturing companies at the device [2], communication, and the cloud level.

The consequence of having a simple and economical IoT device is that for the last five to ten years, hundreds of millions of IoT devices have been sitting on the internet, unpatched and vulnerable, which hackers and criminals have begun to attack. There are no effective, low-cost solutions known to protect vulnerable devices. In the past few years, researchers have investigated alternative safety architectures for low-end networked applications [3]. To gain useful information, the attacker attempts to catch traffic at various points of the transmission, such as the hardware information in analyzing the network traffic [4]. IoT consists of physical objects, sensors, software, and other technology, which helps to connect and exchange data with other devices over the Internet [51]. For example, wearable health monitors, smart security systems, Smart fire alarms, etc. IoT security demands many levels of abstraction and several dimensions. The levels of abstraction range from the physical layers of sensors, computing and communication, and computers to the semantic layer in which all information collected is interpreted and processed [5]. When these sensors are linked, the data obtained by the sensor must be exchanged or sent to the cloud-based data centre for further processing [6]. Message Queue Telemetry Transport is one of the common application layer protocols in the IoT world simply called MQTT. It provides a good basic security feature. However, this method of authentication can face many problems; it may be easier for passive attackers to connect [7,50].

This paper aims to discuss the security requirement of IoT retrofitted devices in the manufacturing environment to acquire and integrate process data into the cloud platform. This security requirement helps secure the manufacturing environment's data against cyber threats during communication with IoT devices and the cloud. Furthermore, it will provide a custom solution designed to meet the memory and performance of Low-end IoT devices. This paper reviews IoT security requirements and solutions, current retrofitting IoT infrastructure in the manufacturing sector and IoT framework architectures with this goal in mind. To achieve this goal, the following contributions have been mentioned:

- Representing a comprehensive review of security requirements of IoT device approaches in the manufacturing environment.
- We are providing a comparison of the domain, architecture, requirements, and solution of chosen papers.
- Illustrating the architecture of IoT frameworks in the context of IoT security and IoT retrofitting.
- Proposing secure IoT Retrofitting System Architecture for Manufacturing Environment.

2. Background

The background is going to represent a short explanation of relevant studies we assessed in security & retrofitting of IoT devices in the manufacturing environment; the evaluation factors are introduced in the reviewed studies.

2.1. IoT Security

In today's research community, the Internet of Things (IoT) is the most discussed paradigm. The Internet of Things (IoT) is rapidly expanding into a variety of applications, including building and home automation, smart transportation systems, wearable devices for healthcare, industrial process control and manufacturing. Several studies have reported that IoT networks face a variety of security issues, including authentication, authorization, information leakage, privacy, verification, tampering, jamming, and eavesdropping. IoT device integration with various technologies and devices creates interoperability with the components in IoT architecture: device layer, communication layer, and application layer. As a result, security measures should be implemented in combination with an analysis of threats and vulnerabilities at each layer [8].

Recent advancements in IIoT security have been analyzed, highlighting how the integration of 5G, AI, and cloud technologies has transformed security protocols in smart manufacturing

 doi:10.20944/preprints202410.2045.v1

environments. This analysis underscores the necessity for enhanced security measures to address the sophisticated challenges faced today [48].

2.1.1. IoT Retrofitting

The concept of Industry 4.0 was born in Germany in 2011 as part of a modernization strategy. Since then, numerous studies have been conducted in the quest for increased productivity and increased competitiveness in the global market. Industry faces a huge challenge to migrate into Industry 4.0. With the help of the IoT retrofitting concept, which is the reuse of old equipment and the integration of IoT technologies, migration becomes less costly and more insightful [9].

2.1.2. Security in IoT Architecture

In determining security for a retrofitted IoT device or applications, IoT architecture plays an important role. Because the security of the retrofitting process depends on the joint and various properties like IoT architecture and communication between them[10]. Most developers consider two types of IoT architecture; three-layered and the other is five-layered. The well-known IoT structure is divided into three layers; device layer, communication layer, and application layer. Each layer has its security requirements. The most generic way is to focus security on the communication layer (Figure 1). However, there is an enormous scope for the development of IoT security, such as hardware security, communication, and application security as seen in Figure 1.

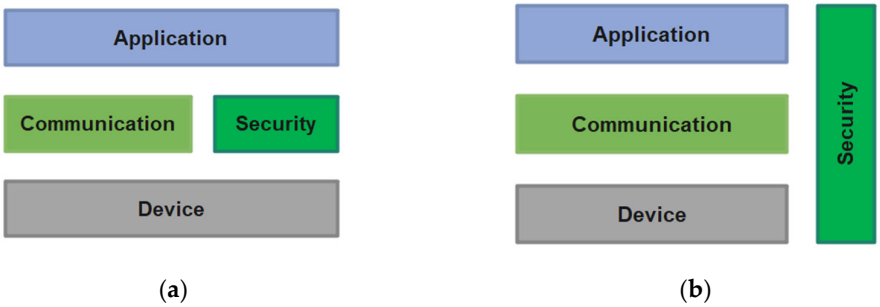

Figure 1. (**a**) The three-layer architecture of IoT [11]; (**b**) The three-layer architecture with its security.

In synthesizing the reviewed literature, Table 1 compares different IoT security protocols and retrofitting strategies based on criteria such as implementation costs, effectiveness of security, scalability, and ease of integration. This comparison highlights the trade-offs faced by manufacturers in choosing IoT solutions to retrofit, thereby emphasizing the need for a protocol selection process that closely aligns with specific operational needs.

Table 1.

Study / Protocol	Security Protocol	Implementation Cost	Integration Level	Scalability	Security Level
Study A [48] (5G)	5G	High	High	High	Strong
Study B [4] (AI)	AI-driven Monitoring	Medium	Medium	High	Strong
Study C [49] (Blockchain)	Blockchain	High	Low	Medium	Strong
Study D [33] (MQTT)	MQTT	Low	High	Medium	Moderate
Study E [46] (CoAP)	CoAP	Low	Medium	Low	Moderate

 doi:10.20944/preprints202410.2045.v1

2.1.3. Integration of Emerging Technologies for IoT Security in Industry 4.0

Some of the recent developments in 5G, AI, and blockchain have critically improved the security of IoT systems in Industry 4.0 environments. For instance, 5G technology enables low latency and high-bandwidth communication that is essential in IoT systems requiring real-time data transfer in manufacturing settings. The utilization of 5G has not only improved connectivity but has also allowed for secure network slicing, thereby reducing the risk of unauthorized access.

IoT monitoring increasingly relies on AI-driven threat detection. Machine learning algorithms can identify and take action on anomalies in real-time, blunting potential cyber threats before they impact operations. For example, AI-enabled predictive maintenance enables constant monitoring of device health, which reduces operational downtime and heads off potential vulnerabilities that could be leveraged in an attack.

The security of IoT is further enhanced with blockchain technology by offering a decentralized approach toward integrity and validation of data and transactions. Researchers have shown how blockchain can be applied to IoT retrofitting for enhanced transparency, immutability of data, and secure communication. In manufacturing, blockchain-based solutions ensure that data across retrofitted IoT devices remain secure and auditable, which is crucial to be able to maintain confidence in automated industrial environments.

2.2. Related Works

The Internet of Things (IoT) opens up ways to exchange and communicate data on the Internet for wearable devices, home appliances, and applications. Innovative home Internet of Things (IoT) gadgets such as cameras, plugs, and doorbells are increasingly being utilized to improve the quality of daily living. Although customers appreciate the functionality that smart home devices offer, these devices' security and privacy aspects have been poorly built from the beginning. In this case, the consumer can face safety, privacy, and security issues at their own home. More sophisticated cyber-security architecture is needed in homes. The impacts of IoT failures can be severe, so IoT studies and research on security issues are of extreme importance. IoT protection is mainly aimed at maintaining privacy, and confidentiality, ensuring the security of IoT users, infrastructures, data, and devices, and ensuring the availability of IoT ecosystem services.

The authors in [1] proposed a mitigation framework that discovers several previously unreported vulnerabilities in some devices like video doorbells, pet feeders, home cameras, and switches. The authors find that some devices use insecure DNS communications, which can be subjected to an MITM attack. A proper encryption method is needed against MITM attacks. IoT attacks can occur in terms of their layer, such as the perception layer, gateway layer, and cloud layer. Navod Neranjan Thilakarathne [12] has tried to summarize IoT security issues in words of primary information security concepts confidentiality, integrity, and availability with regards to its architecture in his article. To improve IoT security, we can take some action, for example, using security credentials, Hashing techniques, encryption mechanisms, and digital signatures.

