International Journal of Advanced Technology and Engineering Exploration, Vol 10(108)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2023.10101133

Review Article

Role of machine learning approach for industrial internet of things (IIoT) in cloud environment-a systematic review

Nabeela Hasan[1*] and Mansaf Alam[2]
Senior Research Fellow, Department of Computer Science, Jamia Millia Islamia, New Delhi, India[1]
Professor, Department of Computer Science, Jamia Millia Islamia, New Delhi, India[2]

Received: 14-February-2023; Revised: 01-November-2023; Accepted: 04-November-2023

Abstract
The industrial internet of things (IIoT) is related to the fourth industrial revolution and includes different applications and innovations for the conduction of industrial activities. The introduction of IIoT has revolutionized how manufacturing and industrial units traditionally worked. The current paper aims to analyse the privacy and security issues incorporated in the IIoT and the role of the machine learning (ML) approach for the IIoT. It also analyses industry focused internet of things (IoT) taxonomies and the application of IIoT systems in various smart cities. It is found that IIoT-enabled devices are based on advanced technologies such as big data, robotics, ML, operational technology (OT), and machine-to-machine (M2M) technologies. It helps to intelligently change the behaviour of different environments without any human intervention. ML-based IIoT devices can be used for smart energy, smart transportation, urban planning, and smart city characteristics.

Keywords
Industrial internet of things (IIoT), Machine learning (ML), Smart energy, Smart transportation, Sensors.

1.Introduction
The industrial internet of things (IIoT) is recognized as the extended use of the internet of things (IoT) and integrated technologies in the manufacturing industry. It involves the implementation of innovative techniques such as machine learning (ML), robotics, big data, machine-to-machine (M2M), and industrial control systems (ICS) by companies in their working processes [1]. IIoT also includes sensors and actuators that have calculating and interactive capacities. Such devices change the entire course of a gathering, exchanging, examining, and transforming data that facilitates the decision-making process. It innovates Industry 4.0 practices and contributes towards industrial development through improved productivity by industries such as power, mining, agriculture, healthcare, and transportation [2]. While focusing on ML, it forms an integral part of the IIoT and contributes to Industry 4.0 growth by providing innovative computing and communication technologies. ML is based on a predictive analysis aspect that helps analyse the large volumes of data produced by IIoT effectively [3].

The in-built trained model in ML extracts knowledge that helps manufacturing and industrial units make the right decisions under complex situations. ML is also capable of detecting a fault, classification of the image, identification of speech, natural language processing which facilitates industrial processes. It also includes other processes such as automatic fruit classification and real-time quality monitoring in the IIoT applications that help in improving industrial applications [4]. This paper specifically aimed to analyse the role of the ML approach for IIoT with the help of a systematic review. We focused on studying the general concept of IIoT and its computing framework and discussing different computing frameworks such as fog computing, edge computing, cloud computing, and distributed computing. The facts related to the application of IIoT systems in various smart city use cases such as smart energy, smart transportation, urban planning, and smart city characteristics were discussed.

The Fourth Industrial Revolution became known as IIoT, which includes different applications and innovations to conduct industrial activities. The introduction of IIoT has revolutionized how

*Author for correspondence

manufacturing and industrial units used to work traditionally [5]. IIoT has led to the introduction of smart industries and factories that use decentralized manufacturing methodologies for growing in complex, competitive environments. It includes the use of technologies and applications such as ML, supervisory control and data acquisition (SCADA) cyber-physical systems (CPS) for the promotion of manufacturing and industrial work [6].

We focused on analysis and systematic review of the privacy and security issues of Industry 4.0 and the role of the IIoT ML method. ML is an artificial intelligence (AI) subset that focuses on developing algorithms, systems, and applications that increase data accuracy automatically. It automatically computes large data sets that facilitate the industries to make business decisions effectively.

We also focused on studying the general concept of IIoT and its computing framework and discussing different computing frameworks such as fog computing, cloud computing, edge computing, and distributed computing. The different computing is used in the IIoT to enhance its working and applications in different industries. We discussed the application of IIoT systems in various smart city use cases such as smart energy, smart commute, urban planning, and smart city characteristics. The use of ML based IIoT devices helps in improving the city workings such as transportation, infrastructure, energy consumption, and pollution prevention.

We provided a comprehensive review of various ML algorithms such as ML classifiers, regression algorithms, feature extraction algorithms, clustering, and neural networks for IIoT-based smart systems. It includes using different algorithms, classifiers, and neural networks such as a k-nearest neighbour, case-based reasoning, decision tree, Naïve Bayes, regression algorithms, support vector, artificial neural network (ANN) algorithm, and ensemble method for the implementation of ML algorithms for IIoT-based smart systems.

