Iftekhar Uddin Ahmed

CHALLENGES AND REQUIREMENTS OF INDUSTRIAL IOT APPLICATIONS

Master of Science
Faculty of Information Technology and Communication Sciences
University Lecturer Jukka Talvitie
Professor Mikko Valkama
May 2023

ABSTRACT

Iftekhar Uddin Ahmed: Challenges and Requirements of Industrial IoT Applications
Master's Thesis
Tampere University
Communication Systems and Networks
May 2023

Internet of Things (IoT) refer to physical systems which are linked together via a network to communicate with one another and their environment. Future industrial systems will have a crucial role for the Industrial Internet of Things (IIoT). With an end goal to grasp the development of IoT and IIoT, in this thesis we give a survey of the Industrial Internet of Things (IIoT) and how it differs from the Internet of Things (IoT). We also discuss numerous IoT applications in various industries, security challenges, advanced features and characteristics of IoT, IIoT, and Industry 4.0. The main objective of this research is to present a thorough overview of the IIoT evaluation. This thesis provides insight to increasing requirements of various IoT and IIoT applications. In addition, the thesis discusses potential IIoT solutions, and considers certain essential security aspects.

Keyword: Internet of Things, Industrial Internet of Things, Industry 4.0, IIoT evaluation.

PREFACE

First of all, I want to thank Almighty Creator from the bottom of my hearts for keeping me mentally and physically fit so that I could complete the necessary task of my thesis.

I am incredibly grateful to my supervisor Assistant Professor Jukka Talvitie for his excellent direction, support, inspiration, encouragement, and thesis revision. His constant oversight of my research during that time was a real blessing, and his wisdom has greatly improved this work. Without his assistance, I could never have successfully completed my dissertation. Moreover, I want to express my gratitude to the remainder of the thesis committee and all the faculty at Communication Systems and Networks department for their ongoing assistance.

I also want to thank my parents, family, and friends, who not only encouraged me to study but also gave me the motivation and support to achieve everything. They have supported me throughout my M.Sc. program with their tolerance, love, and encouragement.

Tampere, May 2023

Iftekhar Uddin Ahmed

CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

AI	Artificial Intelligence
AR	Augmented Reality
BC-ETS	Block Chain-based Energy Trading Scheme
BFT	Byzantine Fault Tolerance
CPMS	Cyber-Physical-based Manufacturing System
CPS	Cyber-Physical Systems
CPS	Cyber-Physical Systems
CSIP	Context-Sensitive Seamless Identity Provisioning
DCS	Distributed Control System
DE	Distributed Energy
DEGCs	DE Generation Companies
DFV	Device Function Virtualization
DL	Data Learning
DLT	Distributed Ledger Technology
DP	Distributed Power
DQN	Deep Q Network
DRL	Deep Reinforcement Learning
DZs	Demilitarized Zones
D2D	Device-to-Device
ENISA	European Union Agency for Network and Information Security
EUOC	Effective Utilization of Channels
FI	Forensic Investigations
FLAN	Factory Local Area Network
FMS	Flexible Manufacturing System
FS	Forensic Security
GAN-C	Generative Adversarial Network-Classifier
HLAN	HQ Local Area Networks
HMI	Human Machine Interface
HTTPS	Hypertext Transfer Protocol Secure
IACS	Industrial Automation and Control Systems
IoD	Internet of Data
IoT	Internet of Things
IIoT	Industrial Internet of Things
IoS	Internet of Services
IRL	Inverse Reinforcement Learning
IT	Information Technology
LANs	Local Area Networks
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MEC	Mobile Edge Computing
MIMO	Multiple-Input Multiple-Output
ML	Machine Learning
MR	Mixed Reality
MRO	Maintenance, Repair and Overhaul/Operation
MQTT	Message Queuing Telemetry Transport
M2M	Machine-to-Machine
n-ICS	Networked Industrial Control Systems
NLI	Natural Language Interface
OT	Operational Technology
PBFT	Practical Byzantine Fault Tolerance
PLC	Programmable Logic Control
PoA	Proof-of-Authority

PoET	Proof-of-Elapsed-Time
PoS	Proof-of-Stake
PoW	Proof-of-Work
P2P	Peer-to-Peer
RB	Resource Blocks
RPL	Routing Protocol in Low-Power and Lossy Networks
SAW	Straightforward Added Substance Weighting
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Networking
SIA	Smart Industrial Applications
SMSs	Smart Manufacturing Services
SVM	Support Vector Machine
TOPSIS	Technique for Order Preference by Similarity to the Ideal Solution
TRUST	Transparency Relying Upon Statistical Theory
TSN	Time Sensitive Networking
TTCP	Three-Terminal Cooperative Stage
WLAN	Wireless Local Area Network
XAI	Explainable AI
5G	Fifth Generation
5G I-IoT	5th Generation Intelligent Internet of Things

1. INTRODUCTION

1.1 Familiarisation of IoT and It’s evolution

IoT stands for Internet of Things. The IoT is an arrangement of interrelated figuring gadgets, mechanical and computerized machines giving extraordinary identifiers and the capacity to move information over a system without expecting human-to-human or human-to-PC cooperation. IoT alludes to any arrangement of physical gadgets that get and move information over remote systems without human intercession. This is made conceivable by coordinating straightforward processing gadgets with sensors in a wide range of items. It brings the intensity of the web, information handling and examination to this present reality of physical articles [1].

At first, organization of personal computers started with the point of monetary and proficient sharing of scant and costly processing assets. Before long, the improvement of TCP/IP convention suites filled the development and lead to the coming of the worldwide systems administration office known as the Internet. From that point forward, the Internet has advanced enormously and has accomplished a very long while of an effective presence. The long periods of development of the current Internet and the headways in applicable fundamental innovations have made ready for the rise of IoT. The development of the Internet comprises of five stages [1].

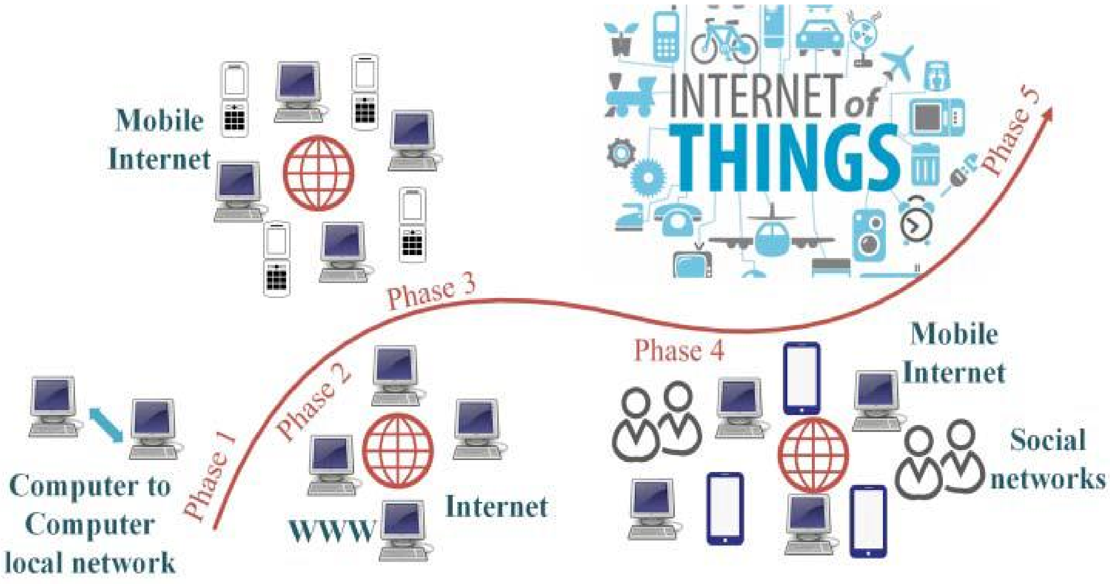

Figure 1. 1. Evolution of IoT [1]

1.2 Working Principles and Applications of IoT

A basic prerequisite of an IoT is that the things in the system must be associated with one another. IoT framework engineering must ensure the activities of IoT, which interfaces the physical and the virtual universes. An IoT eco-system comprises of web-empowered keen gadgets that utilization inserted frameworks, for example, processors, sensors and correspondence equipment, to gather, send and follow up on information they procure from their surroundings. IoT gadgets share the sensor information with an IoT entryway or other edge gadget where information is either sent to the cloud to be investigated or broke down locally [2].

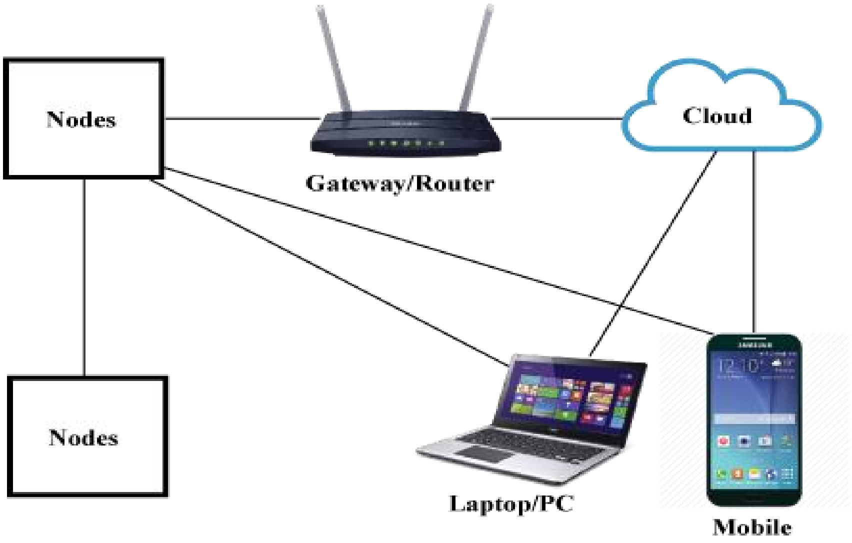

Figure 1. 2. How IoT works [2]

IoT applications have been classified in various manners like as:

- ✓ Wearables
- ✓ Smart City
- ✓ Smart Energy
- ✓ Healthcare

- ✓ Agriculture
- ✓ Home Automation
- ✓ Industrial Automation
- ✓ IoT Automotive
- ✓ Business
- ✓ Tactile Internet
- ✓ Retail
- ✓ Gaming etc.

In our all sphere of life IoT applications are necessary, like as – make cities modern by removing removing waste and creating new facilities, enables healthcare sector more forwardly, use analytical tools for monitoring the farms and gaining insights, help companies discover, track, and analyse client data more quickly, and so on. Besides, lighting, cooling, security systems, and other building operations can be automated with IoT. This technology increases the effectiveness of industrial manufacturing processes while reducing the demand for physical labor,

1.3 IoT Elements

There are six main elements [3] needed for deliver the functionality of IoT as illustrated in the below figure.

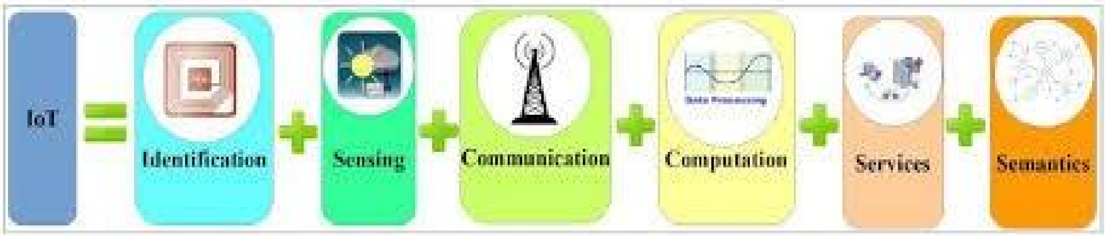

Figure 1. 3. IoT Element [3]

The main elements shown in the above figure are descripted shortly in the following.

1. Identification: Recognizable proof is urgent for the IoT to name and match administrations with their interest. Numerous recognizable proof techniques are accessible for the IoT, for example, electronic product codes and ubiquitous codes. Distinguishing proof strategies are utilized to give an unmistakable character to each protest inside the organization.

2. Sensing: The IoT detecting implies gathering information from related articles inside the organization and sending it back to an information stockroom, information base, or cloud.
3. Communication: The IoT correspondence advances associate heterogeneous articles together to convey explicit brilliant administrations. Normally, the IoT hubs ought to work utilizing low force within the sight of lossy and boisterous correspondence joins.
4. Computation: Understanding the "cerebrum" and processing capacity of the IoT is possible thanks to handling devices and programming tools. Several equipment stages have been created for IoT applications. IoT functionalities are offered at a number of product development stages. The IoT's extensive computational component is organized through cloud platforms.
5. Services: IoT administrations can be sorted under four classes, such as- Identity related Services, Information Aggregation Services, Collaborative Aware Services and Ubiquitous Services. Identity-related services are the most essential and significant administrations that are utilized in different sorts of administrations. Each application that requirements to carry true items to the virtual world needs to recognize those articles.
6. Semantics: Semantic in the IoT indicates a device's capacity to extract information and offer the fundamental types of support. Information extraction incorporates both finding and displaying data. It also requires gathering data in order to decide how to effectively give the required support. As a result, semantic interacts with the IoT by routing requests to the right asset [3].

1.4 Feature of IoT Hardware Platform

IoT Hardware includes a variety of devices, including steering, spans, sensors, and more. These IoT devices manage important tasks such as, system implementation, security, activity determinations, communication, and identification of help specified goals. It might make reference to communication modules, microcontrollers, and SoC modules that make them desirable for use in the creation of IoT. IoT equipment improvement stages have various highlights that make them reasonable for structuring and prototyping IoT gadgets. The fundamental features are Arduino and Raspberry Pi [4].

1.5 What is IIoT?

IIoT, or the Industrial Internet of Things, is a subcategory of IoT that alludes to a framework including organized keen articles, digital physical resources, related conventional data innovations and discretionary cloud or edge registering stages, which empower ongoing, shrewd, and independent access, assortment, examination, interchanges, and trade of procedure, item and additionally administration data, inside the mechanical condition, in order to advance by and large creation esteem. This worth may incorporate: improving item or administration conveyance, boosting profitability, lessening work costs, decreasing vitality utilization, and diminishing the work to arrange cycle. IIoT centers intensely around machine-to-machine (M2M) correspondence, AI, and huge information, which empower associations to open access to exceptional measures of information and concentrate experiences at quick speeds. The IIoT includes a wide scope of mechanical evaluation applications, from AR gadgets and associated, synergistic robots, to clinical gadgets, stock following, and prescient upkeep [5].

1.6 Working Principles of IIoT and It's Applications

IIoT is a system of shrewd gadgets associated with structure frameworks that screen, gather, trade and break down information. Each mechanical IoT ecosystem comprises of Analytics and applications that create business data from crude information and People. The structure of an IIoT engineering necessities to feature extensibility, versatility, seclusion, and interoperability among heterogeneous gadgets utilizing unique advancements [6].