Study [3] describes eight common attacks targeting IoT devices on the physical layer itself. They suggest potential mitigation strategies as well. Some of their methods are using the chain of trust, a lightweight cryptographic encryption technique, two-factor authentication, etc.

A study of [4] has discussed a detailed survey of IoT security solutions. Their paper has discussed issues related to the sensing layer, network layer, middleware layer, gateways, and application layer. They have drawn the solution with blockchain-based solutions, fog computing, machine learning, and edge computing solutions. Another research [5] also suggested using blockchain, fog computing, machine learning, and edge computing techniques as a solution for securing IoT applications. IoT contains lots of information, and consumers primarily manufacturing need to store it in the cloud for further analysis. There are specific security issues that the manufacturing can face during the transfer of data to the cloud.

Authors of [6] suggest that data transfer from the industrial unit to the cloud needs to be fully secured. Several IoT frameworks have been launched to make IoT maintenance. The selected set of IoT platforms includes AWS IoT from Amazon, ARM Bed from ARM and other partners, Azure IoT Suite from Microsoft, Brillo/Weave from Google, Calvin from Ericsson, HomeKit from Apple, Kura from Eclipse, and SmartThings from Samsung, which helps to secure IoT data in the cloud [7].

 doi:10.20944/preprints202410.2045.v1

The authors in [13] proposed an architecture to integrate the whole system with AWS IoT by classifying two, layer-device and an integration layer as Figure 3 shows. Hardware is retrofitted with various sensors to process data and transfer data through LoRa technology. OPC UA works as a middleware to provide platform-independent and service-oriented architecture. AWS Greengrass helps to interact with Raspberry Pi and AWS IoT core. Data can be analyzed in AWS IoT core for forecast learning and predictive analysis.

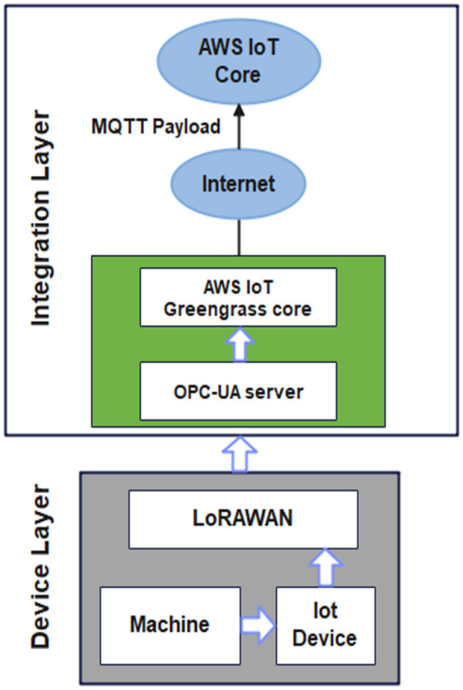

Figure 2. Illustration of how IoT devices can be retrofitted in a manufacturing environment [13].

Also, the authors in [14] proposed a system where an energy sensor was installed with a 20-year-old CNC mill. This sensor sends data using ZigBee to Smart Link. This smart link sends data to the IoT gateway by using Modbus message protocols under TCP/IP. IoT gateway collects all data and sends it to two cloud infrastructures; one is MindSphere Cloud which uses MQTT, and another one is GRV Cloud which uses HTTP in Figure 3.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 25 October 2024 doi:10.20944/preprints202410.2045.v1

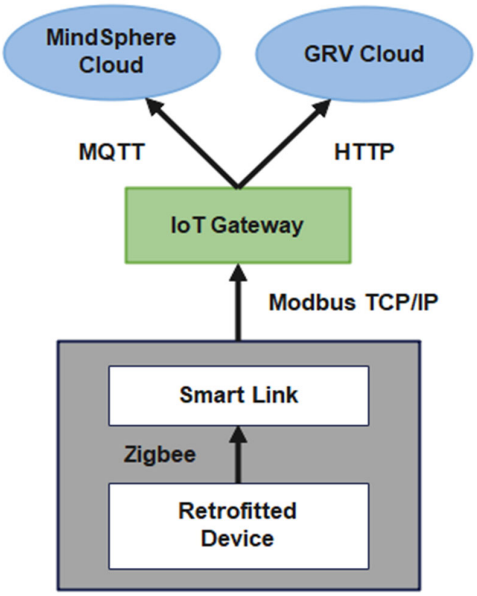

Figure 3. Illustration of how IoT Energy Retrofit device in Industry 4.0 [15].

2.3 IoT Architecture of 5 Popular Frameworks

There are a range of available IoT clouds, such as Azure, AWS, Alibaba, IBM, and Google. Let's get an overview of some IoT frameworks to see how they handle their security.

To optimize the best security in the IoT development framework, Microsoft divided IoT architecture into three layers. These layers are the device, field gateway, cloud gateway, and services as seen in Figure 4. Each layer makes data/information transition from one source to another. During the transition, data/information could be subjected to various attacks such as spoofing, tampering, repudiation, information disclosure, and denial of service of attack. Each layer has its data, authentication, and authorization requirements. The device layer authenticates the device using Transport Layer Security (TLS) or IPSec. Field gateway implements TLS RSA/PSK, IPSec, and RFC 4279 to establish itself as to cloud gateway. On the communication path field gateway and cloud, the gateway implements security on a protocol level (MQTT/AMQP/HTTP/CoAP). Microsoft uses Azure storage service encryption to encrypt data in storage automatically. It also uses Transparent Data Encryption to perform real-time encryption and decryption of the database, backups, and transaction log files.

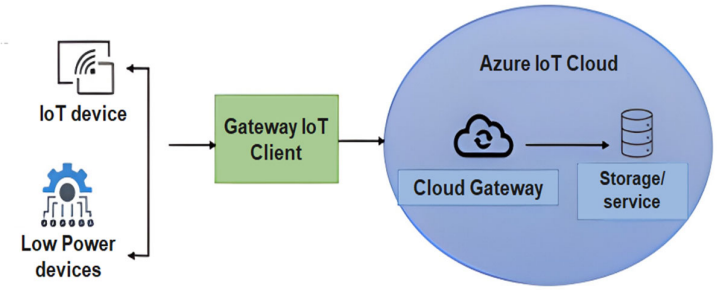

Figure 4. Microsoft Azure IoT Cloud.

AWS IoT provides three layers of services that help to connect IoT devices to other devices and the AWS cloud as seen in Figure 5. First, AWS IoT offers open-source client libraries and application SDKs for various embedded operating systems and microcontroller platforms for the device layer. If an IoT computer can be configured using one of the programming mentioned above languages (C, Node.js), it can bind to the AWS IoT cloud. Second, AWS IoT core connectivity service provides

 doi:10.20944/preprints202410.2045.v1

secure communication with IoT devices and AWS IoT in the communication layer. AWS uses X.509 certificates secure protocols to ensure the security of Device communication. Third, the AWS device gateway supports MQTT, HTTPS, and Web Sockets protocol to provide a secure mechanism for device and AWS IoT applications. In the application layer, data gets stored in AWS RDS DB and DynamoDB. During the transition, data is encrypted using TLS, and the rest of the data is encrypted using AWS-owned keys.

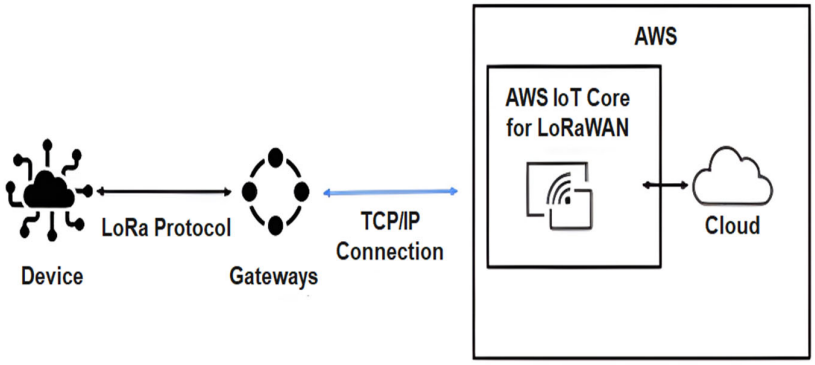

Figure 5. AWS IoT cloud platform.