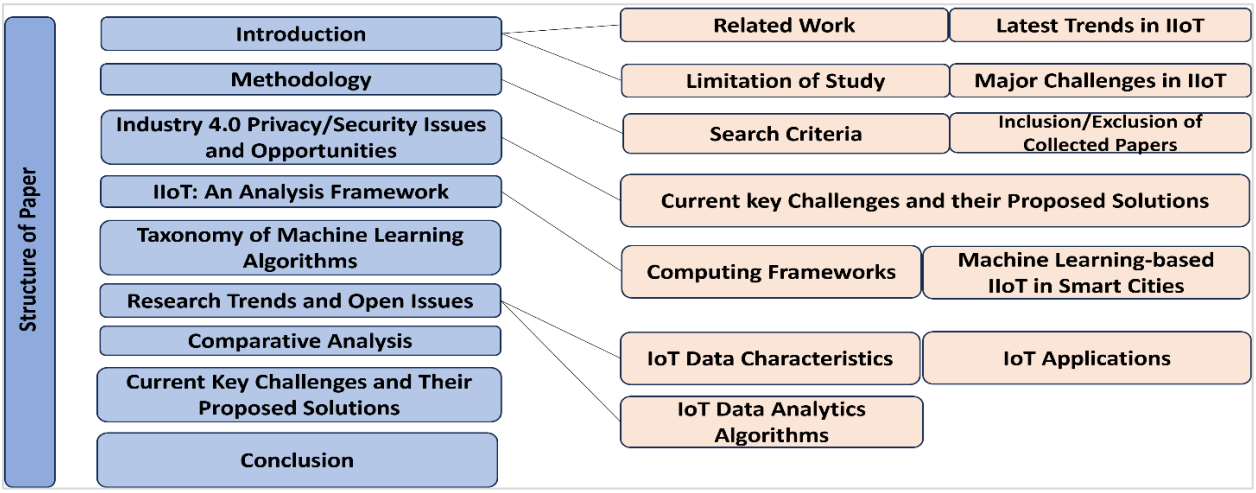


Figure 1 Structure of paper

We also discussed the challenges and issues associated with IIoT systems. It included challenges in IoT data characteristics such as privacy and security, data management, and cost. The challenges related to IoT applications include data integrity, monitoring and detecting, securing communication, and managing updates. The IoT data analytic algorithms challenges are faced in the form of data structures, combining data formats, lack of balance between scale and speed, analytics at the edge, and IoT analytics and AI. The key abbreviations are presented in *Table 1* and paper structure is presented in *Figure 1*.

1.1Related work

The idea of IoT was established in 1999 with the participation of an official of the development community of radio frequency identification (RFID). It may incorporate various technological advancements such as wireless communication, sensor networks, Second/Third/Fourth Generation (2G/3G/4G), General Packet Radio Service (GPRS), Global System for Mobile Communication (GSM), WI-FI, RFID, Global positioning system (GPS), interconnectivity processors, and microcontrollers [7].

The transmission of data by IIoT is based on several protocols based on SCADA systems. However, the major issue with these protocols is that they have been designed without considering the security threats. Thus, modifications have been made in the traditional IIoT protocols, which led to the formation of new protocols such as distributed message queuing telemetry transport (MQTT) and distributed network protocol version 3 (DNP3) [8]. For example, DNP3 is based on SCADA systems that provide reliable information transfer initially. Later issues related to lack of authentic encryption, lack of access control, and insufficient security mechanisms were observed, which reduced the efficacy of DNP3 to low levels. However, when the protocol was modified by including IEC 60870-5 standard, the authentication of the protocol was enhanced [9].

IIoT is also known to be a cluster of applications and devices that relate to communication software. It helps to intelligently change the behaviour of the different environments without any human intervention [10]. While focusing on the location, a taxonomy of IIoT is classified into four layers: an ecosystem, Purdue model, physical, and mobility. The ecosystem is associated with developing IoT ecosystems to monitor the functionality of different devices such as CCTV cameras. The Purdue model is based on the control hierarchy that performs hierarchical functions in manufacturing units [11]. The physical aspect is associated with physical security susceptibility with the help of externally located devices. The mobility aspect is related to wireless devices to convey data with the threat of interference or jamming [12].