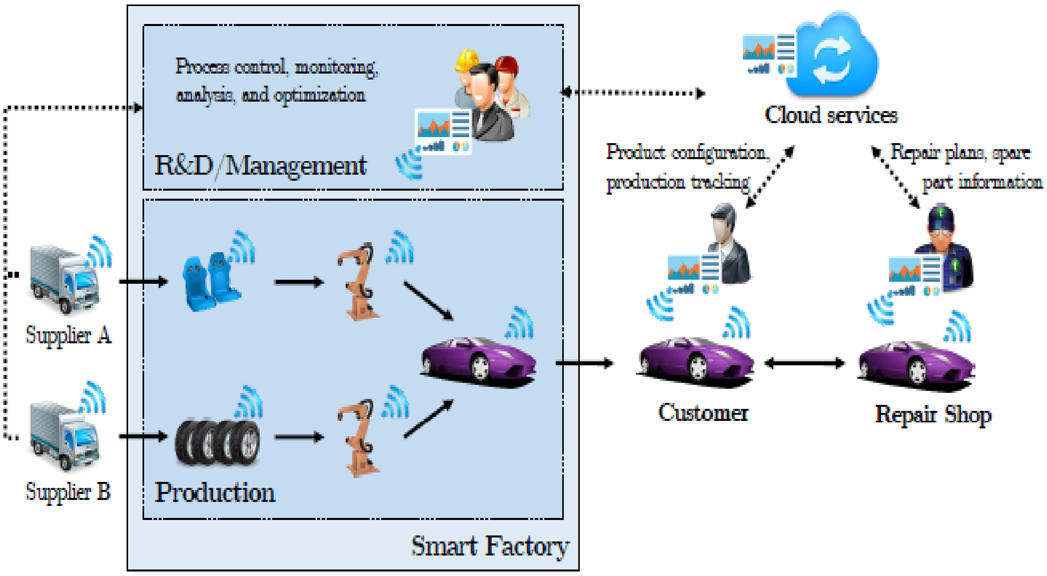
Process control, monitoring, analysis, and optimization
R&D/Management
Cloud services
Product configuration, production tracking
Repair plans, spare part information
Supplier A
Supplier B
Production
Customer
Repair Shop
Smart Factory

Figure 1. 4. How IIoT works [7]

There are different types of IIoT application, such as:

- ✓ Wearables
- ✓ Robotics
- ✓ Industrial Autonomous
- ✓ Energy
- ✓ Transportation
- ✓ Power Management
- ✓ Logistics Management
- ✓ Software Integration
- ✓ Security and Quality
- ✓ Maintenance etc.

Though the use of IIoT, businesses and industries may operate more efficiently and reliably. Like as IoT, IIoT also used to analyze and capture data in many sectors. Home appliance management is the main emphasis of IoT, but IIoT focuses on crucial systems like those in healthcare, aerospace, and factory automation, as well as on connecting people and machines and using data analytics. IIoT is employed in the industrial sector, whereas IoT is used by consumers or end users.

1.7 Objective of This Thesis

This research makes a survey covering the evaluation of IoT and IIoT with 5G Architecture. The main objectives of this research are -

- ✓ To obtain and analyze data using IoT technologies in different fields
- ✓ To improve production methods in industrial settings by IIoT technologies
- ✓ To present the security challenges of IIoT systems and reduce the unwanted various attacks
- ✓ To highlight the use cases and applications in IoT, IIoT and Industry 4.0 and determine existing research issues and their remedies for Industrial IoT

1.8 Organization of This Thesis

This chapter has already covered the introduction. The final section of the report is structured as follows. Chapter 2 discussed the earlier efforts that are closely related to our research. We have discussed security issues in chapter 3, use cases and applications in chapter 4, and advantages of IIoT in manufacturing sector in Chapter 5. In chapter 6, we have concluded our work and offered a strategy for continuing it in the future.

2. IIOT SOLUTIONS IN MODERN AND FUTURE WIRELESS COMMUNICATIONS

2.1 Overview of IIoT

The authors in [6] give an overview of upcoming IIoT (Industrial Internet of Things) solutions. IoT, IIoT, and Industry 4.0 are firmly related ideas however can't be reciprocally utilized. What appears to be a revolution for the consumer sector may simply be another step in the ever-changing world of industrial communications. They describe the comparison between Consumer IoT and Industrial IoT. They define the terms IoT (Internet of Things), IIoT, and Industry 4.0. They also discuss the advantages of this paradigm shift as well as the obstacles to its implementation. They concentrate on the difficulties connected with energy efficiency, real-time performance, cohabitation, interoperability, security maintenance, privacy issue, and so on. In spite of the extraordinary guarantee, there are many difficulties in understanding the opportunities given by IIoT. A comprehensive review of current research activities and possible research pathways for addressing IIoT problems are also given here.

The growing demand for IIoT (Industrial Internet of Things) connectivity standardization and technological solutions that can be used by many industry verticals was reviewed in this article. It also highlights important IIoT connectivity technologies and platforms that have the potential to propel the next industrial revolution. The essay also discusses the major roadblocks to fully fulfilling the IIoT's potential, especially achieving secure connectivity and managing a highly fragmented ecosystem of connectivity solutions and platforms. Finally, future building automation serves as an illustration of IIoT connectivity issues. The problems that must be addressed to fulfill the potential of IIoT connectivity create intriguing research opportunities, as the IIoT is projected to drive industrial progress in the near future [8].

2.2 Case study on IoT evolving into IIoT

Himanshu et al. [9] describe a look at how IoT (Internet of Things) is evolving into IIoT (Industrial Internet of Things), what is Industry 4.0, what are the fundamental distinctions between IoT and IIoT, the difference between Traditional IT Security and IoT Security, what are the IoT features and what are the benefits of IoT and IoT’s advanced characteristics. They briefly describe the applications of IoT like - Smart homes, Transportation, Consumer Applications, Medical, and Healthcare. They also briefly describe the applications of IIoT, such as - Agriculture, Manufacturing, Military Applications, Internet of Battlefield Things, and Ocean of Things. Since the demand for IoT systems is growing in numerous fields every day, as well as the comfort of living that comes with using smart devices but it has some limitations. They also covered security dangers and challenges that IoT-based systems face, as well as strategies to circumvent the system's limits like - Connectivity and Visibility, IIoT Integration, Data Storage, Security, Analytics Challenges. Though certain limits, nevertheless in future it will swiftly boost the economic and production level of industries as well as countries also.

2.3 Case study on 5G I-IoT

This paper proposes a new paradigm for processing massive data intelligently and optimizing communication channels called 5G I-IoT (5th Generation Intelligent Internet of Things) [10]. It is intended to address a number of difficulties, including massive data processing and congested communication channels. As a result, the 5G I-potential IoT's is to intelligently handle massive data, enhance channel usage, and optimize communication channels in order to achieve 4A. the 5G I-IoT worldview depends on an overall 5G cellular network. It presents the different arising innovations, including monstrous MIMO networks, thick static little cell networks, and mobile little cell networks. In the article, they join the ideas of D2D (Device-to-Device) correspondence, little cell passageways, and the 5G I-IoT. The processing center, object processor, and sensor areas are the three building parts of the 5G I-IoT. Also, discuss the interactions between the key components. Then went over some of the most important 5G IoT methods and technologies, such as big data mining, deep learning, and reinforcement learning. Offered an experiment, such as the EUOC (Effective Utilization of Channels) curve, and studied the changes in the major evaluation indicators to establish the efficiency of the proposed 5G I-IoT. Proposed 5G I-IoT goals to accomplish intelligent processing of large information and advancement of correspondence channels. Finally, various applications and unresolved concerns are discussed. This paper provides a fresh take on IoT by incorporating intelligent technologies into 5G's interaction with the IoT (Internet of Things).

Another article provides an overview of the emerging wireless technologies such as 1G, 2G, 2.5G, 3G, 3.75G, 4G, and 5G [11]. To meet the expectations and challenges of the near future, wireless-based networks will have to advance in a variety of ways today and in the near future. They present the aftereffects of an overall overview on the 5G (fifth generation) cellular network design and a portion of the key arising advances that are useful in working on the design and satisfying the needs of clients. In this study, the excellent spotlight is on the 5G cellular network design, enormous various input various result innovation, and D2D (Device-to-Device Communication). Alongside this, a portion of the arising innovations that are tended to in this paper incorporate interference administration, spectrum sharing with cognitive radio, ultra-dense networks, multi-radio access innovation affiliation, full-duplex radios, millimeter-wave answers for 5G cellular organizations, and cloud advancements for 5G radio access organizations and programming characterized networks. An overall likely 5G cellular network design is proposed, which shows that D2D, little cell passageways, network cloud, and the IoT (Internet of Things) can be a piece of 5G cellular network system. This is incorporated in regards to momentum research projects being directed in various nations by research gatherings and establishments that are chipping away at 5G advances. This paper might be giving a decent stage to inspire the analysts for better results of various sorts of issues in cutting-edge organizations [11].

2.4 Analysis of IIoT frameworks

Yuzheng et al. [12] give an extensive study of potential personality goal frameworks for IIoT (Industrial Internet of Things), which is a central foundation in IIoT. Here, research the cutting-edge principles and papers of existing significant character goal frameworks and bring normal parts from them to assemble an overall reference structure for depicting a personality resolution framework. The main contributions all through this article are as per the following:

1) The significance of identity resolution systems in the IIoT is discussed. Discuss identity resolution system design principles for the IIoT. Then, based on key functions, a generic framework for evaluating identity resolution systems is presented.

2) The suggested function-based framework is used to evaluate some key identity resolution systems, including the overview, identification, resolution, security, and compatibility.

3) The systems are evaluated using the principles, and the viability of using them in the IIoT is examined. From the standpoint of technology selection, each system is compared.

4) Various existing systems with these difficulties and some significant research directions are discussed.

5) All issues in this field are examined, as well as some broad perspectives.

This article presents a comparison between IoT (Internet of Things) and IIoT (Industrial Internet of Things) and summarizes the exploration progress concerning edge computing in IIoT. The IoT broadly acknowledged by individuals is essentially utilization arranged and plans to further develop individuals' life quality. The IIoT is creation situated and means to further develop modern creation productivity. Edge computing is continuously applied in different IIoT situations. Since numerous benefits of edge computing applied to the IIoT are – system performance improvement, data security and privacy issue, operational cost reduction, and so on. The edge processing reference design in IIoT is partitioned into the cloud layer and edge layer, and the edge layer can likewise be partitioned into Near-Edge, Mid-Edge, and Far-Edge. For the high-level advancements of edge processing in IIoT, they have made a complete elaboration according to the viewpoints of directing, task booking, information capacity and examination, security, and normalization. The difficulties of edge registering in IIoT are broken down and talked about according to the points of view of 5G-based edge correspondence, load adjusting, edge artificial intelligence, and secure information sharing. The mix of edge figuring with blockchain, machine learning, software-defined networks, and 5G will turn into a conspicuous pattern. What's more, here talked about a few ordinary situations of utilization, expecting to be useful to the advancement and use of edge figuring in IIoT. Not the same as other IIoT or edge registering overview papers, the fundamental commitment of this paper is to highlight the combination use of IIoT and edge computing, attempting to explain the significance of things to come of edge computing in IIoT [13].

Another latest reference structure for remote framework plans in IIoT (Industrial Internet of Things) use-cases has been proposed by Yongkang et al. [14]. The structure presents a nonexclusive plan interaction and distinguishes the critical inquiries and apparatuses of individual systems. In particular, they remove sway factors from unmistakable spaces including modern activities and conditions, information administration elements, and the IT (Information Technology) framework. Then, at that point, map these variables into workgroups and talk about their separate effect on execution measurements and asset use techniques. At long last, conversations happen in four praiseworthy IIoT applications where they utilize the structure to distinguish remote organization issues and arrangement highlights in the constant interaction observing, discrete framework control, portable applications, and range harmonization, separately. The work introduced in this paper has three major commitments as follows:

1) To break down the investigation of mind-boggling IIoT use cases into independent specialized spaces, i.e., OT (Operational Technology) applications, IIoT information administrations, and IT frameworks, every one of which is made out of organized factors that influence the remote organization execution in the objective use cases. By embracing such a system, OT engineers, IT overseers, and organization organizers can address configuration issues in their space mastery and cooperatively add to the remote plan.

2) To configure wireless organization formalized as a bound together interaction. Plan components that address conventional help necessities and accessible assets are distinguished and chosen as framework boundaries to serve in issue targets and conditions. Such a demonstrating approach guarantees that remote procedures what's more arrangements are reusable in various use cases on the off chance that they are tending to a similar plan component.

3) To enumerate the connections between sway factors and plan components platform the hole between the previously separated OT and IT designing spaces, which advances the IIoT information base and motivates new plan, measure, and assessment endeavors on remote practices inside modern plants.

Yongkang et al. [15] describe a novel dimensioning structure to arrange remote use cases and recognize their specific effects and necessities on remote framework plan and challenge the plan work. These elements are examined in a stochastically layered structure utilizing space information from operational technology applications, information administrations, and information technology frameworks, every one of which contains organized factors that characterize remote answers for target use cases. The relationships among intra-and between space factors are likewise examined looking for proficient remote plan arrangements. Given the variety and assortment of IIoT (Industrial Internet of Things) executions, such a structure that recognizes general and explicit remote necessities in individual use cases would be of high viable worth and diminishes the time and cost to modern remote plan and execution. This framework is useful because it standardizes the wireless system design cycle for industrial applications and minimizes the time and cost of modifying design difficulties for diverse use cases.

2.5 Relation between IIoT, Big Data analysis and Cyber-Physical systems

2.5.1 IIoT and Big Data analysis

Khaled et al. [16] investigate Cloud Computing, Big Data, IIoT (Industrial Internet of Things), Industrie 4.0, interrelations between IIoT and Big Data innovations. Additionally, requirements for cloud-based solutions are drawn from the Industrie 4.0 use case scenario for value-based services. The outcomes show that there is no select IoT (Inter-net of Things) and big data stage and definitively it relies upon prerequisites and uses cases. Similarly, show that various present day cloud stages ought to be connected with enormous data frameworks and courses of action. The principal objective of this paper is to distinguish the gap between IoT and big data arrangements and to characterize the difficulties of involving these advancements in Industrie 4.0 plants with examples of real-life implementation.

2.5.2 IIoT and Cyber-Physical Systems

Another article [17] reviewed the current examination workaround IIoT (Industrial Internet of Things) security. Applications for IIoT are a characteristic advancement of IoT. Henceforth, IIoT acquires some security challenges from IoT (Internet of Things). Late exploration interests on these security challenges are mostly about information security, Cyber-Physical Systems trustworthiness, a key foundation for gadgets blending, and sensor the board. Since these security challenges have been profoundly read up in IoT for a really long time, one might gain from the all-around concentrated IoT practices to address these difficulties in IIoT. Contrasted with IoT and IIoT applications have some particular security prerequisites. Because of the distinctions between IoT and IIoT, IIoT has some particular security concerns chiefly on safeguarding basic industry control frameworks. The improvement of IIoT brings the availability, versatility, and constant knowledge for customary industry frameworks. It likewise opens up new assault surfaces on the business frameworks. Since applications for the IIoT is a characteristic advancement of the IoT, IIoT acquires some security provokes from IoT because of the comparative essential design. Since IIoT has explicit elements and necessities contrasted with IoT, the IoT security rehearses should be improved or re-intended for IIoT situations. In this manner, they sorted the security challenges in IIoT frameworks into two categories: the security challenges that exist in both IoT and IIoT, and the security moves explicit to Industry frameworks. In each gathering, they broke down the particular security challenges and concentrated on the past work on tending to these difficulties.