Alibaba offers a device layer, IoT edge layer (connection layer), and Application layer, which is Alibaba cloud IoT as illustrated in Figure 6. Alibaba Cloud IoT Platform has a multi-layered security strategy to ensure communication between devices and the cloud. For each device, the IoT Platform assigns a Device Name that is unique within the same product. The IoT Platform may be directly accessed by devices via a gateway linked to the IoT Platform as sub-devices. In the communication layer, Edge Gateway uses a lightweight encryption channel, LoRa key security, while transiting data to the Alibaba cloud platform. In the application layer, Alibaba Cloud uses PKI certificate management, trusted service management, trusted device authentication, and key management and distribution services to secure data.

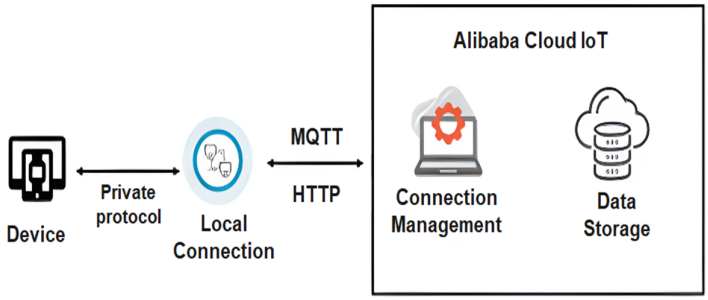

Figure 6. Alibaba IoT cloud.

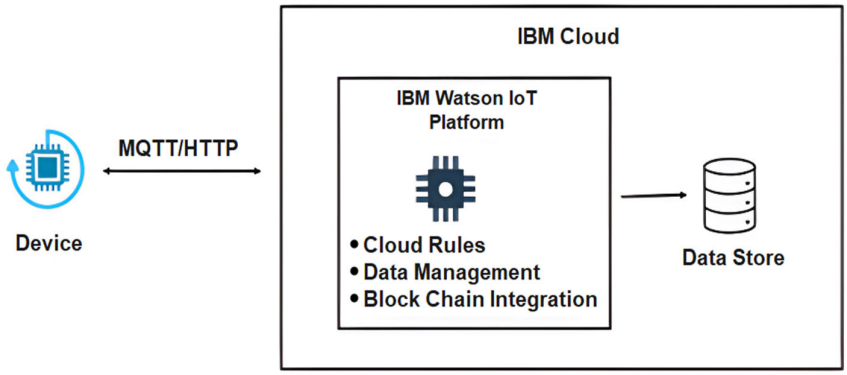

Figure 7. IBM Watson cloud platform.

 doi:10.20944/preprints202410.2045.v1

IBM Watson IoT platform adopts a three-layered architecture, including the device layer, the edge layer, which is the communication layer, and the cloud layer, which is the application layer as illustrated in Figure 6. Wireless protocols like Bluetooth, Zigbee, Wifi, cellular, and RFID, as well as over-the-wire protocols like Ethernet, are used to transmit data from the device layer to the communication layer. IBM Watson IoT platform connects devices, networks, and gateways through a system that uses MQTT and HTTPS open standard-based communication. IoT gateway provides limited device management and registration capabilities. During communication from the IoT gateway to the cloud platform, it uses MQTT or HTTPS over TLS. Communication is secured by a security authorization token too. In the Application layer, cloud Data remains encrypted using AES 256-bit encryption.

Google IoT Core is a fully managed service that allows connecting, managing and ingesting data from millions of devices easily and securely. Google divides the IoT platform into three basic layers: device, gateway, and cloud as illustrated in Figure 8. In device, layer devices can connect to the internet either directly or indirectly. Using a gateway, devices that aren't directly connected to the internet can access cloud services in the communication layer. An IoT gateway system provides communication and translation between devices and the cloud. Data is stored in the cloud in the application layer, which is sent over through MQTT or HTTP protocol from the gateway. Google IoT core supports MQTT and HTTP protocol so that developers can use the existing device with minimal changes and connect all devices, gateways, and Google Cloud.

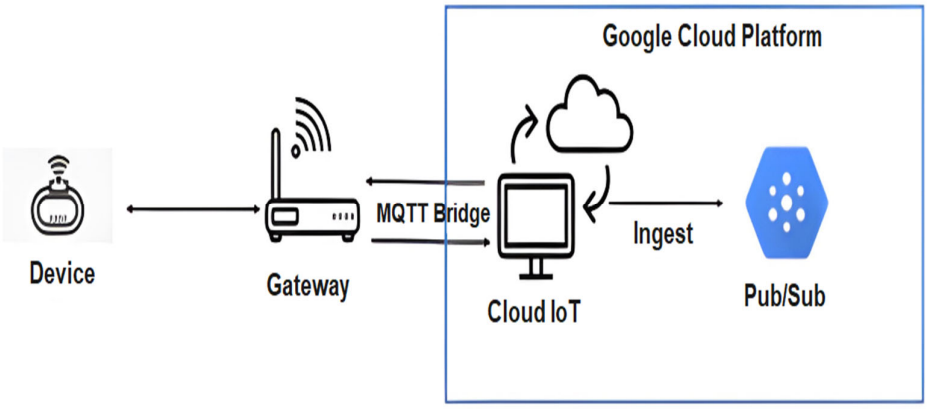

Figure 8. Google IoT cloud core.

2.4. Popular Open-Source IoT Frameworks

In this section, we find out the popular open-source IoT framework by using a Google search engine. We use the keyword "popular open-source IoT framework" for searching purposes. We refer first two pages of Google excluding the ad page. The popular frameworks we find out are listed below in Table 2. There are a range of available IoT clouds, such as Azure, AWS, Alibaba, IBM, and Google. Let's get an overview of some IoT frameworks to see how they handle their security.

Table 2. Popular open-source IoT frameworks.

WebPages	Open-source IoT framework	Higher frequency framework based on mentioned webpages
www.techtic.com	Kaa IoT, Macchina.io, Zetta ,GE PREDIX,ThingSpeak ,DeviceHive ,Distributed Services Architecture,Eclipse , Open Connectivity Foundation , OpenHAB	Kaa IoT
https://geekflare.com	Zetta ,Arduino OpenRemote ,Node-RED ,Flutter, M2MLabs Mainspring	Zetta

 doi:10.20944/preprints202410.2045.v1

	,ThingsBoard, Kinoma, Kaa IoT Platform ,SiteWhere ,DSA ,Thinger	
https://bitnine.net	Arduino,Devicehub.net,IoTToolkit,Open WSN,Particle,SiteWhere,ThingSpeak,We binos, Zetta	Arduino
www.esparkinfo.com	Kaa IoT, Macchina.io, Zetta ,GE PREDIX,ThingSpeak,DeviceHive,Distrib uted Services Architecture, Eclipse,OpenConnectivity Foundation,OpenHAB, CiscoIoT Cloud Connect,Salesforce, Oracle,SAP,Microsoft Azure, Google Cloud Platform, Hewlett Packard Enterprise, DataV by Bsquare, Mindsphere by Siemens, MBED IoT Device platform, Amazon Web Services [AWS], Mocana,RTI	Kaa IoT
www.iotforall.com	DeviceHive,ThingSpeak,Mainflux,Thinge r.io,Zetta	DeviceHive
iot4beginners.com	Kaa, Zetta, thinger.io, ThingsBoard, DeviceHive, Mainflux, ThingSpeak, myDevices, openremote, WSO2	Kaa
iotdunia.com	Kaa IoT, Macchina.io, Zetta ,GE PREDIX,ThingSpeak,DeviceHive ,Distributed Services Architecture · ,Arduino, Node-RED, Flutter	Kaa
www.yumpu.com	Kaa IoT, Macchina.io, Zetta ,GE PREDIX,ThingSpeak ,DeviceHive ,Distributed Services Architecture, Eclipse, Open Connectivity Foundation,OpenHAB	Kaa
www.record-evolution.de	Open Remote, Things Board, Thinger.io,MainFlux, Arduino	OpenRemote
https://internetofthingsagenda.techtarget.com	Open Remote, Device Hive, The Thing System, Distributed Services Architecture, Node-RED, DeviceHub,Kaa	OpenRemote
https://medium.com	Kaa IoT, Macchina.io, Zetta ,GE PREDIX, ThingSpeak, DeviceHive ,Distributed Services Architecture, Eclipse, Open Connectivity Foundation, OpenHAB	Kaa IoT
www.allerin.com	Kaa,Zetta,DeviceHive, SiteWhere Distributed Services Architecture	DeviceHive

Security Aspects of Top 5 Opensource IoT Framework

A brief explanation of the security aspects provided by the selected frameworks based on Table 2, is as follows;

1. KAA IoT security: KAA provides user authentication, access authorization and server authentication using OAuth 2.0 and keylock.
2. Zetta IoT security: While interacting, Zetta keeps track of security credentials and relevant information. Zetta supports MQTT, and CoAP protocol to ensure the security of the IoT environment.

 doi:10.20944/preprints202410.2045.v1

3. DeviceHive security: DeviceHive security is safe by design. The platform is built using modern security techniques. JSON Web Tokens are used to secure DeviceHive authentication (JWT). It supports MQTT protocol and custom firmware as well.
4. Aurdino IoT platform security: Arduino is very aware of the dangers of hacking and is continuously working to improve security in both its hardware and software. Customization users may utilize the Arduino libraries, which include HTTP, MQTT, X.509, and JSON support, to connect to any web service they choose.
5. OpenRemote Security: HTTP and MQTT are examples of standard protocols supported by the OpenRemote platform. OpenRemote protects all assets and keeps stored data fully secured in both cloud and on-premise platforms.