IoT is regarded as a global connecting network that helps remotely connect all the remote locations/devices. The communication technologies in IoT include different electronic devices, mobile devices, and industrial equipment to establish interaction between individuals and devices. It is used in different sectors such as healthcare, mining, logistics, firefighting and transportation to increase their efficacies. It is also used for creating green IoT technologies by connecting millions of sensors through wireless connections. However, its use gets restricted because of the high consumption of power [13]. IIoT helps the manufacturing firms increase their existing systems' capability and use new methods for operations and production. For example, the mining industries have been performing predictive maintenance activities, but with the help of IIoT, the mining industry can use big data analytics for solving critical problems. Due to the increased use of IoT, the spending on IoT has increased significantly in recent years and is expected to reach US1.4 trillion by 2021. The highest spending in IoT is recorded in the manufacturing sector in different regions such as the United States, Asia/Pacific (excluding Japan), and Western Europe [14].

Industry 4.0 emerged in Germany in 2011 to refer to the new German economic policy. The wave of Industry 4.0 led to the enhancement of several technology-based companies such as Siemens, General Electric, and Mitsubishi and facilitated their production processes through automation. Due to the introduction and application of innovations owing to Industry 4.0, there has been an increase in the productivity of manufacturing units from €90 billion to €150 billion [15].

IoT seeks to link and integrate all physical equipment such as sensor nodes, controllers, and identification of radio frequencies, connectivity, and internet protocol. The wireless sensor and activator network (WSAN) create a wide range of infrastructures for applications, such as IIoT, CPS, and interactive internet. The technology-based development and information communications technology (ICT) are also incorporated in the IoT to support Industrial Revolution 4.0IoT helps in meeting the needs of the manufacturers that are in urgent need of developing an integrated connected system to interlink the entire system of production, machinery, distribution, and sales at both local and global levels. It will help streamline and synchronize the overall working process, reducing waste and higher productivity [16].

Technology and digitalization promote business growth by developing business-to-business (B2B) networks. Different industries increasingly adopt IoT and M2M technologies to enhance their networking ecosystems. The use of technologies also opens new avenues for business by increasing the complexity of the business environment and acquiring better information from within and beyond company boundaries [17].

The concept of IoT and IIoT is included in the ICS s that provide critical infrastructure for the supervision of industrial machines and processes. The ICSs include a SCADA system that helps in developing a human-machine interface (HMI). It helps in enhancing supervisory control activities through IIoT based devices monitoring, controlling, and securing applications [18].

IoT has extended the internet connectivity in numerous applications globally and connected billion of devices to acquire high-speed data transfer in 5G enabled industrial environment. The use of IoT-based applications helps develop smart homes, smart factories, smart cities, and secure vehicular Ad Hoc networks [19]. IIoT is regarded as the subset of the IoT that efficiently manages industrial operations and assets. It facilitates Industry 4.0 to Industry 5.0 and narrows the interaction gap between humans and machines. It is used with different applications such as big data, edge computing, and CPS to provide safe networking systems [20]. Big data is increasingly used in the segment of IIoT as it helps in the massive development of IoT devices such as sensors. IIoT based devices ensure interoperability, virtualization, decentralization, real-time capability that help in developing secure networking systems for transactions and communications [21].

1.2Latest trends in IIoT

IoT, big data, cloud computing, AI and CPSs, virtual reality (VR), and augmented reality (AR) are just few of the technologies that form the foundation of IIoT.

a) IoT: IoT devices help gather data and trigger actions in real time, which is very useful in the linked industrial scenario. These gadgets are the backbone of the IIoTs and monitor manufacturing assets all over the world. To significantly reduce labour cost and traditional system administration, IoT devices are used to monitor the whole process, beginning with the raw materials, and ending with the finished goods.
b) Big Data: There is a need for highly advanced high speed computing equipment for huge data analysis since IIoT devices and systems produce large data streams. With latency and real-time considerations in mind, it might be difficult to pinpoint exactly how, when, and in what location the large data will be processed and analysed in IIoT systems. IIoT systems allow various big data gathering, storage, administration, processing, analysis, and actuation technologies to completely manage the analysis of big data services.
c) Cloud Computing: To handle, process, analyse, and store the immense amounts of data generated by IIoT, widely dispersed advanced computing devices are required. Computing, networking, and storage resources from the cloud are made available to all IIoT nodes. Backend clouds are immediately connected with all connected equipment and services. Private cloud services are owned and operated exclusively by IIoT personnel, whereas public cloud services are owned and operated by independent cloud service providers.
d) AI and CPSs: AI technologies guarantee the autonomous and intelligent operation of IIoT systems, which reduces the need for human involvement and maximises productivity. Complex AI technologies, such as systems with multiple agents and conversational AI, are used to give IIoT autonomy. Also, IIoT enables various search, optimisation, and prediction algorithms to be implemented at various levels of the system, from devices and sensors to cloud data centres. Manufacturing machinery and automated factories are only two examples of the types of CPSs that may be empowered by IIoT technologies.
e) VR and AR: Workers in the manufacturing sector might benefit from AR technology during intricate tasks including the assembly and disassembly of complicated machinery, industrial goods, and mission-critical systems. To reduce the number of mistakes made during operations, AR technologies allow for constant monitoring of personnel and machinery. Before implementing changes to IIoT systems, users may test out potential setups of commercial tasks and components using VR technologies. VR may shorten the amount of time it takes to reconfigure industrial facilities and machinery and eliminate the need for them to be shut down entirely.