Hugh et al. [5] examine what IIoT (Industrial Internet of Things) is and how it relates with CPS (Cyber-physical systems) and Industry 4.0. This research proposes an IIoT definition and examines associated partial IoT taxonomies. The industrial internet is a network of things, machines, computers, and people that enables intelligent industrial operations based on advanced data analytics for transformative business outcomes, and it's changing the game for businesses and individuals alike. Industrie 4.0 refers to a set of technology and value chain management ideas. CPS monitors physical processes, creates a virtual duplicate of the actual world, and makes decentralized decisions inside the modular organized Smart Factories of Industrie 4.0. CPS connect and collaborate with one other and humans in real-time via the IoT (Internet of Things). This article gives more context to CPS, IACS (Industrial Automation and Control Systems), and the Industrial Internet, situating them in the context of Industry 4.0. It creates an IIoT analysis framework for enumerating and characterizing IIoT devices for researching system designs and analyzing security threats and vulnerabilities.

2.6 Mobile Edge Computing system in supporting IIoT

The serious issues of the current standard MEC (Mobile Edge Computing) system in supporting IIoT (Industrial Internet of Things) are - complex turn of events, low advancement reuse rate, low viability, versatility, and adaptability. To take care of these issues creators in this paper have been proposed an original MEC structure uniquely for IIoT, named IIoTMEC. They use Docker holder to cut processing and capacity assets of MEC server into various RB (Resource Blocks). In view of the idea of virtualization, a few RBs for DFV (Device Function Virtualization) are utilized to plan actual sensors into virtual sensors and present in a bunch of standardized APIs, which safeguard the equipment improvement of assorted IIoT sensors, to work on the IIoT advancement into programming improvement as it were. A few RBs are utilized to help the activity of IIoT administrations, as conveyed registering. On these premises, an adaptable article arranged IIoT improvement design is built. IIoT-MEC can conquer the disadvantages of the current MEC system in supporting IIoT. Also, the execution method of IIoT-MEC is exhibited with an application model. They likewise examine how the IIoT-MEC would be utilized and what they want to do in future examinations. The fundamental commitment of their IIoT-MEC contrasted and existing MEC system are - straightforward turn of events, high advancement reuse rate, high practicality, versatility, and adaptability [18].

George et al. [19] introduced a structure for condition observing and predictive supporting and creation status observing for resource creating in working environment. They examine the utilization of information diagrams to catch the information from the upkeep work force as well as the connections between the resources and the sensors. They use edge computing which is connected with various sensors to monitor the operating conditions. Edge computing is a technique that allows computation to be performed close to physical devices, boosting data transmission and real-time applications. The structure was tried in a utilization case connected with an Aluminum creation organization based on IIoT (Industrial Internet of Things) prototype. Then the results exhibited potential for additional examination of the mix of information diagrams with AI (Artificial Intelligence), approving the advantages, as far as time, for preparing ML (Machine Learning) models also as applications that can be empowered giving better knowledge to administrators with respect to the creation process. The outcomes introduced in this work can be applied in other creation conditions like those with huge piece of gathering processes. The following stages, it is imagined to broaden the information diagram into a more complete philosophy, equipped for being summed up to manufacturing with comparative issues. A technique for creating production plans across various processing plants, considering both static data and dynamic information investigation is described [20]. A crucial need for establishing whether a product is producible and whether the machines are capable of carrying out the required production stages. Many initiatives in this area aim to transform industrial manufacturing in the future. Edge smart devices continually screen high recurrence machine information and report consolidated machine states to an IIoT stage. A commercial center inside the cloud application MindSphere empowers us to incorporate the necessities of the items and the capacities of the creation locales. Clients are having the option to assess these creation plans in light of span, energy utilization, CO2 impression and so forth. Their method basically depends on a stage that unites the elaborate partners and offers different administrations for testing how a specific item can be created through cooperative endeavors of the elaborate production lines. The fundamental contribution of this study is the inclusion of operational data in the formulation of production schedules and the determination of producibility using runtime data from the machines and factories involved.

2.7 Wireless technologies in IIoT

Authors in paper [21] survey that modern organizations in the production line and interaction computerization and examine latest things as well as future viewpoints in this quickly advancing situation, including mechanical advancements, new fields of use, anticipated execution, and market patterns. These actions have helped industrial networks become more widely adopted. The majority of future perspectives are focused on expanding into new domains of application, as well as adopting new, higher-performing networks within already established technical settings, and developing new standards and technologies. The introduction of industrial networks in IIoT (Industrial Internet of Things) systems, the creation of new generation industrial wireless networks, SDN (Software Defined Networking), and the large use of Ethernet for in-vehicle connectivity foreseen in the automotive business are all excellent examples in this regard. In most of these situations, the TSN (Time Sensitive Networking) set of standards will almost certainly play a crucial role. Collaboration between academics, public research organizations, and the industrial world is encouraged because of the application-driven nature of this research. In the coming years, industrial communication systems will experience significant expansion in terms of research, practical applications, and installations. The main contribution of this paper is as per the following:

1) To give a complete outline of organizations utilized in manufacturing plant robotization and cycle control frameworks alongside their most significant highlights, applications, and execution figures.

2) To present the composite normalization structure and examination of the market status and patterns.

3) To address the future points of view utilizing new advancements, principles, next-generation Ethernet, 5G media communications, remote LANs (Local Area Networks), modern industrial application, ethernet networks, IIoT, and so on for auto applications.

As part of this research, an analysis of existing wireless data transmission technologies revealed that commercially available solutions do not fully match the standards stated for data collecting in predictive MRO (Maintenance, Repair and Overhaul/Operation) management administrations. The IIoT (Industrial Internet of Things) is the technology that allows this system to function. As part of this research, an analysis of existing wireless data transmission technologies revealed that commercially available solutions do not fully match the standards stated for data collecting in predictive MRO management systems. Experts at South Ural State University have created a proprietary wireless communication technology and various industrial field equipment with this technology at their core, in collaboration with the university's partner enterprises. This article discusses the technology's idea and the transmission and coverage range tests that were conducted in a real-world industrial setting. Some of the technology use cases are also discussed here, including one on a university campus and another at a business. The outcomes of the use cases reported in this article show that the unique design solutions may be successfully implemented in steelmaking and other sectors, and they may help to pave the way for their implementation in other industries as well [22].

2.8 Integration of Augmented Reality with IIoT

Vanin et al. [23] designed how AR (Augmented Reality) and the IIoT (Industrial Internet of Things) can be integrated into the educational process through a laboratory complex that is intended for laboratory practical lessons that are attended by engineering students. The combination of AR and IIoT opens up new possibilities in product design and operation. The goal of this integration is to develop skills in debugging such systems and to assess the usefulness of these technologies in the manufacturing and electric power industries, with a focus on electric drive system control. The application of these technologies in relation to the educational process and industry is explained, as well as its relevance and timeliness. The necessity for existing industrial automation systems to be modernized is discussed. A study of existing AR and IIoT technologies is also included. The strength of the article is devoted to describing the modernization of the laboratory facility. The software ThingWorx is described, which allows both the AR and the IIoT to be implemented. An experiment in which the electric drive was started remotely and the operational temperature was controlled by the sensor. Because of the integration of this framework, it was feasible to control the activity of the modern office from a mobile application, utilizing a user interface, from any place on the planet. Though this ThingWorx has certain drawbacks, it has many advantages.

2.9 IIoT forensics

This authors in article [24] puts a contention that, during composing this paper, there actually needs approaches, methods, standards or development models that have an attention on IIoT (Industrial Internet of Things) forensics towards accomplishing Industry 4.0 perseveres. In light of these aspects, the creator investigates the extent of IIoT forensics and places the need of investigating and fusing forensics guidelines and strategies in IIoT. They the significance and furthermore features perrenial open and future issues. Future work targets fostering a nonexclusive IIoT forensic system that is agreeable with existing guidelines that can uphold current future insightful cycles. This paper's contributions are summarized as follows [24] :

1) In the IIoT, emphasized the importance of digital forensic processes, standards, and methods.

2) Provided a contextual assessment of the research.

3) Made a list of current and potential obstacles.

A technique proposed for bringing the manufacturing plant floor information into an IIoT (Industrial Internet of Things) climate and imagining continuous machine examination through AR (Augmented Reality) and MR (Mixed Reality) based on savvy devices [25] [28]. AR is one of the advances that spatially overlays computerized data on the ideal plan of interest on top of real-world conditions. There are many advantages of AR and now a days it is used in different important fields like manufacturing industries. The manufacturing plant floor information from specific machines at a Volvo Group plant was coordinated with IIoT and imagined continuously using AR-empowered devices. The setup interaction for the server and IIoT climate was computerized through a product arrangement, and the presentation and practicality of spatial anchors were assessed by testing exactness, setting off times, and dormancy of information. The outcomes shown promising utilizations of AR/MR on manufacturing plant floors for continuous machine information representation and related investigating. This work effectively showed the objective of bringing the industrial facility information into an IIoT climate for investigating and support purposes in shop floor machines.

The digital transformation is a continuous process that refers to the application of all types of digital technology to improve the efficacy and efficiency of value generation. Authors in [26] presents an IIoT (Industrial Internet of Things) architecture case-based idea where understudies tackle an interdisciplinary issue by demonstrating and carrying out a continuous information stream. They experience in an involved way how to incorporate frameworks and functionalities from the machine at the shop floor to the ongoing announcing for accomplishing more straightforwardness of the creation cycle. The consistent assessment of abilities accomplished show an increment of value in educating by consolidating theoretical and practical instructing parts. Aside from giving students with in-depth knowledge of IIoT-specific software and hardware, the course seeks to improve students' understanding of the interdisciplinary nature of IIoT, which encompasses all fields from data creation to data visualization and analysis.

Recent research on smart manufacturing has observed that the SMSs (Smart Manufacturing Services) plan technique has the following difficulties:

1) Traditional manufacturing machinery rarely make collaborative and data-driven manufacturing services possible.

2) AI and IIoT applications are typically isolated in a specific phase of the product life cycle and are not well integrated across the entire life cycle.

3) The majority of manufacturing machine design and manufacturing system construction approaches are conceptual, with only a few real-world examples.

4) More pragmatic techniques are required, particularly for small manufacturing firms.

In light of the above challenges, an orderly plan technique for brilliant assembling framework development has been proposed by different authors in different articles. A TTCP (Three-Terminal Cooperative Stage) comprising of cloud servers, implanted regulators and portable terminals has been used to coordinate AI and IIoT innovations for the ACMM plan. The strategy can give a few motivations to the assembling business to create SMSs and work with the advancement creation and modified and cooperative creation. The term of smart manufacturing refers to a US initiative that brought together several manufacturing stakeholders. Smart manufacturing has extraordinary potential in the improvement of organization coordinated effort, mass customization, manageability and adaptability. Manufacturing systems become smart when IIoT capabilities are combined with artificial intelligence technologies, resulting in extraordinary increases in production agility, quality, and efficiency. In the age of the IIoT, a smart production unit can be conceived of as a powerful connected industrial system containing materials, parts, equipment, tools, inventory, and logistics that can exchange data and communicate with one another. Both two articles gave an overview on smart manufacturing industry to create SMSs and smart manufacturing sectors under IIoT [27] [28]. Another article reviewed FMS (Flexible Manufacturing System) where use IIoT to perfectly implement manufacturing [29]. In paper [30] showed the current IIoT guidelines and solutions utilized in smart manufacturing system. These observations can successfully overcome the traditional problem of manufacturing system. And the outcomes will be potential directions for future researchers as well as the guarantee of the Fourth Industrial Revolution.

3. IIOT SECURITY ISSUES AND THEIR SOLUTIONS

3.1 Security issue in IIoT

We now provide support for new smart factory services and scenarios such as smart production, smart maintenance, smart logistics, and so on. One of the issues that the modern industrial environment faces is security. Indeed, there are numerous vulnerabilities in smart industrial applications that have been researched in the literature. As a result, discovering IIoT applications and security vulnerabilities in Industry 4.0 is very essential. To improve revenues, industrial systems are utilizing the potential of IoT to eliminate unnecessary operational costs and increase the usability and dependability of industrial assets.

The term Industrial 4.0 has generated a lot of buzz around the world. Industry 4.0 establishes a framework for integrating the IoT (Internet of Things), IoS (Internet of Services), and IoD (Internet of Data) into the industrial realm in order to make it smarter, more flexible, and adaptable. The IIoT alludes to the incorporation of the IoT across numerous modern areas like operations, creation, fabricating, energy, and so on. The IoS is made up of a service-oriented architecture that organizes application software and infrastructure into a series of interconnected services. The IoD enables data to be interconnected as a network, delivering important information like data activity logs, to aid analysis operations.

Several attack methods, such as Measurement Injection Attacks, Physical attacks, and Side-Channel attacks, could impact industrial devices. Other sorts of assaults, such as false logic attacks, deception attacks, and denial-of-service attacks, could be used against industrial control systems. The hacker might also take advantage of the network and communication flaws to launch various forms of attacks against the smart industrial environment [31].

Attackers are now targeting industries, and there is a pressing need to solve this problem. We can be classified IIoT layered architecture and attacks as [32] –

3.1.1 IIoT Layered Architecture

Layer 1: Embedded sensors, actuators, transmitters, and engines run at this level to perform actual cycles.

Layer 2: DCS (Distributed Control System), PIC's (Programmable Logic Control), and gateways connect with the devices at layer 1.

Layer 3: SCADA (Supervisory Control and Data Obtaining), Data Acquisition gadgets and HMI Human Machine Interface) which utilizes IP-based network convention dwell at this layer.

Layer 4: Office Applications, Intranet administrations, Web administrations, and mail administrations are conveyed on this layer.

Layer 5: Enterprise Applications, Cloud processing, Information Analytics, Internet, and Mobile Devices on this layer are liable for Analytics and information mining interaction to convey the data over the web and indeed, even on cell phones.

3.1.2 Possible IIoT attacks

It is open to the public since it makes use of Internet services and provides an attack surface for remote attacks. On this layer, some of the attacks are - Denial of Service, Side Channel attacks, Cloud malware Injection, Authentication, Man-in-the-Middle Cryptographic, Mobile phone attacks, Phishing attacks, SQL Injection, Malware, DNS Poisoning, Remote Code Execution, Brute Force, Web Application attacks, IP Spoofing, Data Sniffing, Data Manipulation, Replay attacks, Wireless Network attacks, Reverse Engineering.