3. Methodology

This research is based on a literature review to comprehensively understand and summarize the current landscape of IoT security requirements and solutions. The literature review method, in general, consists of a statement and research on a specific issue [16]. Our literature review is divided into six stages to facilitate the completion of the proposed SLR study; (i) Planning; (ii) Research questions (iii) Search process (iv) Inclusion and exclusion criteria (v) Data collection (vi) Final selection. This type of research allows for discovering research trends, raising essential topics and genuine concerns, and identifying research opportunities in less-explored areas.

3.1. Planning

In the planning stage, the primary focus is to establish the research objectives, which are:

To understand the current state of IoT security requirements and solutions.

To propose a secure retrofit IoT system architecture that can be employed in a manufacturing environment.

In alignment with these objectives, specific research questions were formulated to guide the review process.

3.2. Research Questions

The research questions for the current literature review (LR) study are provided in this section. Four research questions (RQs) are given to discuss comparable difficulties and associated concepts, as this study leads us to develop a comprehensive answer to the manufacturing environment. A literature review (LR) discovers, selects, and critically evaluates research. This method will be used to address the following research questions.

RQ1: How are the architectures to integrate IoT?

RQ2: What are the security requirements and solutions in terms of securing IoT devices?

3.3. Search Process

This section discusses how each article for this study was identified. Some specified electronic databases were evaluated and consulted to extract relevant studies on the security of IoT devices, and IoT retrofitting approaches. We intend to represent the technique of selecting papers and the search process based on the SLR approaches, including keyword searching, research paper titles, and the quality of the publishers, as shown below. The following strings are obtained by searching the below phrases and their synonyms for the essential components [16].

(“IoT” OR “Internet of things”) AND “security” AND “requirements” AND (“manufacturing” OR “Industry”)

Searching academic databases, which are referenced in this work, is the most frequent approach to obtaining legitimate papers in every area. It is assumed that these articles have covered books. As a result, no books representing the topic have been searched. Table 3 lists the most essential databases for the study topic. The study needs to exclude IEEE publications from the ACM digital library to do a better analysis of the papers.

 doi:10.20944/preprints202410.2045.v1

Table 3. Searched databases.

Database	URL
IEEE Xplore	http://ieeexplore.ieee.org
ACM digital library	http://dl.acm.org
Wiley	https://onlinelibrary.wiley.com
Taylor & Francis	https://www.tandfonline.com
Sage	https://journals.sagepub.com

3.4. Inclusion and Exclusion Criteria

Following the initial selection of studies from the database search, the subsequent phase filters the retrieved studies and chooses the relevant ones for a more in-depth analysis. According to the SLR methodology outlined in [18], guidelines for choosing relevant research must be established. Mainly, a set of inclusion/exclusion criteria must be defined. Our inclusion/exclusion criteria are discussed in Table 4.

Table 4. Inclusion and exclusion criteria.

Inclusion Criteria	Articles are related to IoT security in manufacturing Article content applicable to research questions. The article must report either architecture or security of IoT devices nor both. Articles should be review, survey or original article which contains in-depth literature review.
Exclusion Criteria	Articles not focusing on security of IoT device or manufacturing. Articles are out of the scope of this study. Articles were published before 2018.

3.5. Data Collection

Table 5 illustrates the process of data collection. The initial stage of data collection involves extensive literature search and review. Initially, a systematic search was performed on various databases over three months from January to March 2023. This search utilized specific keywords and search strings to yield precise results related to the scope of our study.

Once the articles were identified, we applied pre-defined inclusion and exclusion criteria to select the most relevant and recent contributions in the domain of IoT security. Particularly, articles published before 2018 were excluded to maintain a focus on the latest advancements.

Following this, the remaining articles were scrutinized in more detail. Each article was reviewed for its relevance to our research questions and its overall quality. Specifically, the quality of each article was assessed using a predefined set of criteria to ensure the integrity of our review process.

Out of the initial pool of 134 articles, only 45 were chosen for the final review. These selected articles not only met the relevance and quality criteria but also contributed significantly to the IoT security domain.

Table 5. Data collection process.

Keywords	Delimitation Criteria	Database/ Journal/ Conference	Hits	Selection after reading title
"IoT AND security AND requirements AND manufacturing" OR "IoT AND security AND requirements AND industry"	Language: English Document Type: Conference & journals (Related to Computer science, IT & cyber security)	Sage	14	7
		Wiley	42	7
		Taylor & Francis	9	5
		ACM	69	17
		IEEE	44	10

 doi:10.20944/preprints202410.2045.v1

OR "Internet of Things AND security AND requirements AND manufacturing" OR "Internet of Things AND security AND requirements AND industry"	Advanced search based on keywords, abstract & Publication year :2018 to 2024			

3.6. Final Selection

After evaluating and analyzing the primary studies, to conduct a more comprehensive and accurate analysis we eventually selected fourteen articles as our final research according to the entire text and the quality of the review. These fourteen articles were also chosen based on inclusion/exclusion criteria. All of the articles and citations were managed using Mendeley software. Figure 9 shows how we finally selected our papers for review purposes.

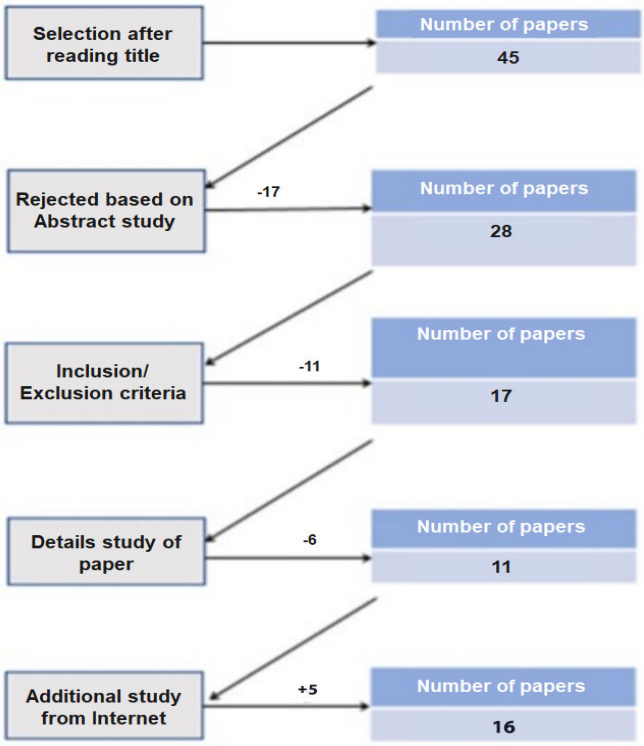

Figure 9. Final Selection Criteria.

4. Security Requirements and Solutions in IoT

In this section, we provide a detailed analysis of the publications selected for the final review. We discuss the common security requirements identified in IoT systems and the proposed solutions to address these requirements. Each selected publication is critically reviewed to understand its contribution to the field. These 16 chosen papers cover research from 2018 to 2024 as shown in Figure 11. This figure also shows there is some redundancy in terms of article coverage year. Furthermore, the type & domain of the research paper, implemented IoT architecture, security requirements and solutions are explained. Considering our efforts in reviewing papers, we found out researchers are implementing almost the same architecture to implement IoT communication and they face common security requirements but provided security solutions are different. The provided categorization scheme's overview, as well as their area, are presented in Table 6.

 doi:10.20944/preprints202410.2045.v1

Table 6. Review of the Selected Paper in the combination of security requirement and architecture.