1.3Major challenges in IIoT

Many technological issues, including connectivity, confidentiality and security, flexibility, diversity, adaptability, dependability, and resource management, have emerged because of the complex and diverse nature of IIoT systems which is shown in *Figure 2*. Nonetheless, there are still significant problems that must be fixed. These difficulties are discussed as follows:

a) Data Management: Because of the widespread use of disparate IIoT devices, the amount of data has exploded. More and faster streams of sensed data are being produced as sensors and actuators become more incorporated into industrial systems. These diverse IIoT devices collect and store the sensed data, while cloud servers and edge servers process the information in real time and for future use. Sensitive data poses significant challenges in terms of processing, dissemination, accessibility, and retention.
b) Heterogeneity: The difficulty lies in the fact that an IIoT system must integrate and collaborate with technologies from a wide variety of vendors. Synchronization, shared resources, shared data,

compatibility, and data security all make it harder to integrate and collaborate. Flexible and effective methods of cooperation and interoperability still need further improvement.

c) Robust and flexible data analytics: There is a pressing need for powerful and adaptable big data analytics tools to realize the IIoT's potential and reap the full benefits of the massive amounts of data produced by IIoT gadgets. Traditional database management solutions can't deliver the goods because they can't effectively handle and analyse the massive amounts of data involved. Critical real-time industrial automation tasks, such as fault prediction, predictive maintenance, increased output, decreased disruptions, and identifying anomalies, rely on the timely processing of the IIoT data.

d) Authentication: Trust among consumers is a major factor in whether a technology is adopted and used by its target audience. Commercial clients' confidence in IIoT-based solutions is crucial to their widespread adoption. The security and privacy of IIoT systems have been recognized as a serious concern in the recent academic literature, even though these systems are still in their infancy. Weak safety and confidentiality of IIoT systems would deter consumers from adopting these IIoT systems because of the significant correlation between the security and confidentiality of technology and the confidence of their customers.

e) Co-existence of Protocols: Both academics and businesses have recently shown an increasing interest in the IIoT. For information to be shared, communication is essential in the IIoT. Thus, connectivity in IIoT must be capable to link many diverse devices, providing sufficient bandwidth for data transmission, and ensuring predictable behaviour with minimal latency. In addition, there are time, validity, accessibility, and safety constraints in many industrial applications. The IoT makes use of several technologies for communication, guidelines, and regulations.

f) Decentralization: Edge computing, networking, and storage services are necessary due to the variety of data sources and the high volume of continuous data flows being generated. However, edge services and data handling on the edge are completely coordinated by centralized cloud controllers, allowing edge computing to enhance end nodes. Because of this reliance, it is essential that all communication routes within an industrial system be highly accessible.

g) Emergence of IIoT Operating Systems (OSs): Operating systems for IoT devices are optimised for their limited resources, such as memory, size, battery consumption, and processor speed. Researchers like TinyOS and Contiki as IoT OSes because they meet most of their needs. Small memory footprint, real-time, low-power consumption, equipment agnostic tasks, privacy, communication, protocol support, storing data, consistent connectivity, and end device control are all possible criteria for an IoT OS

h) Security: Keeping the public safe during emergencies and disasters using IIoT should be a top concern. Timely event identification, alert generation, site-localization, and notification of emergency response service providers like the fire department, the ambulance service, disaster management teams, traffic officers, and other law enforcement agencies are crucial to ensuring the security of commercial employees and machinery in the event of an emergency. However, communication infrastructures being unavailable or broken is a big problem in disaster zones.

Figure 2 Major challenges of IIoT

1.4Limitations of study

As with most of the research, the results of this one need to be interpreted with caution. The following sections elaborate on the research's caveats:

a) A modern and sufficient body of past works is required for a more applicable contribution. In contrast, we want to fill in the blanks with our research by analysing the literature thoroughly.

b) This research lacks several methods that have been undertaken in this context, despite the effort to provide a comprehensive review by addressing multiple approaches and techniques that have been implemented in different ways to solve IIoT difficulties.

c) While the design viewpoint for Industry 4.0 as a whole and the innovations and implementations are beyond the scope of this research, they are discussed in detail here to help explain different features and ways for employing them.
d) Due to the sheer volume of labour involved, the authors of this research choose to gloss over the security concerns surrounding the IIoT.
e) Human-centered needs for Industry 4.0 are briefly covered due to the study's emphasis on the technological aspects of IIoT and Industry 4.0.