3.1.3 Taxonomy of IIoT attacks and their impact

The attack taxonomy aids in the comprehension and classification of security occurrences. IIoT Attacks scientific categorization contains four aspects assault vector, assault target, assault effect, and assault result. We can demonstrate any assault on an Industrial Infrastructure utilizing the four aspects which uncovers the data about how the assault was performed, what parts are impacted, and what the aggressor had the option to accomplish. The primary aspect is the way or means by which an aggressor can get sufficiently close to a PC or organization. Assault vectors are sub partitioned into Cyber assault and Physical assault. The digital assault vectors contain the passage focuses on IT networks wherein no actual access is required, while the actual assault vectors need the assailant to collaborate with the gadget or individuals in the business. The subsequent aspect alludes to the objective which is the part on which the assault was arranged. The third aspect of assault sway is the impact of the assault performed. It is the result of the framework after the assault is done on it mostly a few endeavors are executed on the framework which makes the framework perform a malevolent assignment or change the normal way of behaving of the framework.

The proposed IIoT attack taxonomy categorization is displayed in Fig. 3.1. which contains 4 aspects, attack impact, attack vector, attack target, and attack consequence.

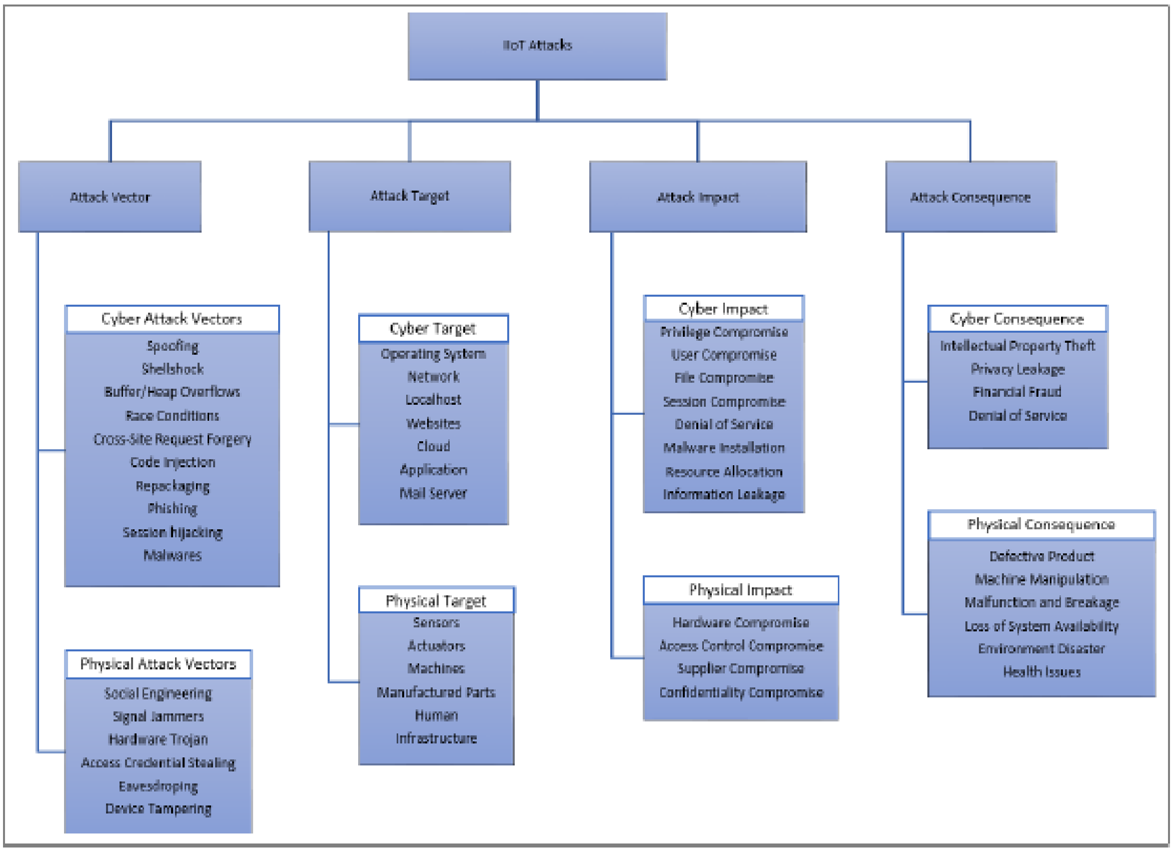

Figure 3. 1. IoT Attack Taxonomy [32]

With the expansion in arising dangers to IIoT, it is fundamental that the security difficulties ought to be considered from the initial stage itself. This scientific classification can help in planning the assault and recommending the alleviation designs and forestalling assaults on Industries.

3.2 IIoT security challenge

The IIoT security field is different. It covers enormous ventures, basic foundations, military, and public administrations. Likewise, it covers more modest organizations and explicit industry branches with few producers, with their own difficulties and necessities. In a climate of high recurrence of individuals and regularly unfortunate organization security settings, there is an issue regarding the level of safety for those IoT executions. WLAN setting is an extremely normal answer for organizations and offers a rundown of expected dangers and how to stay away from them, well defined for this issue.

To handle Wi-Fi Network security issues, it executes the WPA2 standard (ESP32 module) and SHA-2 encryption for correspondence with support applications. An expansion to security settings would be suggested best security practice for proprietors of the Wi-Fi organizations associating the larger cooler and serving unit, like utilizing the different Wi-Fi networks for IIoT units, dealing with the firewall settings of AP, and changing the default organization accounts usernames and passwords. Correspondence with cloud administrations is upheld as it were in HTTPS and restricted to the compelled set of orders, handicapping malevolent assaults execution by means of cloud assault vector.

To guarantee safe help and alleviate unapproved firmware establishment, updates are intended to be carefully marked [33].

3.3 IIoT security with AI

IoT (Internet of Things), as an indispensable piece of both individual lives and modern conditions, has benefitted from AI (Artificial Intelligence) for investigation. It permits associations, cooperation, and information trade among machines and devices for functionality and higher proficiency without requiring any human tuned-in. This computerization requires a gigantic measure of trust while using AI. This reality accentuates why integrating XAI (Explainable AI) in an AI-based IoT framework is fundamental. XAI has drawn in broad consideration late years and an appropriate XAI model ought to be coordinated into the framework to acquire unwavering quality and straightforwardness for AI-based frameworks.

All things considered, TRUST (Transparency Relying Upon Statistical Theory) is a model-freethinker, high-performing, and reasonable framework for mathematical applications. TRUST XAI model is the factual way of behaving of the AI's results in an AI-based framework. It is helpful for the network safety of the IIoT (Industrial Internet of things). Results show that TRUST XAI gives clarifications to new arbitrary examples with a typical achievement pace of 98% [34]. Contrasted with LIME, a well-known XAI model, TRUST is demonstrated to be unrivaled with regards to execution, speed, and the strategy for reasonableness. In spite of TRUST's advantages, it has a few disadvantages also. Because of utilizing data gain in picking the agents, TRUST could overfit the preparation set, which leads to small performance showing on inconspicuous information. If the Gaussian presumption can't be made or the likelihood conveyance of information changes, the result of TRUST wouldn't be solid.

3.4 IIoT security architecture and protection strategy

The IIoT's most basic architecture is made up of three layers: the Data acquisition layer, the Data transmission layer, and the Data processing layer [35] [36]. These layers are the fundamental technology of the underlying industrial IoT system. At the same time, the security flaws in these technical solutions have become the industrial IoT system's "Safety board." According to recent hacker attacks on industrial IoT systems, as well as a slew of security concerns to industrial IoT systems. In order to create a security protection strategy for various industrial IoT applications, we require an industrial IoT security protection framework, like –

1. Data Acquisition Layer Security: It safeguards the security of IoT terminal gadgets. To keep assailants from attacking the modern IoT inner organization through the IoT botnet infection, it is important to direct an inside and out examination of the assault standard of the IoT botnet infection.

2. Data Transmission Layer Security: It is basically used to guarantee the security of information transmission during correspondence, counting personality verification and information privacy of correspondence terminal gear. To guarantee the data transmission layer to give secure and precise information transmission administrations, and to prepare for information robbery and man-in-the-center assaults, the MQTT correspondence convention embraced by most modern IoT frameworks should be encoded and communicated, and it got to by utilizing the MQTT convention.

3. Data Processing Layer Security: Its focal point is to safeguard the security of the correspondence server through traffic investigation. For the MQTT intermediary server broadly utilized in the modern IoT framework, to stay away from the mock bundle assault, the MQTT convention profound parcel review firewall safeguards the MQTT intermediary server and channels out as indicated by the easy access control rules. Strange qualities,

correspondence traffic that doesn't conform to the MQTT convention determination. Simultaneously, for the high-level diligent assault started by the all-around fabricated fashioned information bundle, the interruption identification framework for the MQTT convention is utilized to screen the organization correspondence traffic and the terminal device.

3.5 Blockchain-based security for IIoT

Many proposals have been made to use a blockchain to address the increasing security concerns of IIoT due to its decentralized nature. The use of blockchain in conjunction with IIoT provides a number of advantages in terms of enhancing and resolving some of the security challenges. A blockchain is a cryptographically-secured and temperature-resistant DLT (Distributed Ledger Technology) that connects several computers in a P2P (Peer-to-Peer) network that functions without the involvement of a third party. New blocks are added to the network using consensus techniques including PoW (Proof-of-Work), PoS (Proof-of-Stake), PoA (Proof-of-Authority), and PoET (Proof-of-Elapsed-Time), BFT (Byzantine Fault Tolerance), PBFT (Practical Byzantine Fault Fault Tolerance), and others.

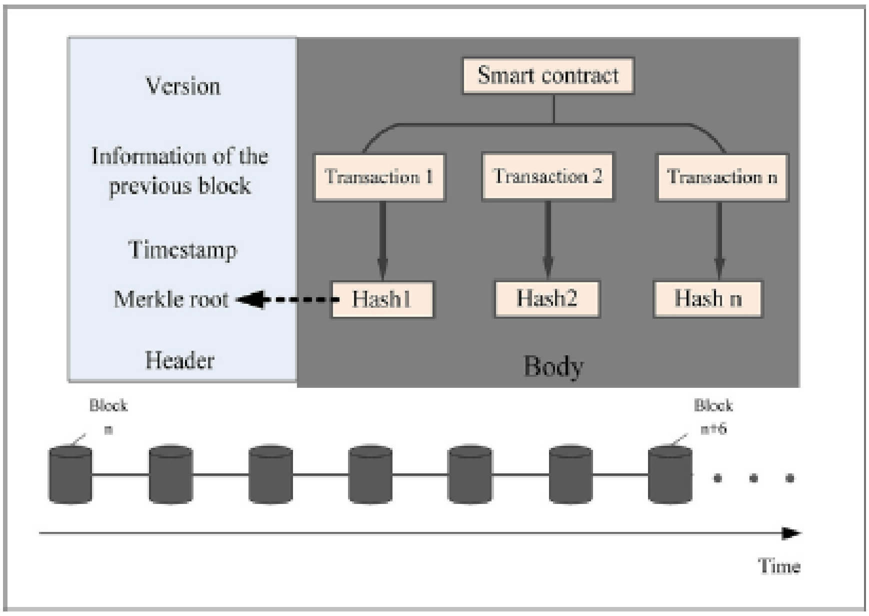

Figure 3. 2. Basic Structure of Blockchain [37]

The blockchain is a progression of information blocks, which are created by cryptography and consecutively associated with hash values. As displayed in Fig. 3.2, each square comprises a header and a body. The header acknowledges most elements of the blockchain, while the body keeps all the exchange data in the past period. The header contains the hash worth of the past block, which is determined by the hash capacity of the header of the past square. The header and body are connected up by means of the Merkle root. Being a significant information construction of the blockchain, the Merkle root can quickly sort and confirm the presence furthermore, the respectability of square information. The decentralized attributes of the blockchain impeccably match the decentralized conveyance of highlight point direct energy exchanges in the Industrial Internet. The highlight point direct energy exchanges in the Industrial Web can disregard the issue of clogging the executives. Contrasted and the brought together electric energy exchange mode, the blockchain framework decreases the working expense of the framework and guarantees working productivity. The detectability, straightforwardness, and non-alter capacity of blockchain information guarantee the reasonableness, security, and data legitimacy of highlight point direct power exchanges. Simultaneously, the shrewd agreement in the blockchain can give security to the two players in the electric energy exchange to guarantee the safe also, smooth advancement of the exchange [37].

3.5.1 Permissioned Blockchain-based Security

A permissioned blockchain has been proposed to use for secure information partaking in IIoT. A permissioned blockchain is appropriate for a gotten IIoT organization of devices on the grounds that an association can characterize the jobs of the members utilizing shrewd agreements and confine their admittance to the organization. The jobs additionally characterize which part can peruse the information of the organization and execute some composing tasks. Agreement hubs assume an essential part across the organization. It guarantees limited execution of exchanges and works on the security of IIoT device correspondence. To accomplish protection and security, this execution is alluring since it characterizes the jobs and access control system of the members, utilizes a savvy contract that stores endorsement fact to ensure controlled exchange conjuring, agreement hubs confirm and verify the exchanges as well as stores the condition of all substances, codes, and information of the brilliant agreement. Additionally, in a permissioned blockchain organization, exchanges are not unknown between the members which gives the association of the blockchain a valuable chance to check who performed exchanges and it helps the administrator to guarantee security and protection. In this way, straightforwardness and trust between the validated gatherings are laid out which is a fundamental prerequisite to improving the security of IIoT. A permissioned blockchain empowered IIoT is reasonable to work on the security of the entire organization and guarantee protection while speaking with different devices [36].

3.5.2 Blockchain-based secure transaction model

The aim of the article [37] is to increase the intelligence, real-time, and security of direct transactions between DEGCs (DE Generation Companies) and customers, as well as to minimize the default frequency of DP (Distributed Power) transactions. A significant volume of P2P (Peer to Peer) energy transactions increases credit risk and complicates DE (Distributed Energy) transaction management in the IIoT. Due to these factors, a universal P2P energy transaction architecture and a universal energy blockchain were developed for use in typical IIoT situations. At first, establishes a DE transaction mechanism within the energy blockchain architecture. The chained transaction design ensures transaction reliability and intelligence. The use of blockchain in credit risk management was investigated when it comes to the credit issuance of DE transactions. A blockchain-based credit evaluation system was created using smart contracts to make credit values open, transparent, and unchangeable. A payment strategy based on credit value was created to facilitate quick and frequent energy transfers in terms of transaction speed and frequency. The transaction policies are continuously changed, and blockchain technology is continuously enhanced. Investigating and implementing blockchain in IIoT DE transactions will be more beneficial.

3.5.3 Blockchain-based secure and efficient energy trading

BC-ETS (Block Chain-based Energy Trading Scheme) is a protected and effective energy exchanging plot in light of blockchain, which is material to the dispersed energy exchanging foundation upheld by the IIoT. The energy trading methodology in BC-ETS [38] is divided into two layers, which can not only protect privacy but also accomplish power supply and demand balance. The electrical energy is held in the energy storage device in the first layer, and the transactions in the private blockchain only transfer energy ownership. The aggregator acts as a manager on the second layer, managing cross-regional energy trading on the consortium blockchain. Aggregators are present on both layers of the system to schedule electric energy in order to balance supply and demand. There are five system flows in the suggested model:

(1) The system's first-level private blockchain transaction information is transferred to the regional aggregator for processing.

(2). Aggregators serve as regional managers, coordinating energy transactions throughout the region.