Publisher Year Author	Title	Domain	Type	Architecture	Requirement	Solutions
Willey 2019 Fadi Al-Turjman et al [19].	An overview of security and privacy in smart cities' IoT communications	Non-manufacture	Review	Physical layer, Network layer, Database layer, virtualization layer, Data analytics and mining layer, Application layer	data privacy, integrity, confidentiality and availability	black networks (BNs), trusted software-defined networking (SDN) controller named as TTP, unified registry (UR), and key management system (KMS)
Willey 2020 Samundra Deep et al [20].	A survey of security and privacy issues in the Internet of Things from the layered context	General	Survey	Perception layer, Network layer, Middleware layer, Application layer	data privacy, integrity, confidentiality, availability	data encryption, key management scheme and lightweight cryptographic algorithms
Willey 2020 Gupta et al [22].	An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols	General	Review	Perception Layer, Transmission Layer, and Application Layer.	confidentiality, integrity, and user privacy. Trust Management	Trust management
Sagepub 2019 Trung Dong Mai [23]	Research on Internet of Things security architecture based on fog computing	General	Research Article	Perceptual layer, Transport layer, Processing layer, Application layer	data traceability, integrity, identity authentication, credibility management, confidentiality, and privacy protection	Light weight encryption method
Sagepub 2020 Liu et al [24].	A new model of industrial internet of things with security mechanism—An application in complex workshop of diesel engine	Industry	Research Article	data acquisition layer, data access layer, data processing layer, data transfer layer, network layer, and data application layer	user access system and the reliability and integrity of data transmission	security transmission mechanism at all levels
Sagepub 2019 Aydos et al [25].	Assessing risks and threats with layered approach to Internet of Things security	General	Research Article	Perception layer, Network layer, Data processing layer ,Application layer	integrity, accessibility and privacy	risk-based IoT security model

 doi:10.20944/preprints202410.2045.v1

ACM 2020 Selimis et al [26].	RESCURE: A security solution for IoT life cycle	General	Research Article	Device layer, Cloud layer	Authentication, Privacy, Integrity	SRAM-PUF
ACM 2020 Tange et al [27].	Towards a systematic survey of industrial IoT security requirements: research method and quantitative analysis	Manufacturing	Survey	N/A	CIA Triad, Authentication, Access control,Network Security, Data security	MQTT, Key distribution,.Fingerprint
Taylor & Francis 2018 Mendez Mena et al [28].	Internet of things: Survey on security	General	Survey	Perception layer, Network layer, Application layer	attack resiliency, authentication, access control, client Privacy	Encryption scheme, key distribution mechanism, privacy policy
IEEE 2020 Iqbal et al [29].	An In-Depth Analysis of IoT Security Requirements , Challenges and their Countermeasures via Software Defined Security	General	Review	Perception layer, Network layer, Application layer	availability, confidentiality, integrity, non-repudiation, privacy and authentication	Multi firewalls and hypervisors integration solution, VArmour DSS ,Deception Virtual Security Framework, OneControl, DefenseFlow
IEEE 2020 Sharma et al[30].	Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey	General	survey	Physical layer, Data Link layer, Network layer, Transport layer, Application layer	Security,privacy,trust	Access control, Quick identification and release of patches, Credential management, Firmware security, Device policy compliance, Script disabling, Continuous application security
IEEE 2020 Ebo et al [31].	An Enhanced Secured IOT Model for Enterprise Architecture	SME	Research Article	Perception Layer, Network Layer, Processing Layer, Application Layer, Service Management Layer	authentication, authorization, access control, and non-repudiation	Enterprise's IoT framework
IEEE 2021 Serror et al[32].	Challenges and Opportunities in Securing the Industrial Internet of Things	Industry	Survey	Perception layer, Network layer, Application layer	key management, user/device authentication, access control, and privacy preservation	Public-key mechanism,fingerprinting, rules& policiees for access control & encrypted data

 doi:10.20944/preprints202410.2045.v1

IEEE 2024 Kim et al[48].	Analysis of Recent IIoT Security Technology Trends in a Smart Factory Environment	Smart Manufacturing	Research Article	Integration of 5G, AI, and cloud technologies with operational technology.	Enhanced security for interconnected systems in smart factories, focusing on operational reliability and data integrity.	Implementation of advanced monitoring systems and real-time data analytics to detect and mitigate threats.
MDPI 2024 Juma et al[49].	Securing Big Data Integrity for Industrial IoT in Smart Manufacturing Based on the Trusted Consortium Blockchain (TCB)	Smart Manufacturing	Research Article	Trusted Consortium Blockchain (TCB) architecture with hyperledger fabric modular.	Integrity of big data across IoT devices and platforms in smart manufacturing, with a focus on real-time transaction monitoring and peer validation.	Blockchain-driven data validation and encryption methods to ensure data security and integrity, supporting high transaction throughput and low latency.

5. Retrofitted IoT System Architecture in Manufacturing Environment

This section details the structure of the IoT system architecture, explaining how the device, communication, and application layers interact with each other. By understanding the mechanics of the system, we can better identify potential security vulnerabilities. Retrofitting approaches in a manufacturing environment with IoT devices require a device layer, communication layer, and application layer as illustrated in Figure 10. The device part typically consists of a retrofitted device, a local wireless connection, and an IoT gateway.

These IoT gateways allow fast and easy access to the IoT device, and they are compatible with IoT clouds. For large data packages, cloud computing is a simple way to travel. It is a two-way exchange of data between a computer and a remote service over the Internet. A connection to the Internet Protocol (IP) network is created by an IoT computer and then hooked up to the cloud. To communicate and link with each other, the large quantities of data generated by IoT devices need extreme efficiency. IoT in the cloud offers the connectivity required to exchange information between devices and make sense of it at a faster pace. There are a range of available IoT clouds, such as Azure, AWS, Alibaba, IBM, and Google, which we have discussed in the previous section.

 doi:10.20944/preprints202410.2045.v1

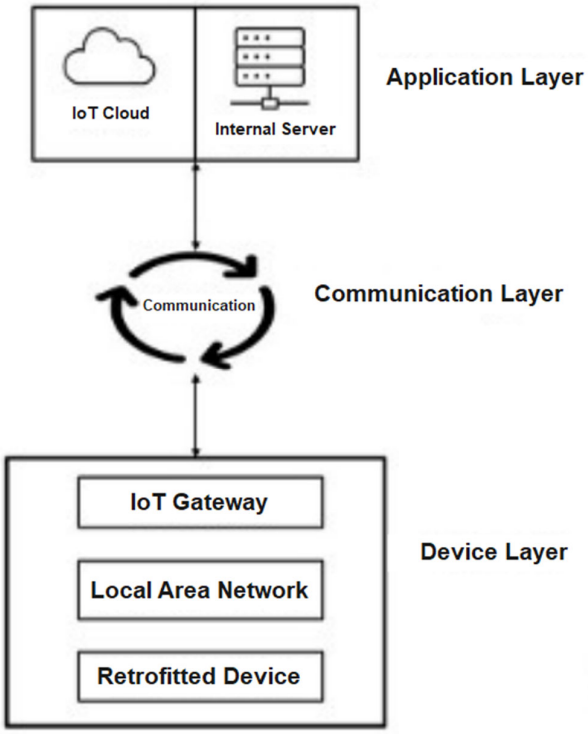

Figure 10. General IoT System Architecture.

5.1. Device Layer

As mentioned in Section 2, the individual machine plays a different significant role in retrofitting. As many low-cost devices are available, we assume the IoT system in the manufacturing environment should be built with this low-cost IoT device. The device should be powerful and capable of interacting with other devices in terms of communication. The device layer identifies objects, gathers data, and collects data from surrounding environments.

IoT devices use a gateway to communicate with external networks. Table 7 presents the connections between IoT devices and gateways through local area networks such as Wi-Fi, ZigBee, Bluetooth, LoRAWAN, etc.

Table 7. Comparison of Local Area Networks.