2.Methodology

The study uses open application programming interfaces (API)s from scholarly databases and web search engines like Web of Science, IEEE Xplore and Scopus to collect and evaluate a collection of academic articles released as journal articles and conference papers shown in *Figure 3.* The process of compiling these texts entails the following phases.

2.1Search criteria

The search procedure begins with a look through four scholarly databases (Springer, ACM, Elsevier, and IEEE). The three terms 'Industrial Internet of Things', 'Industrial IoT' and 'IIoT' are used to filter research publications that meet the inclusion requirements. When searching, just the AND operator is employed. The enormous number of duplicated and ineffective results produced by the OR operator prevents its application. The results obtained are further categorised by the years 2015-2023 and according to their sources which is shown in *Figure 4(a)* and *3(b*). Following the procedures, we narrow down the pool of studies to 65 total publications.

a) In all, we looked at 2,536 research which includes both journal articles and conferences whose distributions is shown in *Figure 5*, but we were able to exclude 2046 of them just by reading their titles. Authors themselves execute eliminations based on titles.
b) 490 studies are still outstanding. There are a total of 413 studies that were disqualified due to inadequate abstracts.
c) A total of 23 papers have been discarded as irrelevant because of these meta-analyses. Examining the various parts of the research paper reveals that it does not provide answers to any of the issues being investigated. For this reason, we do not include studies of this kind, resulting in a total of fifty-four recognised studies.
d) Sixty-five research articles were ultimately included after the snowball method contributed eleven additional publications. In snowballing, the appropriate articles were found by consulting the references of the chosen research. This is an attempt to include research that are significant but have not been uncovered in previously evaluated articles.

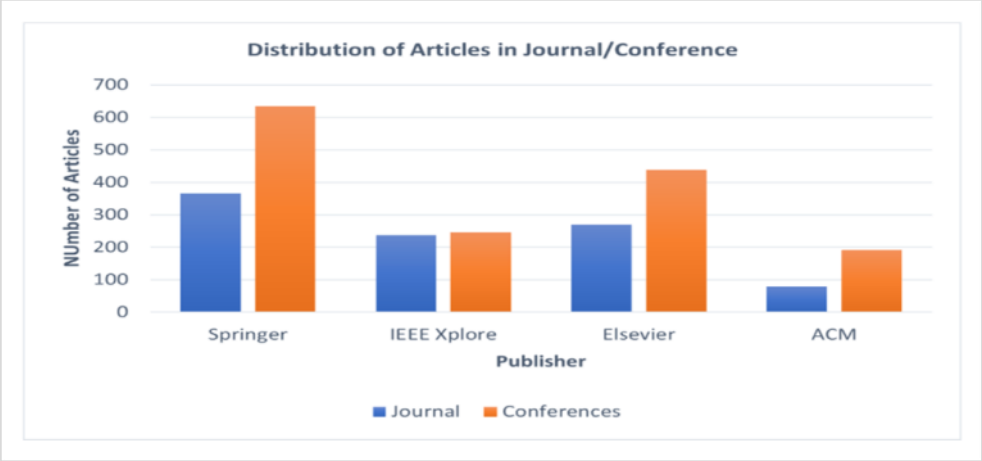
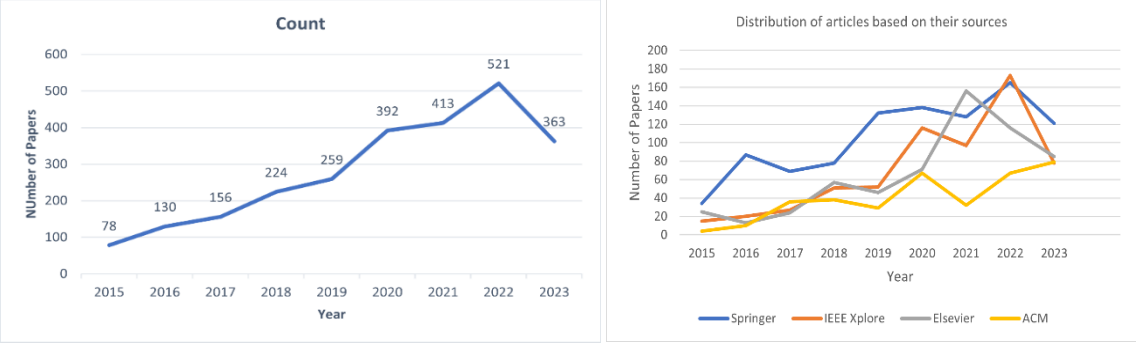


Figure 3 Distribution of articles in journal and conferences



(a) (b)