(3). Choose an accounting node at the second level of the system to handle the consortium blockchain's accounting.

(4). Select the next accounting node after calculating the credibility score.

(5). After each cycle of accounting, switch to the new accounting node.

To improve system availability, a credibility-based equity proof mechanism is also created. It uses the IoT devices' comparatively modest computational power in the energy internet. The investigation reveals that BC-ETS can meet the security requirements and performs better than other similar energy trading schemes. BC-ETS in light of blockchain consolidates cryptographic natives, for example, the elliptic bend calculation, bilinear planning, and advanced signature, which can significantly work on the security of the framework. The security examination is led as follows:

(1) Integrity verification

(2) Data security

(3) Account security

(4) Transaction confirmation

(5) Privacy protection

(6) Cannot reuse energy certificate

By security examination and execution assessment, the proposed plot is ended up being secure as well as proficient [37].

3.6 Cybersecurity and Industry 4.0

IIoT attributes are read up for contrasts among IIoT and IoT, IIoT resource scientific categorization, IIoT security challenges as well as IIoT dangers scientific categorization and assaults situations. It's vital to carry out coordinated security and security the board for Industry 4.0 to join method for insurance for physical, data, and devices spaces. In IoT/IIoT environment there are three the fundamental gathering challenges [39] -

1. Network related with connections and correspondences among endpoints, doors, and clouds.

2. Data examination performed for handling, sifting also, and collection of the information coming from the IoT devices in various levels of the IoT environment.

3. Incorporation empowering ongoing bidirectional stream of information, like cloud APIs and remote order, what's more, control of IoT gadgets through the cloud.

The ENISA (European Union Agency for Network and Information Security) archive gives the consequences of a hole examination directed to distinguish principal challenges furthermore, proposals of IoT/IIoT. The IoT/IIoT Security Framework developed by ENISA is based on semantic details from six ENISA documents, including -

1. Security and Resilience of Smart Home Environments. Best practices and suggestions (2015).

2. IoT Security Recommendations for Critical Information Infrastructures in the Context of IoT (2017).

3. IoT Security Best Practices in the Context of Smart Manufacturing (2018).

4. Towards a secure Cloud and IoT convergence (2018).

5. Gap Analysis of IoT Security Standards Mapping existing standards versus security and privacy concerns in the IoT space (2018).

6. Cybersecurity in Industry 4.0: Challenges and Recommendations (2019).

3.7 IIoT digital forensics and security issue

The improvement of forensic examination and IIoT uncovers security concerns and significant related work to do to have a safer computerized world. The measurable associations all over the planet are disturbing to the associations about interruption and weaknesses. The installed frameworks and shrewd gadgets are expanding in number for public utilization transparently need to address, what's more, teach the current populace across the globe. The IIoT contraptions and presentation of touchy data raise the need to develop conversations among scientific agents within associations and scientific agents.

The major FS (Forensic Security) capabilities are designed to protect connected smart devices and systems equipped with intrusion detection systems. Where sensitive data is securely transported to a secure location or kept on a cloud or local server. The more advances in technology are made, the more crucial IIoT devices are connected in a secure environment using appropriate software and smart mobile-based applications. Vulnerabilities will exist in these unsecured devices, and intruders will be able to access them from anywhere. The FI (Forensic Investigations) to gather evidence at the device level is a little easier with secure connectivity and environment, but IIoT-based with many varied configurations and devices in place will be a major issue for FI [40].

3.7.1 IIoT Identified Security Threats

The IIoT forensic investigation will be undertaken using the framework outlined above, which is one of the most effective forensic investigation models currently available. In today's digital environment, security worries about IIoT smart devices arise at various times, including mechanical, moral, and security concerns.

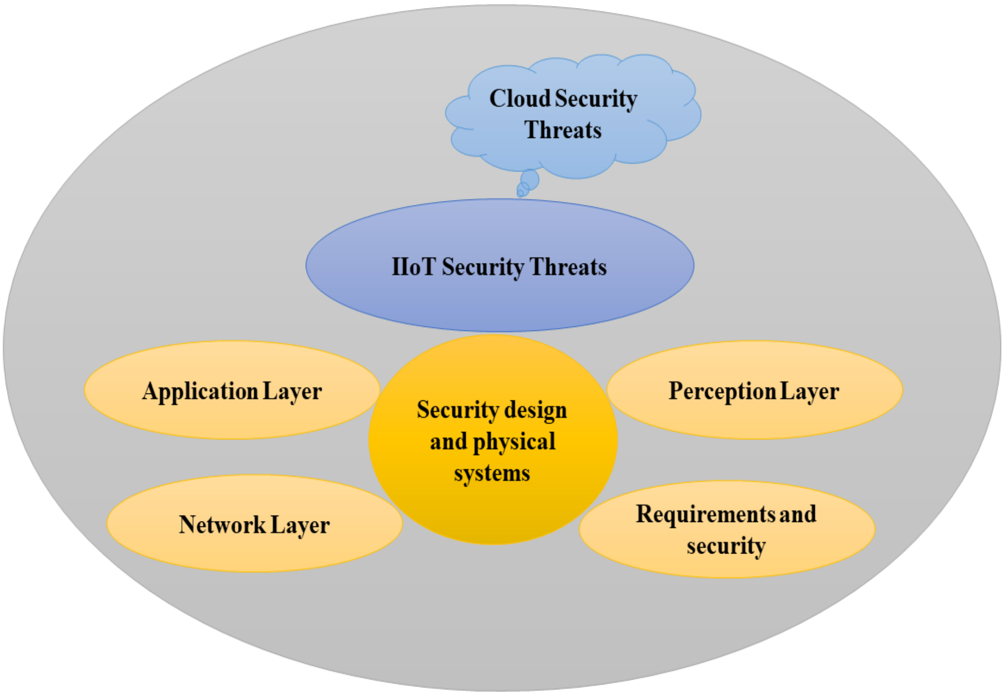

Figure 3. 3. IIoT Security Threats [40]

Fig. 3.3. depicts a fundamental security concern as well as a comparison of the number of layers and connections in the current environment. The researchers are working on various IIoT architectural structures. Because of technological developments and various smart gadgets in today's digital age, there is some ambiguity about the end consequence.

3.8 IIoT security & graph-based framework

IIoT alludes to the use of IoT in modern administration to work on the by and large functional productivity. With IIoT that speeds up the modern computerization process by enlisting a huge number of IoT devices, solid security establishments are to be conveyed befitting the dispersed network also, obliged functionalities of the devices. Late years saw serious assaults taking advantage of the weaknesses in the gadgets of IIoT organizations. Besides, attackers can utilize the relations among the weaknesses to infiltrate profound into the organization.

Graphs, being effective to address relations among elements, can encode the weak relations in the organization successfully. A graph-based security framework is a solution that protects the IIoT network against vulnerabilities found in network devices. This framework can be divided into three steps, like as – pre-processing, graph modeling, and Analysis. This graph is used to determine crucial parameters that represent various security-relevant network information. Risk mitigation measures lower the network's overall threat level. The proposed model and methodologies allow a security administrator to see the threat levels posed by the network's vulnerabilities. It also provides a platform for security administrators to determine the best threshold values for threats, hops, and hotspot indexes within the IIoT network's limits. The techniques pave the path for a more secure IIoT world [41].

3.9 IIoT security & decision-making model

In today's world, industrial growth is a slew of activities where an organization's effectiveness and efficiency are heavily reliant on how it analyzes business data. The IIoT, an innovative industrial initiative, facilitates resource utilization, cost-effective manufacturing, and product specification. Advances in communication and control technology have led to the emergence of a new generation of infrastructures that can manage an increasing number of tasks without human cooperation. Furthermore, intelligent and smart objects/sensors are continuously expanding in scope and capability to meet consumers' needs. For Order Preference by Similarity to the Optimal Solution, can give secure data transmission furthermore, recording/capacity utilizing different imparting boundaries.

All things considered, a novel and productive direction cycle guarantee smooth information transmission and information dividing between network elements. This model arranges huge boundaries utilizing the TOPSIS (Technique for Order Preference by Similarity to the Ideal Solution) strategy for its dynamic model with the IIoT to guarantee productive detecting reports and getting information transmission among IoT devices. It recognizes genuine IoT devices utilizing the TOPSIS technique so the CM could distinguish right detecting reports while dealing with the accessibility of records, move of information over the Internet, and so on. Besides, SAW (straightforward added substance weighting) was utilized to get a weighted amount of presentation rating of every elective's general attributes. It was altogether quicker and better at accurately arranging the sent information through the TOPSIS and SAW components. Moreover, the component was approved widely utilizing different assessment standards such as information transmission, the exactness of shared information, and detecting time. Besides, the reenactment results recommended that our proposed model accomplishes an 85% improvement in progress rate in contrast with the current methodology [42].

3.10 Deep Learning based security issue for IIoT

To manage the investigation utilizing such an enormous measure of IIoT information, unique DL (Data Learning)- based logical models are conveyed. The educational experience in a scientific model requirement to follow a solid and reliable life cycle for urgent investigation and independent direction. Likewise, considering the weaknesses in various levels of an IIoT organization, the growing experience ought to be solid and dependable. A dependable DL-based system is proposed to steer the assault identification plots for IIoT. This system considers ill-disposed preparation of the model for recognizing expected assaults in RPL (Routing Protocol in Low-Power and Lossy Networks). This aids in accomplishing a dependable learning model. A GAN-C (Generative Adversarial Network-Classifier) strategy has been created for assault location occasions which is a two-phase mix of GAN and SVM models. Here assesses the exhibition improvement in GAN-C regarding an independent SVM (Support Vector Machine) classifier. The proposed technique embraces equal learning and recognition model which upholds DL on computationally obliged IIoT gadgets. The aftereffects of the equal model are assessed in an IIoT organization to draw an exhibition correlation among disseminated and incorporated assault identification in an RPL network. The utilization of the equal GAN-C model likewise shows a critical decrease in preparing time [43].

In IIoT, the data correspondence advancements empowered by IoT could significantly work on the productivity and practicality of data trades between both vertical and flat framework mixes. Similarly, AI calculations, especially DRL (Deep Reinforcement Learning), are feasible for aiding robotized control of perplexing IIoT frameworks, with the backing of conveyed edge registering foundation. DRL calculations gain proficiency with a strategy that maps crude inputs straightforwardly to the circulation of activities, with the goal of amplifying the prize capacity. To become familiar with the approach, the DRL calculations depend on DNNs to separate elements that inexact the worth works straightforwardly founded on the gathered crude information. Notwithstanding recognizable execution enhancements of DNNs, the security dangers acquired by enormous interconnections IoT and the weaknesses of profound brain networks utilized in DRL should be entirely researched and moderated before broad sending. A DRL-based regulator was planned that could be conveyed at the edge processing server to empower robotized control in an IIoT setting. At that point, explore noxious ways of behaving of enemies with two assaults: (i) work-based assaults that can be sent off during the preparing stage and (ii) execution-based assaults that can be sent off in the wake of the preparing stage, to concentrate on the security effects of weak DRL-based regulators. According to the foe's viewpoint, the greatest entropy IRL (Inverse Reinforcement Learning) is utilized to surmise a prize capacity through the perception of framework directions heavily influenced by prepared DRL-based regulators. The approximated reward work is then used to send off assaults by the foe against the DQN (Deep Q Network)- based regulator. Through reenactment, assess the effects of two explored assaults, observing that assaults are progressively effective with expanding precision of the control model. Besides, talk about certain tradeoffs between control execution and security execution of DRL-based IIoT regulators, and framework a few future examination bearings to get AI to use in IIoT frameworks [44].

4. USE CASES AND APPLICATIONS OF IIOT

Modern applications are encountering expanded security gambles because of their functional reconciliation with data innovation furthermore, openness to the digital world. The innovation behind this incorporation is the IIoT, which is utilizing n-ICS (Networked Modern Control Frameworks). Security in the IIoT coordinated modern applications and advances is an extraordinary worry as this is a half and half mechanical development of IoT, CPS (Cyber-Physical Systems), and Big Data. IIoT is the driving innovative starting point for the control and activity of SIA (Smart Industrial Applications). SIA incorporates savvy power frameworks, compound, petro-synthetic, fabricating, food and drink, and some more. Training and control of these advances are turning out to be increasingly more essential with the incorporation of IIoT what's more, digital organization. IIOT and the n-ICS incorporate OT (Operation Technology) with IT (Information Technology), consequently, the activity of modern applications is slowly confronting security and takes a chance for its ensuing incorporation with web innovation. Industrial procedures, such as asset performance monitoring, workflow optimization, and plant safety management, heavily rely on OT domain data in their production processes [45].

4.1 Use case in Industrial Sector

3 fundamental difficulties have been distinguished in the utilization of the Confirmation Case technique for IIoT. To accomplish an overall objective, we examine the three following issues. At first, a short examination of cutting edge explores and assets in the area of Confirmation Case is finished. Also, we discuss unambiguous parts of the IIoT Affirmation Case with a center around Security Affirmation. Finally, an advancing course is created to satisfy the hole in security and well-being shown by IIoT, which is addressed in Figure. 5.1 [46].

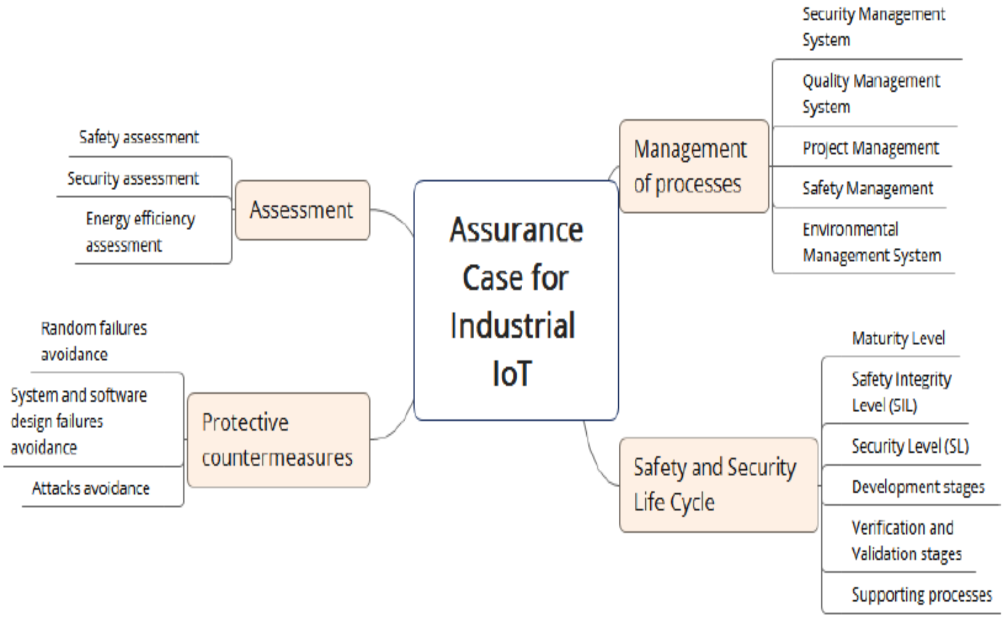
Assurance Case for Industrial IoT
Assessment
Safety assessment
Security assessment
Energy efficiency assessment
Protective countermeasures
Random failures avoidance
System and software design failures avoidance
Attacks avoidance
Management of processes
Security Management System
Quality Management System
Project Management
Safety Management
Environmental Management System
Safety and Security Life Cycle
Maturity Level
Safety Integrity Level (SIL)
Security Level (SL)
Development stages
Verification and Validation stages
Supporting processes

Figure 4. 1. Structure of Assurance Case for Industrial sector in IoT [46]

Validation of a suggested architectural model [47] has been shown and analyzed as an assault on a water source, on the basis of this IT and OT integrated flow control system communication infrastructure for n-ICS. Network-based on the IIoT there are 4 components to infrastructure: n-ICS backed Factory local area network (FLAN), manufacturing network zone corporate cloud, headquarters/IT network, and WLAN incorporates demilitarized zones (DZs) and HQ local area networks (HLAN) for the headquarters zone (DMZ) (HQ). It has been MN utterly isolated from all other networks by a specific firewall. Consequently, MNZ IT devices can be safeguarded. it would be challenging to get through this firewall with physical systems to safeguard using conventional security procedures.