Local Area Networks	Pros	Cons
Wi-Fi	S.Habibah [33] et al mentioned in their paper that Wi-Fi is a secure choice for communication. Wi-Fi protocol includes two security features which are Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access(WPA).	Wi-Fi needs more energy than other communication technology which makes it undesirable[34].
ZigBee	Zigbee is a wireless network for consumer electronics devices that is meant to be simple and low-cost[35].	Mendez Mena et al [28] mentioned that there are threats in Zigbee-enabled systems include traffic sniffing (eavesdropping), packet decoding, and data manipulation/injection.
Bluetooth	Bluetooth Low Energy protocol is a short-range communication technology that saves a lot of energy [36]. There are four different access security modes available with Bluetooth which ensures privacy, authenticity and integrity of endpoint data [35].	Bluetooth may face issue to communicate to a long distance IoT node[37].

 doi:10.20944/preprints202410.2045.v1

LorRAWAN	The LoRaWAN protocol offers a number of benefits in IoT applications, including low cost, low power, security, and ease of implementation [38]. Additionally, LoRaWAN provides two -layer security which provides confidentiality, integrity and authenticity [39]	There are weaknesses of LoRaWAN v1.0 such as the bit-flipping attack, in which an attacker can alter the content of a message over the connection between the network server and the application server [40]

5.2. Communication Layer

The communication layer maintains connectivity, and message routing between the device layer and application layer. It receives information from the device layer and forwards it to the application layer using capabilities such as the Internet. The communication layer enables connectivity using the IoT gateway (which is mentioned in 6.1). The objective of allowing connectivity is to transmit data to the application layer using the Internet. The communication layer enables the developer to establish how IoT messages are sent and received by the device layer and how data is stored in the cloud.

To ensure that all information transmitted over the network is encrypted to outside parties, the developers can use a secure communication protocol such as MQTT, CoAP, AMQP, and DDS [41]. These protocols are used in interaction among IoT devices and cloud infrastructure and are presented in Table 8.

Table 8. Comparison of Communication Protocol.

Communication Protocol	Advantages	Disadvantages
MQTT	MQTT is a low-power, low-bandwidth protocol commonly utilized by IoT devices[42]. It provides data confidentiality, authentication for the security mechanism [28].	MQTT protocol does not provide encrypted connection[28]. In MQTT Authentication is accomplished with a basic username and password combination, which is sent in plaintext [27]. So, according to [43] MQTT offers basic and unsecure communication methods.
CoAP	For communication, CoAP provides data confidentiality and integrity, authentication, non-repudiation, and replay protection [33].	CoAP protocol is running over UDP, and data transmission is not reliable [44]. CoAP only allows four types of messages and the packet size shorter than MQTT.
AMQP	AMQP protocol for the establishment of secure, scalable, and advanced clustering messaging infrastructures over an ideal network [45]	AMQP uses the Simple Authentication and Security Layer (SASL) framework for authentication. Nebbione et al. [46] mentioned on their paper that according to the NVD database, a wide range of vulnerabilities in AMQP-based products and services have been found in the last few years.
DDS	Concerning security DDS supports DDS and TLS for ensuring confidentiality, integrity and authenticity in communication [46]	Michaud et al [47] shared in their paper that sometimes in DDS system, node misconfiguration can be utilized to carry out malicious operations.

5.3. Application Layer

The application layer comprises of application and a server. Popular frameworks, they call it the IoT cloud (Figure 10). IoT cloud server (by Microsoft Azure, IBM Cloud, Amazon AWS, Google Cloud, etc.) is a powerful and cost-effective solution used by built-in applications and custom portals to connect, manage and track information. However, for applications developed without using any framework, the IoT cloud server can be an internal server of that organization.

One of the security measures has already been taken care of if IoT applications are created utilizing existing frameworks such as those listed above. Otherwise, developers need to consider security at the application, database, and server part, such as user access, data security, software security (using SSDLC such as OWASP, MS SDL, NIST 800-64), firewall configuration, etc.

 doi:10.20944/preprints202410.2045.v1

6. Proposed Secure Retrofitted IoT System Architecture in Manufacturing Environment

In this section, the analyzed results from the literature review data are presented. Through evaluating a few studies, we identify that security in IoT is a critical issue in a manufacturing environment. To increase security, we intend to discuss security requirements for retrofitting IoT devices in manufacturing environments. By examining each layer of IoT architecture, this article includes both ease and protection. The paper aims to discuss the security requirement of IoT retrofitted devices in the manufacturing environment to acquire and integrate process data into the cloud platform. The security requirements and solutions we have discussed in this paper can impact IoT devices.

We assume that our IoT environment of manufacturing is located on the same floor or same room because Wi-Fi is efficient among all these networks. Wi-Fi traffic is sent between IoT devices and gateways. In a manufacturing environment, they have primarily IoT devices with low power consumption; as a result, MQTT is the most commonly used protocol between gateways and the cloud because it's a lightweight protocol with a fast response time. In addition, it ensures low bandwidth data transfer as well. As illustrated in Figure 6, the retrofitted device produces a significant volume of data. For successful IoT-driven device implementation, storage capacity is necessary; Cloud computing is one of the architectures which will ease architectural computing and resource demands.

7. Sustainability in IoT-Enabled Manufacturing

7.1. Sustainable IoT Architecture

The integration of IoT in manufacturing not only enhances security and efficiency but also plays a pivotal role in sustainable manufacturing practices. Sustainable IoT architecture focuses on optimizing resource utilisation and minimising waste. By leveraging data collected from IoT sensors, manufacturing units can significantly reduce energy consumption and optimize supply chain management. This approach not only conserves resources but also reduces operational costs, making it a financially viable option for manufacturers. Furthermore, retrofitting existing equipment with IoT devices, as proposed in this paper, extends the lifecycle of machinery, thereby reducing electronic waste and promoting the sustainable use of resources.

7.2 Eco-Friendly Security Solutions

The proposed secure IoT system architecture emphasizes not only the security of IoT devices but also their environmental impact. The use of energy-efficient algorithms and protocols in securing IoT devices contributes to the overall reduction in energy consumption of the manufacturing unit. Moreover, the adoption of cloud-based solutions and edge computing in IoT infrastructure minimizes the need for extensive on-site data centres, which typically consume significant amounts of energy. Additionally, the use of Trusted Consortium Blockchain (TCB) technology has been proposed to ensure the integrity of big data in industrial IoT settings. The approach not only enhances security but also supports sustainable manufacturing practices by reducing energy consumption and optimizing data processing and verification processes [49]. By ensuring that the security solutions are eco-friendly, manufacturers can work towards a greener and more sustainable future, aligning with global environmental goals and standards.

8. Discussion

This extensive literature review has revealed some significant developments and challenges pertinent to IoT security in the context of retrofitting at manufacturing sites. One of the key points emerging from this study is the role of new technologies like 5G, artificial intelligence, and blockchain in meeting complex security requirements within Industry 4.0. Each of these technologies possesses its own strengths and potential weaknesses, further indicating that a tailored approach is needed when retrofitting IoT devices in manufacturing environments.

The study by Kim et al. [48] presents that 5G technology offers prominent scalability and increased security features, largely due to the feature of network slicing, which efficiently isolates the IoT devices from any unauthorized access. However, the high deployment cost associated with 5G

 doi:10.20944/preprints202410.2045.v1

technology can act as a bottleneck for any small or medium-sized enterprise. In not all manufacturing environments, the capital outlay required to implement infrastructure for 5G could thus be justified, and the deployment of 5G is likely to be more feasible in large-scale operations only where the requirement for low latency and high-bandwidth communications is paramount.

Specifically, the integration of AI-driven security, as noted by Hassija et al. [4], forms a remarkable development in view of real-time threat detection and anomaly surveillance. AI lets IoT systems detect and respond to security threats dynamically, allowing for enhanced overall system resilience. This is particularly valuable for predictive maintenance, whereby continuous monitoring can often mitigate vulnerabilities before they emerge. However, like 5G, AI-based systems can require a significant computational overlay and considerable expertise in implementation. Although the price is moderate, the level of integration required for AI would be demanding for legacy systems, where the processing is either not powerful enough or compatible with AI frameworks.

Juma et al. [49] investigated blockchain, one of the promising technologies that would ensure data integrity across IoT networks. Blockchain, being a decentralized system, serves to complement the needs of industrial IoT by preventing tampering with data and offering transaction transparency. The study shows that blockchain technology adds the most value when data permanence is required, as in quality and regulatory compliance in manufacturing [51]. Yet, considering the high costs involved in implementing blockchain and its relatively limited scalability on selected use cases, it would seem that the deployment of blockchain would be preferable in highly specific instances than blanket implementation in all IoT retrofitting applications.