Figure 4 Number of Articles based on their sources in 2(a) and Number of included articles from 2015-2023 in 2(b)

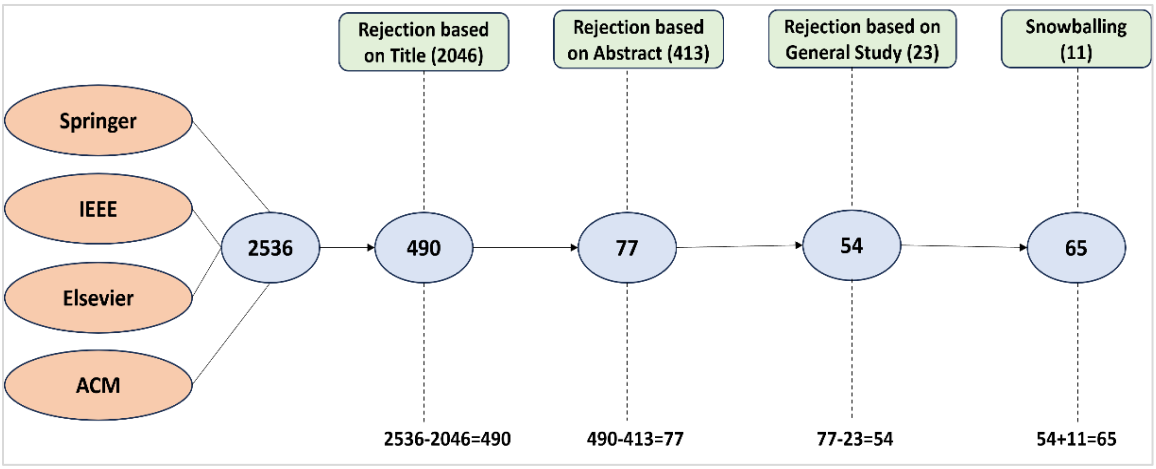


Figure 5 Summary of search process

2.2Inclusion/exclusion of collected papers

Articles were gathered once a search string was first defined. This query is made up of three search phrases joined together with an OR operator: "Industrial Internet of Things," "Industrial IoT," and "IIoT." Scopus (an abstract and citation database), IEEE Xplore (a digital library), and Science Direct (an online platform) were the three reference sources used. The publications should be published in peer-reviewed journals, have search phrases included in the titles, abstracts, and keywords, and be available online by August 2023. *Table 2* shows four inclusion criteria and eight exclusion criteria that were created to make the study more objective.

Table 2 Inclusion/exclusion criteria with description

	Criteria	Description
Inclusion	Survey or Review	All survey and review papers on IIoT
	Experimental Study	This article presents several answers to existing challenges in the field of IIoT research as well as experimental data to back them up.
	Theoretical Study	The essay provides only theoretical hypotheses to address certain issues in the field of IIoT research.
	Practical Study	The issues, answers, and practical applications of IIoT in industry are discussed in this article.
Exclusion	Implicitly Related	The article's emphasis on IIoT research is not stated. However, you won't find any mention of IIoT anywhere outside of the article's Highlights or Authors' Profiles.
	Wrongly Related	In the case of older articles, the text conversion process often results in mismatched characters. Like the "IIoT" for "Pot" or "cot" in a picture.
	Not Related	The scope of this study does not include defining IIoT.
	Non-Research Articles	These articles do not include any research study, for e.g., blogs

Criteria	Description
Non- Peer Reviewed Articles	These articles are not peer reviewed, for e.g., Procedia Engineering
No- Access Articles	Articles that are not fully accessible without subscription
Duplicate Articles	Articles that appeared more than once in multiple databases

3.Industry 4.0 privacy/Security issues and opportunities

In addition to power optimization and real-time productivity needs, safety is another crucial issue in IIoT. Notably, the industrial internet is a resource-controlled communication network that depends primarily on low bandwidth channels to transmit central processing unit (CPU), memory, and energy usage between lightweight devices [22]. Traditional protection methods are thus not adequate for ensuring complicated IIoT systems like safe protocols [23], easy-to-use encryption [24], and privacy assurances [25]. Current encryption methods from the industrial WSNs may be evaluated to protect the IIoT infrastructure before creating secure protocols IIoT. Small computational and memory resources, for example, prohibit the use of basic encryption that requires resources, for example, public-key cryptography (PKC). This issue is increasingly important in applications with large data interchange with real-time demands. To address risks to privacy and security in IIoT, a comprehensive strategy may be argued for, as stated in [26]. This research implies that the whole life cycle of systems and products must be considered in platform stability, safe design, security monitoring, identity authentication, and industrial rights management. When building a secure IIoT infrastructure, several safety characteristics need to be considered [27].