4.1.1 Safety issues in the Industrial sector

Terrible incidents frequently happen in the sector, primarily due to carelessness and improper employee oversight. The purpose of death, disability, and property harm. Exploiting fires and poisoning Gas leaks are major causes of accidents in the sector. When an accident occurs, prevention is preferable to intervention happens. Tracking and warning are the only ways to prevent these occurrences before the disaster happens [28].

4.1.2 IIoT reusable components

The two IIoT applications that were chosen, Smart Logistics and Predictive Maintenance, include a wealth of linked data, actors, and process flow interactions. Actors consist of suppliers, buyers, logistics service providers, transportation automobiles, shipping containers, pallets, manufacturing equipment, workforce, robotics, etc. These participants are shoppers and producers of data who work with reusable parts. A logistics application primarily refers to the exchange of products between involved parties. Along with handling and environmental conditions, it also entails tracking and monitoring these commodities. Predictive In manufacturing, maintenance is used to anticipate when machines in a production line will need repair, either due to unexpected machine failure or due to expected wear of machine parts. Maintenance is planned for and carried out with a minimum of disturbance to the production schedule [48].

4.1.3 NLI in IIoT application

In [49] proposed a use case of Natural Language Interface (NLI) in IIoT implementation. They show a beginning stage plan standard of a semantic portrayal to communicate IIoT connections and propose an information-centered work process of IIoT mechanization framework design. IoT networks are getting harder to manage and govern as smart devices and sensors become more widely available. NLI would enable people to communicate with the devices using human language by translating the user instruction into a meaning representation that a computer can understand, also known as a logical form. By adopting human language as an input format, NLI simplifies human-machine communication. Commercial virtual assistants with NLI have been widely utilized in homes up until this point, including Google Assistant and Amazon Alexa. Despite the rapid advancement of conversational interfaces in smart home and personal intelligent assistant use cases, industrial sensor and actuator networks, often known as the IIoT, have received relatively less attention in terms of research and implementation of IIoT.

4.2 Manufacturing Sector

IIoT gives significant data to deal with improvers to get to information and assess them all the more rapidly, independently, and from a distance and make the fundamental cycle transformations in a modern plan of action. This likewise upgrades the speed at which Functional Insight and Business Knowledge changes and improvements are carried out to carry serious advantages to numerous enterprises. The execution of Modern IoT frameworks empowers programmed stock observing, confirmation of plan consistency, and cautioning when deviations happen. It can permit the observing of creation lines from the refining system to the pressing of completed merchandise. This extensive constant checking of the cycle prescribes functional alterations to work on functional expenses for the executives. Makers use IoT to consolidate energetic, capable, and mechanized creation tasks, in which upkeep plans are free. The applications and advantages of IIoT in manufacturing sectors are given below [30] -

- ✓ Machine observation
- ✓ An increase in production
- ✓ Worker Security
- ✓ Increased upkeep
- ✓ Real-time data
- ✓ A decrease in manufacturing costs
- ✓ Smart Supply Chain
- ✓ Smart Supply Chain
- ✓ Automated vehicle operation
- ✓ Lessens errors
- ✓ Acquire important knowledge
- ✓ Safety
- ✓ Product testing and continuous improvement
- ✓ Data Gathering
- ✓ Improving product quality
- ✓ Decision-making
- ✓ Intelligent factories

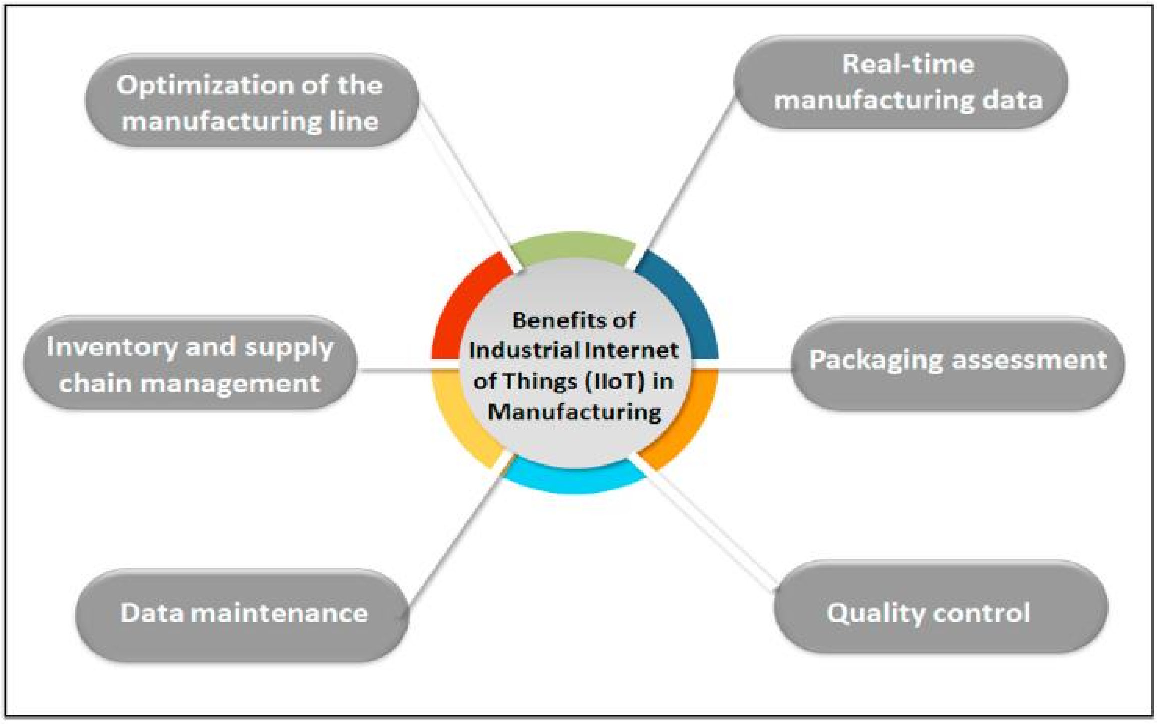
Optimization of the manufacturing line
Real-time manufacturing data
Benefits of Industrial Internet of Things (IIoT) in Manufacturing
Inventory and supply chain management
Packaging assessment
Data maintenance
Quality control

Figure 4. 2. IIoT in manufacturing sector [30]

Manufacturing sector is one of the most important use cases in IIoT field; that's why the more details regarding this sector is discussed in the next chapter.

4.3 Garments Sector

The sewing area is where the majority of the production in the clothing business takes place. It is a laborious process since the tailor must work at a high rate of speed while carefully monitoring and controlling the desired quality attributes. By integrating IIoT, sewing parameters may be monitored and controlled in real-time utilizing LED, a small LCD display, a buzzer, etc. This enables the tailor to work effectively by taking prompt corrective action when necessary. The study thus focused on adopting IIoT-based solutions to monitor sewing operation-related concerns and generated a chance to change labor-intensive processes into a smart production line by employing IIoT in the clothing-making process the process of making clothing [50].

4.4 Health Sector

Nowadays, we are seeing the expanded utilization of shrewd devices and correspondence applications in medical services observing, what's more, their effect on the exercises of medical doctors, nurses, and patients, as well as the medical services industry. It is assessed that by 2020, the IoT will contribute $1.9 trillion to the worldwide economy and $117 billion to the IoT-based medical services industry. In view of this gauge, it is normal that IIoT-driven medical services observing is an arising medical care administration that may possibly reform the medical services industry IIoT has an exceptional impact across numerous enormous and little medical services businesses. Accordingly, a rising number of wearable IoT sensors, instruments, and applications are being utilized for various checking applications to keep away from preventable demise because of emergency clinics or other related mistakes. The blunders might happen previously, during, or after hospitalization. Right now, IIoT can possibly save 50,000 individuals every year in the US by staying away from preventable passings because of medical clinic blunders. It guarantees patient prosperity and security by organizing basic patient data and synchronizing related assets quickly through interconnected sensors.

Protected and top-notch medical care administration is of central significance to patients. Yet, one of the significant issues in the IIoT-based medical care framework is the assurance of protection. In general, a medical care specialist organization gets information from its clients and offers them enrolled centers or medical care experts. The supplier may likewise appropriate the information to medical coverage organizations also, drug organizations. Additionally, patient information can be helpless against programmers during cloud moves or on the other hand synchronization with interconnected gadgets. Along these lines, we really want to shield this data from unapproved access, which might bring about the posting of individual data in the public area, or obstruct fundamental clinical hardware. A security break of a patient's observing devices and information might cause the patient social shame, mental issues, or antagonistic actual impacts. Subsequently, information assurance in the type of watermarking and validation is vital in an IIoT-based medical services framework.

Here, a monitoring framework for the health IIoT is shown, where ECG and other healthcare data are gathered by mobile devices and sensors and securely communicated to the cloud for easy access by healthcare experts. To prevent clinical error and data fraud, healthcare providers will use signal augmentation, watermarking, and other analysis. By implementing an IoT-driven ECG-based health monitoring service in the cloud, this approach's appropriateness has been verified through simulation and experimental evaluation [14].

Other authors [51] [62] proposed a wireless multimedia medical sensor network-based platform for safe context-sensitive seamless identity provisioning (CSIP) mutual authentication for the healthcare system. In order to reduce computational costs and achieve WMSN security objectives including session-key agreement and resistance to privilegedinsider, replay, user masked, and secret gateway guessing attacks, this study has taken advantage of the two-factor technique. The suggested authentication satisfies the requirement for platform adaptability, making it appropriate for all real-time, mission-critical application systems. Additionally, the suggested technique demonstrates that it requires less computation to boost system performance efficiency. Additionally, it resolves the inherent trade-off between security level and increased communication overhead, resulting in better bandwidth usage and fulfillment of the needs for both security and real-time [52].

4.4.1 IIoT, Industry and Hospital 4.0

The ubiquitous application of the IoT paradigm along with analytics and artificial intelligence in industrial applications is known as the IIoT. The idea of Hospital 4.0 is an extension of I4.0, and it is predicated on the interaction and collaboration of cyber-physical systems, IoT sensors, internet-based services, and people in the delivery and consumption of healthcare services. Similar to I4.0, the prerequisites for a genuine adoption of the H4.0 paradigm can be broken down into 3 categories [53] :

1. Inescapable dissemination of sensors, ready to gauge the patient and climate

2. Enormous correspondence capabilities

3. Capacity to store, recover and expound massive volumes of data

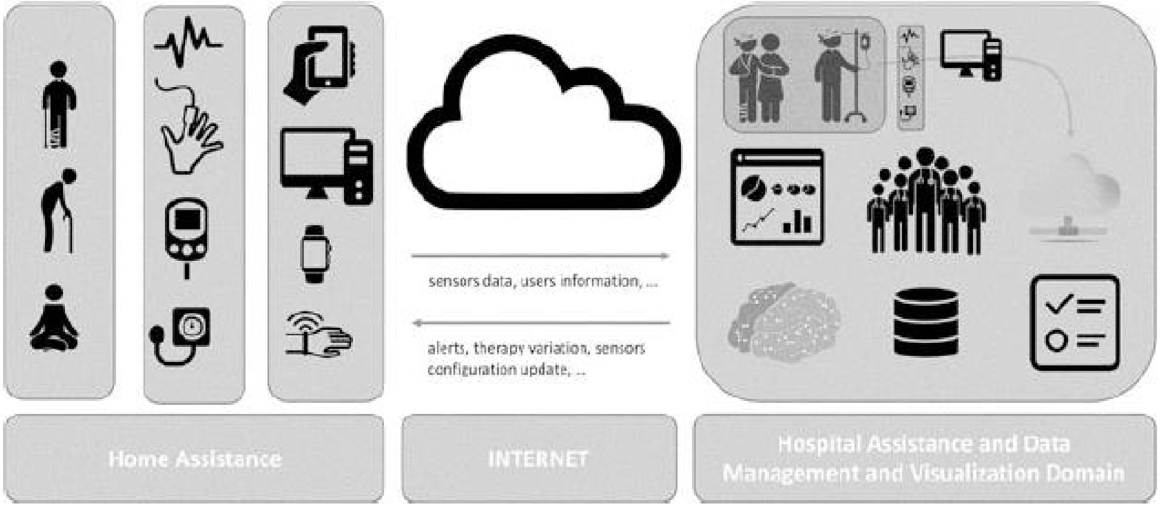
sensors data, users information, ...
alerts, therapy variation, sensors configuration update, ...
Home Assistance
INTERNET
Hospital Assistance and Data Management and Visualization Domain

Figure 4. 3. Model of Hospital 4.0 [53]

A new hospital concept called H4.0 that makes use of all cutting-edge technologies is seen in Figure. 4.3.

4.5 Educational Sector

For educational institutes this means adjusting their instructive proposal to the new advanced necessities - understudies ought to be capable to tackle complex issues that are connected with IIoT. A promising methodology in this set comprises dynamic learning which allows understudies the opportunity to independently foster savvy fixes. Consequently, comments that conventional learning plants are increasingly changing to advanced learning industrial facilities. Understudies need to procure new abilities in both hypothetical as well as useful angles. The last option becomes significantly more significant since the joining of cross-area ideas and frameworks requires the experience of framework limits. Computerized learning manufacturing plants are a promising idea to apply case-based situations in a modern close-to-creation climate. Subsequently, expert understudies are taught inside the advanced learning manufacturing plant Shrewd Creation Lab on the off chance that based courses.

In order to tackle an interdisciplinary challenge, students offer an IIoT case-based paradigm where they model and execute a real-time data flow. They learn firsthand how to link systems and capabilities from shop floor equipment to real-time reporting to increase the transparency of the manufacturing process. In request to give future workers the skill and capacities they need to carry out these IIoT use cases in industry utilizing the IIoT-design. This engineering empowers research-situated showing in an exceptionally youthful field of modern exploration [54].

5. ADVANTAGES OF IIOT IN MANUFACTURING PROCESS

Every day, manufacturing includes more intricate processes, and these intricate mechanisms need sophisticated monitoring systems to guarantee high quality. Direct data from the production processes can be provided through industrial IoT.