On the other hand, lightweight protocols like MQTT and CoAP provide economically feasible solutions for secure IoT communication (Bhawiyuga et al. [33]; Nebbione & Calzarossa, [46]). It is particularly advantageous for resource-constrained devices because of the low-power, low-bandwidth characteristics of MQTT, thus easily embedding these protocols into existing devices with very minimal hardware changes. CoAP, on the other hand, being equally inexpensive is not as suitable for scaling applications due to constrained message size and reliance on UDP, which reduce reliability. These protocols provide medium security but can be quite easily integrated into systems, hence being practical choices for small-scale manufacturing units or projects on a constrained budget.

The research concludes that while technologies like 5G, AI, and blockchain indeed introduce better security and scalability features, they also come with higher implementation challenges and costs. On the other hand, lightweight protocol alternatives like MQTT and CoAP do seem economic, though at some cost regarding scalability and security. It points out the necessity for a hybrid approach in retrofitting IoT systems at manufacturing levels, therefore allowing manufacturers to select appropriate technologies given specific operational needs, budgetary constraints, and favored security levels. Future studies should, therefore, focus on the formulation of flexible, multi-tier security frameworks that will encapsulate the ideal features of these technologies to realize custom-tailored, cost-effective IoT retrofit options for diverse manufacturing conditions.

9. Conclusion and Future Work

In this research, the information has been gathered by the SLR method. After evaluating our selected articles, we found that several security issues are involved in integrating IoT products with existing systems. This paper presents security requirements for retrofitted IoT devices to operate in a manufacturing environment safely and to prevent security breaches. This discussion would help to reduce the security vulnerabilities of retrofitted IoT-based systems. The proposed IoT system architecture Figure 11 suggests a security-based architecture to incorporate a vast volume of data. Therefore, the proposed architecture can mitigate data breach risks significantly. In the future, the proposed secure IoT system architecture to strengthen security for secure communications can be implemented and hopefully can be easily integrated with the existing practice, as well as existing frameworks.

 doi:10.20944/preprints202410.2045.v1

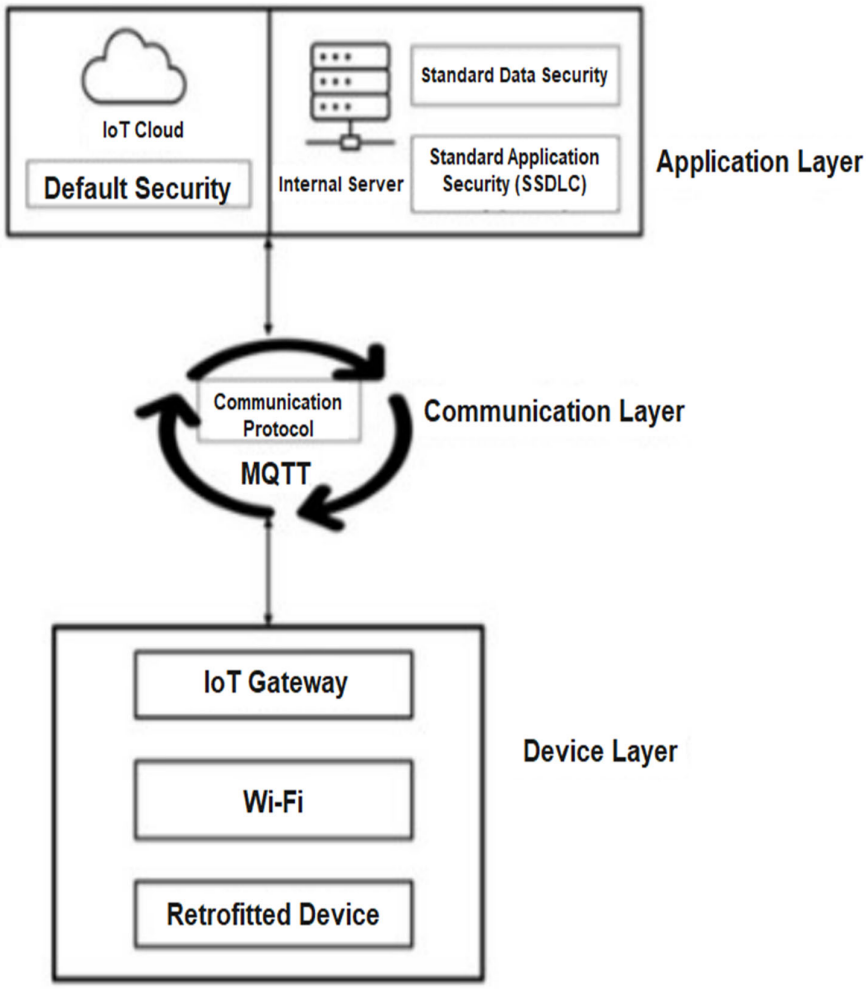

Figure 11. Proposed secure IoT system architecture for a manufacturing environment.

Acknowledgements: The research has been carried out under the program Konsortium Kecemerlangan Penyelidikan (JPT(BKPI)1000/016/018/25 (KKP/2020/UKM-UKM/4/3)) provided by Ministry of Higher Education of Malaysia.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. C. Ye, P.P. Indra, D. Aspinall, Retrofitting Security and Privacy Measures to Smart Home Devices, 2019 6th Int. Conf. Internet Things Syst. Manag. Secur. IOTSMS 2019. (2019) 283–290. https://doi.org/10.1109/IOTSMS48152.2019.8939272.
2. A. Gupta, P. Gupta, J. Chhabra, 07414782, (2015) 285–289.
3. T. Alladi, V. Chamola, B. Sikdar, K.K.R. Choo, Consumer IoT: Security Vulnerability Case Studies and Solutions, IEEE Consum. Electron. Mag. 9 (2020) 17–25. https://doi.org/10.1109/MCE.2019.2953740.
4. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures, IEEE Access. 7 (2019) 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045.
5. I. Ahmad, M.S. Niazy, R.A. Ziar, S. Khan, Survey on IoT: Security Threats and Applications, J. Robot. Control. 2 (2021) 42–46. https://doi.org/10.18196/jrc.2150.
6. N. Santhosh, M. Srinivsan, K. Ragupathy, Internet of Things (IoT) in smart manufacturing, IOP Conf. Ser. Mater. Sci. Eng. 764 (2020). https://doi.org/10.1088/1757-899X/764/1/012025.
7. M. Ammar, G. Russello, B. Crispo, Internet of Things: A survey on the security of IoT frameworks, J. Inf. Secur. Appl. 38 (2018) 8–27. https://doi.org/10.1016/j.jisa.2017.11.002.
8. A.D. Jurcut, P. Ranaweera, L. Xu, Introduction to IoT Security, 2019. https://doi.org/10.1002/9781119471509.w5gref260.