1. IIoT devices must be manipulative to prevent possible physical assaults, such as illegal reprogramming and passive secret theft, while accepting authorized operators to upgrade the security infrastructure.
2. Storage of the IIoT device from adversaries should be safeguarded by maintaining the data encoded to keep it private.
3. The communication network between IIoT devices should be protected to ensure integrity and authenticity.
4. IIoT infrastructure requires effective identification and authorization procedures to allow the IIoT resource to be accessed only by authorized organizations.
5. The system must be accessible in regular operation, even in malevolent users causing physical harm to the equipment. This feature ensures the solidity of IIoT.

Symmetric-key encryption often may offer a lightweight IIoT device solution. The key storage and key management are still significant problems with symmetric key encryption, particularly with limited devices. In addition, if one device is hacked in IIoT, all other keys may be leaked. PKC usually offers safer features and less storage but has a significant processing cost owing to sophisticated encryption. Therefore, lowering the cost of complicated security protocols for publicly available cryptosystems remains an essential issue for the security of IIoT. In PKC, elliptic curve encryption offers a lightweight computing resource solution. It offers reduced key size reduces the storage needs and transmission.

It is essential to offer identity in IIoT systems to get legal access. The Trusted IIoT infrastructure should guarantee that the authenticity of records used in naming systems, such as domain name systems (DNS), is recognized. The DNS may offer the internet username translation services; nevertheless, the DNS remains susceptible to other assaults by intentional opponents [28] in an unsafe manner. Even for a restricted and closed setting, this problem is valid. Thus, the entire naming system is still unsafe without any validity security of identification. A security addition to DNS, such as the domain name service security extension (DNSSEC), enhances security described in IETF RFC4033 [29]. However, because of its high cost of computing and transmission, it is challenging to deploy DNSSEC to the IIoT infrastructure.

IIoT devices should follow authentication methods and policies to exchange/publish data. Because of IIoT devices' resource limitations, low-cost authentication methods were not supplied as much as needed [30]. PKC systems offer creating authentication and authorization schemes, but they do not provide a worldwide root certification authority (CA) that mainly inhibits the implementation of many theoretically viable schemes. Without the global root CA, designing a secure authentication solution in IIoT is extremely difficult. Therefore, if we are presently going to offer secure authentication for devices IIoT, we must utilize the cost-effective methods that run counter to the primary aim of the lightweight concept of IIoT [31]. In addition, it is challenging to certify each item in IIoT as the overall

quantity of items may be enormous. Confidentiality is an extensive and varied notion. The literature has given several definitions and viewpoints. In general, IIoT's three guarantees of privacy [32] are:

1. Knowledge of the privacy concerns associated with the gathering.
2. Processing of information by individuals, and
3. Awareness of and control of the future use and distribution to other entities.

Data gathering method and data anonymization procedure are two main challenges for privacy. The act of collecting and accessing data during data collection usually deals with smart items; data anonymization is a procedure that ensures data anonymity through cryptographical protection and the disguise of data relations due to private data collection and storage limitations. However, due to the variety of data anonymization, many cryptographic systems may be used, which challenges privacy protection. Meanwhile, the data gathered must be exchanged across IIoT devices, and data anonymization is difficult to calculate on encrypted data.

3.1Current key challenges and their proposed solutions

There are several security issues plaguing the IoT sector that must be addressed urgently if the IoT industry is to advance. One of the biggest problems with the IoT is that its gadgets are so different from one another that a universal fix is impossible. Challenges, knowledge gaps, and potential approaches are all broken out in great depth in *Figure 6.*

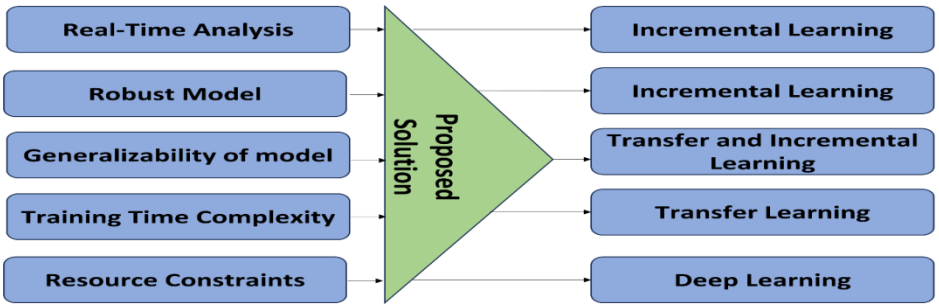


Figure 6 Current key challenges and their proposed solutions

a) Real-Time analysis: Any model's adoption at the corporate level requires real-time analysis. Most intrusion detection system (IDS) models described in the literature cannot be accessed online. The difficulty of separating benign from malicious communications lies at the heart of malware categorization. While online Learning analyses a continuous flow of data, offline mode applies ML models to stagnant datasets. As of now, malware detection has not made considerable use of real-time data analysis. Since the model may be changed to account for newly added information, incremental learning may be the answer for real-time analysis. Important past outcomes may be stored away for later use in gaining insight into comparable future data. In the context of support vectors, Qureshi et al. [33] employ a similar strategy by retaining ancient samples that have the potential to develop into support vectors.