5.1 IIoT Advantages

Following the development of Industry 4.0, the manufacturing sector and other related industries became more responsive, dependable, user-centric, and productive enough to explore innovative business plans that reduced downtime, maximized asset utilization, allowed for remote diagnosis, and allowed for proactive and predictive maintenance, etc. The following is a list of the top benefits of IIoT [55] -

a) Increase Productivity: Industry 4.0 empowers the production lines to be more adaptable, and dynamic, outfitted with keen sensors, actuators, and independent frameworks.

b) Cost minimizing: One of the essential objectives of industry 4.0 is to diminish the general expense by decreasing waste creation and expanding benefits.

c) Realtime monitoring: Fame is a significant consider the whole business world as it further expands the interest for the items which is the main objective of any advertising association. Through constant observation of the creation framework, the general speed of the efficiency can be developed which influences the overall inventory network.

d) Improve working environment: Real-time HVAC systems, safety, and security, cleanliness, humidity and radiation detection, communication, and collaboration facilities have all advanced thanks to modern ubiquitous computing and other enabling technologies of the IIoT, which give factory workers a better and more comfortable working environment.

e) Improve effectiveness: To maximize competitive advantage, the industry manager must manage scalability, flexibility, and agility.

5.2 Application of the smart manufacturing sector

Big data and machine learning are combined in the IIoT. Scalability, real-time capabilities, interoperability, data protection, and security are essential components of an IIoT architecture. In an industrial business model, process improvement specialists can use IIoT to collect data and assess it more quickly, independently, and remotely. The following are significant IIoT applications in the manufacturing sector [56] –

- ✓ Machine monitoring
- ✓ productivity improvement
- ✓ Improved maintenance
- ✓ Reduction in manufacturing
- ✓ Worker safety
- ✓ Built-in intelligent network
- ✓ Real-time information
- ✓ Smart pumping
- ✓ Simplification of production
- ✓ Tracking machines
- ✓ Automate driving system
- ✓ Smart Supply chain
- ✓ Monitoring of product development
- ✓ Reduction in expenses
- ✓ Reduces mistakes
- ✓ Gain useful information
- ✓ Security
- ✓ Testing of products
- ✓ Enhance product quality
- ✓ Decision making

5.3 Four industrial revolutions with smart manufacturing

The initial, two Industrial Revolutions were driven by new advances that could produce steam (1700s) and power (1800s). The third modern upset was driven by both new, mechanized, actual advances and the original data innovations that included sensors, machines, and programming (1900s). The new blast of new interchanges and sensor innovations has empowered universal actual availability among smart gadgets, machines, sensors, and actuators which is called IIoT (today). A comparative blast of new information investigation innovations, particularly, Artificial Intelligence, has empowered general admittance to cloud-based insightful administrations. The two innovations have given the groundwork for the fourth modern unrest. Manufacturing is now becoming a part of the global smart ecosystem known as smart manufacturing thanks to the pervasive physical and informational connectivity. What is typically referred to as Industrial Revolutions is almost always highly beneficial to manufacturing [28].

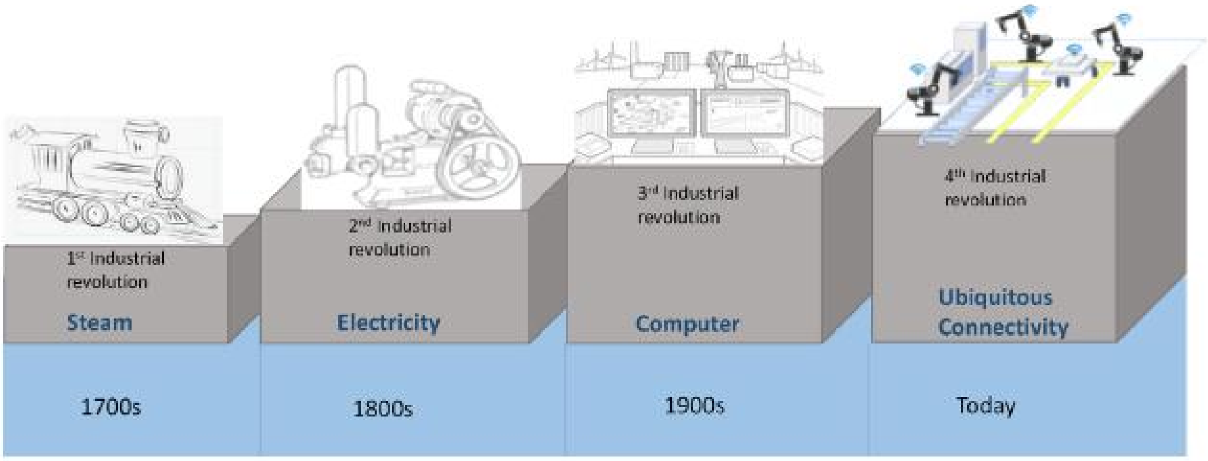
1st Industrial revolution
Steam
1700s
2nd Industrial revolution
Electricity
1800s
3rd Industrial revolution
Computer
1900s
4th Industrial revolution
Ubiquitous Connectivity
Today

Figure 5. 1. Four Industrial Revolutions [28]

5.4 Advantages of IIoT in manufacturing factories

The advantages of IIoT in manufacturing are listed here [56] [51] –

a) Remote Management: IoT-enabled devices and machines enable partners to connect digitally so that they may exchange operational data and commands.

b) Packaging Assessment: IoT sensors are used in building an intelligent asset management system in manufacturing machinery and equipment to allow condition-based repair and maintenance notifications.

c) Real-time Manufacturing Data: IIoT sensors assist in locating and monitoring important assets, tracking and tracing inventories, and events along the supply chain, and informing clients of any material deviations.

d) Inventory and Supply Chain Management: Real-time data on the supply chain can be accessed using the IIoT. As they move through the supply chain, products, machinery, and materials can all be smoothly tracked.

e) Quality Control: IIoT engages the creators to assemble full information connects with unrefined components utilized and its piece which are used for tackling distinct quality-related matters and right them.

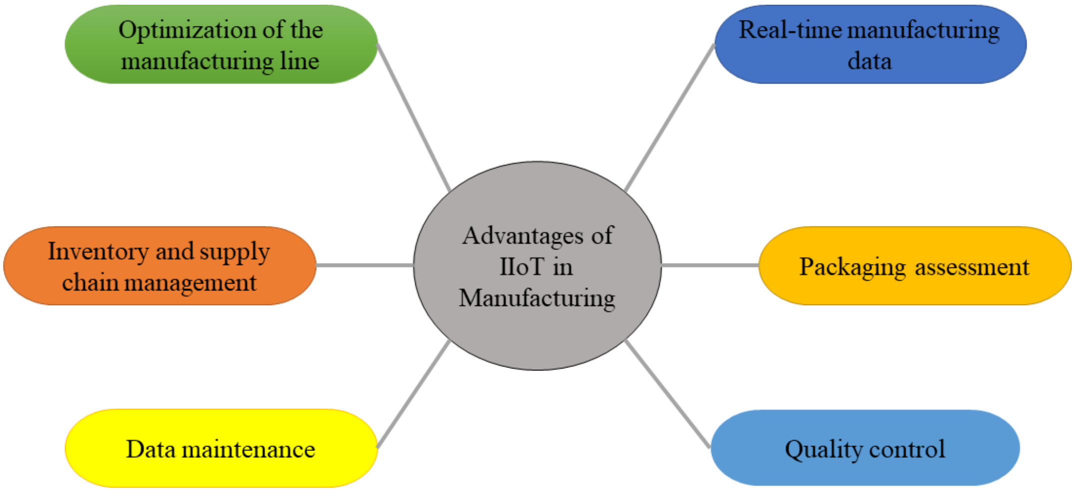
Optimization of the manufacturing line
Real-time manufacturing data
Inventory and supply chain management
Advantages of IIoT in Manufacturing
Packaging assessment
Data maintenance
Quality control

Figure 5. 2. Advantages of IIoT in manufacturing [56]

f) IoT Operations Management: The ascent of different IoT plans has made a demand for information technology development teams in the engineering and manufacturing sectors.

g) Optimization of Manufacturing Line: IoT sensors in items help the makers can acquire experiences in the use designs, item treatment of various clients, and follow item.

h) Return on Investment: By connecting an ever-increasing number of objects and pieces of machinery in an intelligent network, IoT enables businesses to create enormous economic value through innovation and offers the high returns on investment.

i) Data Maintenance: Data is continuously gathered from every piece of machinery using an IoT sensor device, and it may be further analyzed using big data to make important decisions. The use of devices and business systems generates huge data that aids in the creation of new ideas, business processes improvement, and discover new insights.

j) Security: IIoT-related large information investigation assists with working on the general workforce's wellbeing, and security in the manufacturing plant.

5.5 Challenges and Opportunity of IIoT in manufacturing

The adoption of IIoT still faces several difficulties despite having a large range of applications with potential advantages. Some of the main obstacles to the adoption of the IIoT are listed here [55] [51] –

a) Heterogeneity: The IIoT faces difficulties when attempting to communicate via sensing technologies and provide universal access to the shared data produced by machines due to the amalgamation of numerous heterogeneous devices/machines, complex system architectures, and heterogeneous hardware and software platforms. So, heterogeneity is a significant problem for IIoT applications.

b) Data integration: IoT-enabled sensors gather unprocessed industrial data from multiple areas/branches of the business. This data is quite complex because it can be huge data that is both structured and unstructured with different dates. Thus, there is a complex relationship between the data from many industries. So, integrating the data is important to utilize it to the organization's advantage.

c) Cybersecurity: The ongoing Industry 4.0 and IoT together vow to present strong plans of action through stable availability and productive utilization of cutting-edge universal inserted frameworks. These frameworks produce, dissect, and share basic and delicate business information that should be safer and shielded from Cyber-assaults as this may seriously harm the association too as it very well may live compromise. Accordingly, security and protection together are the innate test in the IIoT framework.

d) Connectivity and Visibility: One more confounded challenge during the execution of IIoT is the absence of availability between various parts and machines for the executives.

e) Scarcity of standardization: As work to embed ongoing innovation onto previous, it experiences an extensive variety of different norms and plans standards in every element from transmission convention to different entertainers in the IIoT framework.

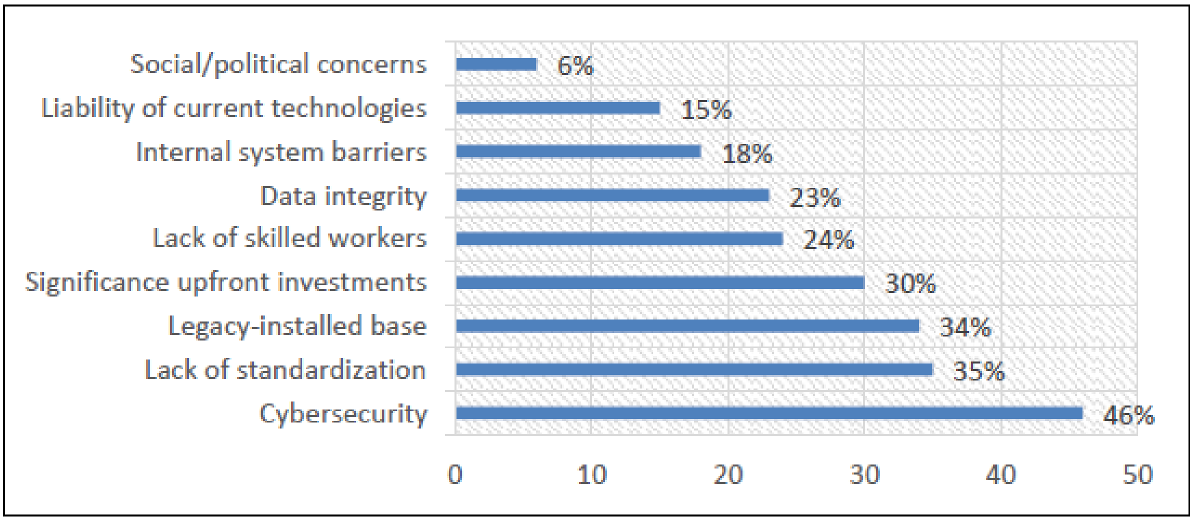

Figure 5. 3. Challenges percentage in performing IIoT [55]

f) Integration of Traditional System: IoT integration for industrial settings is more complex than for traditional Machine-to-Machine and networked devices. To fix the problems, the industrial challenge is to combine outdated equipment with cutting-edge technologies.

g) Scarcity of expertise people: A significant justification for why business associations are as yet not anxious to take on IIoT as detailed by the study is an absence of talented specialists. In this advanced time, organizations can't play out the whole errand in isolation. They should rely upon current systems administration advances, environments, and working stages which are extremely basic to win.

h) Capital: It is crucial to use new technology with qualified professionals and people to automate everything and achieve optimization. Therefore, firms must wisely pay for upfront costs while considering the future benefit.

5.6 Overcome the Challenges of IIoT in manufacturing factories

Designing and assembling organizations confronting IIoT challenges today might appear to be overpowering. Execution of nature of IoT innovation, the venture of enormous sum in industry foundation and IIoT structure can be the answer for the difficulties of IIoT. The accompanying are the different perspectives to beat the difficulties of IIoT by the producers [51] :

a) Decentralization: Decentralization of the board empowers producers to conquer the difficulties of IIoT.

b) Edge Computing: Edge computing is a distributed computing technique that uses edge or smart devices as the computer nodes. By sending data at the edge of networks, it helps to lower transmission costs, reduce latency, speed up fault reaction time, and improve user experience. Edge computing performs real-time data analysis and aids in rapid data delivery. Increasing the market for edge computing is a current trend that addresses the IIoT problems.

c) IIoT Gateway: One answer to the IIoT difficulty is the integration of the IoT gateway with the business's current infrastructure. It offers a safe connection to any industrial infrastructure and aids in resolving interoperability and machine-to-machine communication problems.

d) Clustering of IoT Gateway: IoT Gateway clustering ensures the continuity of cloud connectivity and data storage while assisting in the resolution of issues that came up during the integration of OT systems with IT systems.

5.7 Key foundation of IIoT in the manufacturing sector

Establishing a cyber-physical-based manufacturing system is a shared objective across all advanced smart manufacturing modes (CPMS). The CPMS has garnered a lot of interest from both academia and business and has recently displayed the following technical tendencies [57].

i. Interconnection of shop-floor heterogeneous creation factors: Because of the design of IoT, all heterogeneous elements in shop-floor can be detected dependably, and the monstrous assembling information of which can likewise be sent progressively. In this way interconnection of all heterogeneous shop-floor creation, factors can be accomplished.

ii. Big data analysis on manufacturing: With the big data investigation techniques, the assembling information gathered on the shop floor can be utilized to make an examination, including creation hardware wellbeing appraisal and anticipating, item quality and dependability investigation, creation task planning and gauging, and creation process coordinated effort and streamlining.

iii. Service-oriented manufacturing innovation: Based on arranged assembling innovation, actual assembling assets are virtualized with the hypothesis of advanced depiction and distributed computing. As to the requests of creating tasks, producing administrations are looked at, joined, coordinated, and improved to acknowledge sharing and collection of different assembling administrations. In a cloud manufacturing stage, various information things of an assembling gear will be utilized for various independent direction errands like assistance choice, synthesis, and planning [58].

iv. Virtual reality with Smart Manufacturing: By implementing virtual reality and augmented reality technology in product design, manufacture, maintenance, and production equipment overhaul, will increase production efficiency, lower production costs, and improve product quality.

v. Cloud computing with Smart Manufacturing: A service-oriented manufacturing paradigm known as cloud manufacturing provides for ubiquitous and on-demand network access while virtualizing manufacturing resources as manufacturing services that can be managed in the cloud in an unified manner. To enable effective on-demand creation of highly customized products, cloud manufacturing attempts to effectively integrate and share distributed manufacturing resources. Higher standards for computer technology have been proposed by the CPMS to enhance simulation, analysis, and decision-making capabilities [58].