9. T. Lins, R.A.R. Oliveira, L.H.A. Correia, J.S. Silva, Industry 4.0 retrofitting, Brazilian Symp. Comput. Syst. Eng. SBESC. 2018-Novem (2018) 8–15. https://doi.org/10.1109/SBESC.2018.00011.
10. N. Tuptuk, S. Hailes, Security of smart manufacturing systems, J. Manuf. Syst. 47 (2018) 93–106. https://doi.org/10.1016/j.jmsy.2018.04.007.
11. A.M. Mzahm, M.S. Ahmad, A.Y.C. Tang, Enhancing the Internet of Things (IoT) via the Concept of Agent of Things (AoT), J. Netw. Innov. Comput. 2 (2014) 101–110.
12. N.N. Thilakarathne, Security and Privacy Issues in IoT Environment, Int. J. Eng. Manag. Res. 10 (2020) 26–29. https://doi.org/10.31033/ijemr.10.1.5.
13. S.K. Panda, A. Blome, L. Wisniewski, A. Meyer, IoT Retrofitting Approach for the Food Industry, IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA. 2019-Septe (2019) 1639–1642. https://doi.org/10.1109/ETFA.2019.8869093.
14. E.L.C. Macedo, E.A.R. De Oliveira, F.H. Silva, R.R. Mello, F.M.G. Franca, F.C. Delicato, J.F. De Rezende, L.F.M. De Moraes, On the security aspects of Internet of Things: A systematic literature review, J. Commun. Networks. 21 (2019) 444–457. https://doi.org/10.1109/JCN.2019.000048.
15. F. Lima, A.A. Massote, R.F. Maia, IoT Energy Retrofit and the Connection of Legacy Machines Inside the Industry 4.0 Concept, IECON Proc. (Industrial Electron. Conf. 2019-Octob (2019) 5499–5504. https://doi.org/10.1109/IECON.2019.8927799.
16. P. Asghari, A.M. Rahmani, H.H.S. Javadi, Service composition approaches in IoT: A systematic review, J. Netw. Comput. Appl. 120 (2018) 61–77. https://doi.org/10.1016/j.jnca.2018.07.013.
17. K. Maswadi, N.B.A. Ghani, S.B. Hamid, Systematic Literature Review of Smart Home Monitoring Technologies Based on IoT for the Elderly, IEEE Access. 8 (2020) 92244–92261. https://doi.org/10.1109/ACCESS.2020.2992727.
18. B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, S. Linkman, Systematic literature reviews in software engineering - A systematic literature review, Inf. Softw. Technol. 51 (2009) 7–15. https://doi.org/10.1016/j.infsof.2008.09.009.
19. F. Al-Turjman, H. Zahmatkesh, R. Shahroze, An overview of security and privacy in smart cities' IoT communications, Trans. Emerg. Telecommun. Technol. (2019) 1–19. https://doi.org/10.1002/ett.3677.
20. S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, A. Kashif Bashir, A survey of security and privacy issues in the Internet of Things from the layered context, Trans. Emerg. Telecommun. Technol. (2020) 1–20. https://doi.org/10.1002/ett.3935.
21. M.G. Samaila, M. Neto, D.A.B. Fernandes, M.M. Freire, P.R.M. Inácio, Challenges of securing Internet of Things devices: A survey, Secur. Priv. 1 (2018) e20. https://doi.org/10.1002/spy2.20.
22. B.B. Gupta, M. Quamara, An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols, Concurr. Comput. . 32 (2020) 1–24. https://doi.org/10.1002/cpe.4946.
23. T.D. Mai, Research on Internet of Things security architecture based on fog computing, Int. J. Distrib. Sens. Networks. 15 (2019). https://doi.org/10.1177/1550147719888166.
24. J. Liu, M. Chen, L. Wang, A new model of industrial internet of things with security mechanism—An application in complex workshop of diesel engine, Proc. Inst. Mech. Eng. Part C J. Mech. Eng. Sci. 234 (2020) 564–574. https://doi.org/10.1177/0954406219884970.
25. M. Aydos, Y. Vural, A. Tekerek, Assessing risks and threats with layered approach to Internet of Things security, Meas. Control (United Kingdom). 52 (2019) 338–353. https://doi.org/10.1177/0020294019837991.
26. G. Selimis, R. Wang, R. Maes, G.J. Schrijen, M. Münzer, S. Ilić, F.M.J. Willems, L. Kusters, RESCURE: A security solution for IoT life cycle, ACM Int. Conf. Proceeding Ser. (2020). https://doi.org/10.1145/3407023.3407075.
27. K. Tange, M. De Donno, X. Fafoutis, N. Dragoni, A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities, IEEE Commun. Surv. Tutorials. 22 (2020) 2489–2520. https://doi.org/10.1109/COMST.2020.3011208.
28. D. Mendez Mena, I. Papapanagiotou, B. Yang, Internet of things: Survey on security, Inf. Secur. J. 27 (2018) 162–182. https://doi.org/10.1080/19393555.2018.1458258.
29. W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, Y.A. Bangash, An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security, IEEE Internet Things J. 7 (2020) 10250–10276. https://doi.org/10.1109/JIOT.2020.2997651.
30. V. Sharma, I. You, K. Andersson, F. Palmieri, M.H. Rehmani, J. Lim, Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey, IEEE Access. 8 (2020) 167123–167163. https://doi.org/10.1109/ACCESS.2020.3022661.
31. I.O. Ebo, O.J. Falana, O. Taiwo, B.A. Olumuyiwa, An Enhanced Secured IOT Model for Enterprise Architecture, 2020 Int. Conf. Math. Comput. Eng. Comput. Sci. ICMCECS 2020. (2020). https://doi.org/10.1109/ICMCECS47690.2020.247112.
32. M. Serror, S. Hack, M. Henze, M. Schuba, K. Wehrle, Challenges and Opportunities in Securing the Industrial Internet of Things, IEEE Trans. Ind. Informatics. 17 (2021) 2985–2996. https://doi.org/10.1109/TII.2020.3023507.

33. A. Bhawiyuga, M. Data, A. Warda, Architectural design of token based authentication of MQTT protocol in constrained IoT device, Proceeding 2017 11th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2017. 2018-Janua (2018) 1–4. https://doi.org/10.1109/TSSA.2017.8272933.
34. W. Shen, B. Yin, X. Cao, L.X. Cai, Y. Cheng, Secure device-to-device communications over WiFi direct, IEEE Netw. 30 (2016) 4–9. https://doi.org/10.1109/MNET.2016.7579020.
35. T. Gebremichael, L.P.I. Ledwaba, M.H. Eldefrawy, G.P. Hancke, N. Pereira, M. Gidlund, J. Akerberg, Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges, IEEE Access. 8 (2020) 152351–152366. https://doi.org/10.1109/ACCESS.2020.3016937.
36. Z.B. Celik, E. Fernandes, E. Pauley, G. Tan, P. Mcdaniel, Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities, ACM Comput. Surv. 52 (2019). https://doi.org/10.1145/3333501.
37. M. Aazam, S. Zeadally, K.A. Harras, Deploying Fog Computing in Industrial Internet of Things and Industry 4.0, IEEE Trans. Ind. Informatics. 14 (2018) 4674–4682. https://doi.org/10.1109/TII.2018.2855198.
38. R. Hassan, F. Qamar, M.K. Hasan, A.H.M. Aman, A.S. Ahmed, Internet of things and its applications: A comprehensive survey, Symmetry (Basel). 12 (2020) 1–29. https://doi.org/10.3390/sym12101674.
39. S. Haiba, T. Mazri, Secure communication in E-health care system monitoring, ACM Int. Conf. Proceeding Ser. (2019) 1–9. https://doi.org/10.1145/3368756.3368980.
40. X. Yang, LoRaWAN: Vulnerability Analysis and Practical Exploitation, (2017). http://repository.tudelft.nl/.
41. What is an IoT Gateway? | Lanner, (n.d.). https://www.lanner-america.com/blog/what-is-an-iot-gateway/ (accessed December 21, 2020).
42. A. Bicaku, M. Tauber, J. Delsing, Security standard compliance and continuous verification for Industrial Internet of Things, Int. J. Distrib. Sens. Networks. 16 (2020). https://doi.org/10.1177/1550147720922731.
43. U. Hunkeler, H.L. Truong, A. Stanford-clark, MQTT-S – A Publish / Subscribe Protocol For Wireless Sensor Networks, (n.d.).
44. B. Cendón, M2M interworking technologies and underlying market considerations, Mach. Commun. (2015) 79–92. https://doi.org/10.1016/b978-1-78242-102-3.00005-8.
45. J.E. Luzuriaga, M. Perez, P. Boronat, J.C. Cano, C. Calafate, P. Manzoni, A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks, 2015 12th Annu. IEEE Consum. Commun. Netw. Conf. CCNC 2015. (2015) 931–936. https://doi.org/10.1109/CCNC.2015.7158101.
46. G. Nebbione, M.C. Calzarossa, Security of IoT application layer protocols: Challenges and findings, Futur. Internet. 12 (2020) 1–20. https://doi.org/10.3390/fi12030055.
47. M.J. Michaud, T. Dean, S.P. Leblanc, Attacking OMG Data Distribution Service (DDS) Based Real-Time Mission Critical Distributed Systems, MALWARE 2018 - Proc. 2018 13th Int. Conf. Malicious Unwanted Softw. (2019) 68–77. https://doi.org/10.1109/MALWARE.2018.8659368.
48. Kim J, Park J, Lee JH, Analysis of recent IIoT security technology trends in a smart factory environment. In2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2023 Feb 20 (pp. 840-845). IEEE. https://doi.org/10.1109/ICAIIC57133.2023.10067004
49. Juma M, Alattar F, Touqan B, Securing big data integrity for industrial IoT in smart manufacturing based on the trusted consortium blockchain (TCB). IoT. 2023 Feb 6;4(1):27-55. https://doi.org/10.3390/iot4010002
50. Safavi S, Shukur Z. Conceptual privacy framework for health information on wearable device. PloS one. 2014 Dec 5;9(12):e114306. https://doi.org/10.1371/journal.pone.0114306
51. Safavi S, Meer AM, Melanie EK, Shukur Z, Cyber vulnerabilities on smart healthcare, review and solutions. In2018 Cyber Resilience Conference (CRC) 2018 Nov 13 (pp. 1-5). IEEE. https://doi.org/10.1109/CR.2018.8626826