6. CONCLUSIONS

The IoT is a network of objects with distinct element identification, embedded software intelligence, sensors, and pervasive internet connectivity. Over the past few years, IoT has significantly increased in popularity, if not attention, in academia and business [59]. It enables remote sensing and management of objects on top of the existing network infrastructure. Creating opportunities for a closer link between computer-based systems and the physical environment. It allows for a large number of resource-constrained, communication-capable heterogeneous smart items with specific or general purposes. The IIoT was created in recent decades by the fusion of traditional production engineering, automation, and the IoT. The IIoT is a physical network of things, items, or devices for sensing and remote control, that enables better integration between the physical and virtual worlds. One of the best-known technology concepts is the IIoT, which involves enablers [26].

Industrial machine sensors and actuators are connected to local processing and the Internet, and then to other significant industrial networks that can produce value on their own. These are the two main components of the industrial internet [60]. The start of the 21st century is set apart by the fourth industrial revolution, otherwise called Industry 4.0, and the advanced change of business. Industry 4.0 and the underlying digital transformation are both advancing exponentially [61].

In Industry 4.0, interconnected PCs, machines, and smart materials associate with each other and the climate to convey and, in the end, settle on decisions with almost no human mediation. Predictive maintenance is made possible by the IIoT, which is employed in the manufacturing sector. It is the emerging pattern of the modern revolution, equivalent to the IIoT, and alludes to the fourth modern upheaval, as portrayed in the title picture. The term is interchangeable with IIoT and is currently perceived around the world. Industry 4.0 isn't just about putting resources into new innovations and apparatuses to further develop production effectiveness. IoT, IIoT, and Industry 4.0 are firmly related ideas, but they can't be reciprocally utilized.

In this report, we have defined IoT, IIoT, and Industry 4.0, as well as their key features, applications, prototypes, and use cases. Besides, we have discussed the security challenges of IoT and IIoT for their realization. Since IIoT applications are a logical development of IoT, IIoT inherits some IoT security problems due to the two technologies shared fundamental design. Over the years, a number of activities have been completed, including research investigations, theoretical analyses, experimental sessions, and standardization initiatives. The main goal of our study is to give a systematic overview of the evaluation of the IIoT, which provides ideas for a new range of services and user encounters. This thesis endeavors to examine the potential momentarily character goal frameworks that might be utilized in the IIoT. Researchers may be inspired by this review to pursue better solutions to various IoT and IIoT-related issues in the next generation and learn how this technology will take the world to the next level. The limitation of our work is that there is no implementation to evaluate it. The future work will be to develop the system and make collaborations with the 5G.

REFERENCES

[1] A. Kalla, P. Prombage, and M. Liyanage, "Introduction to IoT," *IoT Security: Advances in Authentication,* pp. 1-25, 2020.

[2] G. Pradyumna, B. Omkar, and B. Sagar, "Introduction to IOT," *International Advanced Research Journal in Science, Engineering and Technology,* vol. 5, no. 1, pp. 41-44, 2018.

[3] G. Fadlallah, H. Mcheick, D. Rebaine, and M. Adda, "Towards mobile collaborative autonomous networks using peer-to-peer communication," in *Proceedings of the 7th International Conference on Software Engineering and New Technologies*, 2018, pp. 1-8.

[4] M. Meruje, M. G. Samaila, V. N. Franqueira, M. M. Freire, and P. R. M. Inácio, "A tutorial introduction to IoT design and prototyping with examples," *Internet of Things A to Z: Technologies and Applications,* pp. 153-190, 2018.

[5] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in industry,* vol. 101, pp. 1-12, 2018.

[6] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE transactions on industrial informatics,* vol. 14, no. 11, pp. 4724-4734, 2018.

[7] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd annual design automation conference*, 2015, pp. 1-6.

[8] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, "Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation," *IEEE industrial electronics magazine,* vol. 11, no. 1, pp. 28-33, 2017.

[9] H. Jaidka, N. Sharma, and R. Singh, "Evolution of iot to iiot: Applications & challenges," in *Proceedings of the international conference on innovative computing & communications (ICICC)*, 2020.

[10] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies," *IEEE Communications Magazine,* vol. 56, no. 10, pp. 114-120, 2018.

[11] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE access,* vol. 3, pp. 1206-1232, 2015.

[12] Y. Ren, R. Xie, F. R. Yu, T. Huang, and Y. Liu, "Potential identity resolution systems for the industrial Internet of Things: A survey," *IEEE Communications Surveys & Tutorials,* vol. 23, no. 1, pp. 391-430, 2020.

[13] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in industrial internet of things: Architecture, advances and challenges," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 4, pp. 2462-2488, 2020.

[14] Y. Liu, M. Kashef, K. B. Lee, L. Benmohamed, and R. Candell, "Wireless network design for emerging IIoT applications: Reference framework and use cases," *Proceedings of the IEEE,* vol. 107, no. 6, pp. 1166-1192, 2019.

[15] Y. Liu, R. Candell, M. Kashef, and L. Benmohamed, "Dimensioning wireless use cases in Industrial Internet of Things," in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2018, pp. 1-4: IEEE.

[16] K. Al-Gumaei *et al.*, "A survey of internet of things and big data integrated solutions for industrie 4.0," in *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2018, vol. 1, pp. 1417-1424: IEEE.

[17] X. Yu and H. Guo, "A survey on IIoT security," in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, 2019, pp. 1-5: IEEE.

[18] X. Hou, Z. Ren, K. Yang, C. Chen, H. Zhang, and Y. Xiao, "IIoT-MEC: A novel mobile edge computing framework for 5G-enabled IIoT," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1-7: IEEE.

[19] G. Siaterlis *et al.*, "An IIoT approach for edge intelligence in production environments using machine learning and knowledge graphs," *Procedia CIRP,* vol. 106, pp. 282-287, 2022.

[20] D. Dhungana *et al.*, "Multi-factory production planning using edge computing and IIoT platforms," *Journal of Systems and Software,* vol. 182, p. 111083, 2021.

[21] S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: Next-generation Ethernet, IIoT, and 5G," *Proceedings of the IEEE,* vol. 107, no. 6, pp. 944-961, 2019.

[22] V. V. Abdullin, D. A. Shnayder, A. R. Khasanov, and D. F. Tselikanov, "IIoT-Based Approach to Industrial Equipment Condition Monitoring: Wireless Technology and Use Cases," in *2020 Global Smart Industry Conference (GloSIC)*, 2020, pp. 399-406: IEEE.

[23] P. Vanin, A. Nesterov, and I. Kholodilin, "Integration of IIoT and AR technologies to educational process through laboratory complex," in *2018 Global Smart Industry Conference (GloSIC)*, 2018, pp. 1-6: IEEE.

[24] V. R. Kebande, "Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0," *Forensic Science International: Reports,* vol. 5, p. 100257, 2022.

[25] J. Rosales, S. Deshpande, and S. Anand, "IIoT based augmented reality for factory data collection and visualization," *Procedia Manufacturing,* vol. 53, pp. 618-627, 2021.

[26] B. Mayer, D. Tantscher, and C. Bischof, "From digital shop floor to real-time reporting: An iiot based educational use case," *Procedia Manufacturing,* vol. 45, pp. 473-478, 2020.

[27] L. Bu, Y. Zhang, H. Liu, X. Yuan, J. Guo, and S. Han, "An IIoT-driven and AI-enabled framework for smart manufacturing system based on three-terminal collaborative platform," *Advanced Engineering Informatics,* vol. 50, p. 101370, 2021.

[28] M. Javaid, A. Haleem, R. P. Singh, S. Rab, and R. Suman, "Upgrading the manufacturing sector via applications of industrial internet of things (IIoT)," *Sensors International,* vol. 2, p. 100129, 2021.

[29] C. Cronin, A. Conway, and J. Walsh, "Flexible manufacturing systems using IIoT in the automotive sector," *Procedia Manufacturing,* vol. 38, pp. 1652-1659, 2019.

[30] Y. Lu, P. Witherell, and A. Jones, "Standard connections for IIoT empowered smart manufacturing," *Manufacturing letters,* vol. 26, pp. 17-20, 2020.

[31] I. Jamai, L. B. Azzouz, and L. A. Saïdane, "Security issues in Industry 4.0," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020, pp. 481-488: IEEE.

[32] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, 2018, pp. 124-130: IEEE.

[33] D. B. Knezevic and N. Kasunic, "Security challenges of Wi-Fi connected beer cooler and serving IIoT device," in *2020 5th International Conference on Smart and Sustainable Technologies (SpliTech)*, 2020, pp. 1-5: IEEE.

[34] M. Zolanvari, Z. Yang, K. Khan, R. Jain, and N. Meskin, "Trust xai: Model-agnostic explanations for ai with a case study on iiot security," *IEEE internet of things journal,* 2021.

[35] H. Chen, M. Hu, H. Yan, and P. Yu, "Research on industrial internet of things security architecture and protection strategy," in *2019 International conference on virtual reality and intelligent systems (ICVRIS)*, 2019, pp. 365-368: IEEE.

[36] S. Yeasmin and A. Baig, "Permissioned Blockchain-based Security for IIoT," in *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 2020, pp. 1-7: IEEE.

[37] W. Hu and H. Li, "A blockchain-based secure transaction model for distributed energy in Industrial Internet of Things," *Alexandria Engineering Journal,* vol. 60, no. 1, pp. 491-500, 2021.

[38] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet of Things Journal,* vol. 7, no. 1, pp. 16-32, 2019.

[39] Z. Guan, X. Lu, N. Wang, J. Wu, X. Du, and M. Guizani, "Towards secure and efficient energy trading in IIoT-enabled energy internet: A blockchain approach," *Future Generation Computer Systems,* vol. 110, pp. 686-695, 2020.

[40] V. Sklyar and V. Kharchenko, "ENISA documents in cybersecurity assurance for industry 4.0: IIoT threats and attacks scenarios," in *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2019, vol. 2, pp. 1046-1049: IEEE.

[41] V. V. R. G. Saigopal and V. Raju, "IIOT digital forensics and major security issues," in *2020 International Conference on Computational Intelligence (ICCI)*, 2020, pp. 233-236: IEEE.

[42] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnerability exploitations," *IEEE Access,* vol. 6, pp. 43586-43601, 2018.

[43] G. Rathee, S. Garg, G. Kaddoum, and B. J. Choi, "Decision-making model for securing IoT devices in smart industries," *IEEE Transactions on Industrial Informatics,* vol. 17, no. 6, pp. 4270-4278, 2020.

[44] S. Nayak, N. Ahmed, and S. Misra, "Deep learning-based reliable routing attack detection mechanism for industrial Internet of Things," *Ad Hoc Networks,* vol. 123, p. 102661, 2021.

[45] X. Liu, W. Yu, F. Liang, D. Griffith, and N. Golmie, "On deep reinforcement learning security for Industrial Internet of Things," *Computer Communications,* vol. 168, pp. 20-32, 2021.

[46] A. Chowdhury and S. A Raut, "Benefits, challenges, and opportunities in adoption of industrial IoT," *International Journal of Computational Intelligence & IoT,* vol. 2, no. 4, 2019.

[47] A. S. Kumar and E. Iyer, "An industrial iot in engineering and manufacturing industries—benefits and challenges," *International journal of mechanical and production engineering research and dvelopment (IJMPERD),* vol. 9, no. 2, pp. 151-160, 2019.

[48] J. Cheng, W. Chen, F. Tao, and C.-L. Lin, "Industrial IoT in 5G environment towards smart manufacturing," *Journal of Industrial Information Integration,* vol. 10, pp. 10-19, 2018.

[49] C. Liu, Z. Su, X. Xu, and Y. Lu, "Service-oriented industrial internet of things gateway for cloud manufacturing," *Robotics and Computer-Integrated Manufacturing,* vol. 73, p. 102217, 2022.

[50] J. Li, A. Maiti, M. Springer, and T. Gray, "Blockchain for supply chain quality management: challenges and opportunities in context of open manufacturing and industrial internet of things," *International Journal of Computer Integrated Manufacturing,* vol. 33, no. 12, pp. 1321-1355, 2020.

[51] M. Rajesh and S. B. Narayana, "Application of IIoT system in the Sewing Section of a Garment Industry," in *2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON)*, 2021, vol. 1, pp. 244-246: IEEE.

[52] V. Sklyar and V. Kharchenko, "Challenges in assurance case application for industrial IoT," in *2017 9th IEEE international conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS)*, 2017, vol. 2, pp. 736-739: IEEE.

[53] S. Sen and L. Song, "An IIoT-Based Networked Industrial Control System Architecture to Secure Industrial Applications," in *2021 IEEE Industrial Electronics and Applications Conference (IEACon)*, 2021, pp. 280-285: IEEE.

[54] R. Karthikeyan, K. Sakthisudhan, G. Sreena, C. Veevasvan, and S. Yuvasri, "Industry safety measurement using multi-sensing robot with IIoT," *Materials Today: Proceedings,* vol. 45, pp. 8125-8129, 2021.

[55] S. S. Arumugam *et al.*, "Accelerating industrial iot application deployment through reusable ai components," in *2019 Global IoT Summit (GIoTS)*, 2019, pp. 1-4: IEEE.

[56] Z. Gui and A. Harth, "Towards a data driven natural language interface for industrial IoT use cases," in *2021 IEEE 2nd International Conference on Human-Machine Systems (ICHMS)*, 2021, pp. 1-3: IEEE.

[57] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," *Computer Networks,* vol. 101, pp. 192-202, 2016.

[58] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial internet of things (IIoT) healthcare applications," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 6, pp. 2736-2744, 2018.

[59] L. Faramondi, G. Oliva, R. Setola, and L. Vollero, "Iiot in the hospital scenario: Hospital 4.0, blockchain and robust data management," *Security and privacy trends in the industrial internet of things,* pp. 271-285, 2019.

[60] A. Rayes, S. Salam, A. Rayes, and S. Salam, "Internet of things (IoT) overview," *Internet of Things From Hype to Reality: The Road to Digitization,* pp. 1-34, 2017.

[61] R. Moura, L. Ceotto, A. Gonzalez, and R. Toledo, "Industrial Internet of Things (IIoT) platforms-an evaluation model," in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2018, pp. 1002-1009: IEEE.