b) Robust Model: To put it simply, robustness is the quality of having test set outcomes that are comparable to those acquired from the training set. To be useful in the actual world, ML models need to be quite strong [34]. It is possible to create robust implementations of the least absolute shrinkage and selection operator (LASSO) [35] and support vector machine (SVM) algorithms. Though effective in principle, not all the models have been widely used at the company level due to their lack of resilience. The problem of obtaining robustness in practise may be addressed with the help of Incremental Learning. Due to the dynamic nature of real-world data, a model's training set may change significantly from its validation set. Incremental learning is a continuous learning process in which the model becomes stronger with each new iteration. Some efforts employ adversarial data creation and other deep learning methods to test the system's resilience. The results may be quite astounding when Incremental and deep learning are combined.

c) Generalizability of Model: Generalizability requires, and is guaranteed by, robustness. To determine generalizability, we look to how well a model does in novel testing environments [36]. A model's resilience and universality are often

evaluated separately, but a model that is both must be created for sustainability. The combination of transfer and incremental might be the answer to this problem. Image categorization [37], target identification [38], and intrusion detection [39] are common applications, but Incremental Learning is less common in the field of information security. In a similar vein, transfer learning may be used with other anomaly detection methods to provide unprecedented outcomes regarding generalizability and robustness.

d) Training time complexity: Training durations for most Intrusion Detection models are prohibitively lengthy, degrading model performance to the point that trade-offs in system performance may be necessary. The complexity of deep learning models makes this problem much more difficult to solve. The term "Transfer Learning" refers to the practise of applying a previously learned model to new problems with comparable characteristics. While this idea is being put to good use in other applications of ML, it has seen very little exploration in the realm of malware research. When Deep Learning is combined with Transfer Learning, system performance is improved significantly since better results are achieved in less training time.

e) Resource Constraints: Energy, expenditure, and overall dimensions are all areas where IoT devices are notoriously limited. With regulations in place, it's difficult to guarantee safety. When it comes to inexpensive IoT gadgets, meeting all the necessary security standards is a huge worry. These limitations prevented the full potential of deep learning approaches from being realized. Effective hyperparameter tweaking methods, like those found in deep learning, could be the answer. Feature engineering is not required for deep learning, but it helps keep the model lean. Next, the model may be applied locally, at the node, for quicker response times in the event of an attack. Therefore, effectively using deep learning techniques may assist alleviate the impact of resource limitation and make use of recently developed methods.

4.IIoT: an analysis framework

IoT is a structure with different wireless devices, digital gadgets, individuals, mechanical devices are interconnected with unique identifiers (UIDs). IoT creates an integrated network that gathers and shares electronic information. It is used in several areas of daily life, such as surveillance, creating an intelligent environment, healthcare, and transportation [40].

4.1Computing frameworks

While focusing on the taxonomy of IoT, it is based on several different computing frameworks such as edge computing, fog computing, cloud computing, and distributed computing which are shown in *Table 3*. The different framework enhances the efficacy of the IoT application and makes it more useful for industrial purposes [41].

4.2ML-based IIoT in smart cities

In the last few years, significant growth has been observed in the segment of ML with the increasing use of ML-based applications in daily life. ML enhances data processing, storing, and transferring in different IIoT applications such as IIoT predictive maintenance and smart city (traffic flow prediction). For example, in the case of IIoT predictive maintenance, ML identifies, supervises, and examines variables during the operations.

Table 3 Computing frameworks

S. No.	Reference	Computing framework	Storage	Architecture	Computational capabilities	Turnaround time	Distance from source	Analysis
1	[42, 43]	Fog Computing	Limited	Distributed	lower	fast	closer	Short-term
2	[44, 45]	Edge Computing	Limited	Distributed	lower	fast	closer	Short-term
3	[46, 47]	Cloud Computing	Unlimited	Distributed	lower	fast	Far away	Long-term
4	[48, 49]	Distributed Computing	Limited	Distributed	lower	fast	closer	Short-term

It also alerts the organizers to perform maintenance activity before system failure. ML deals with cyberattack incidents while performing predictive maintenance analytics by creating a causative attack [50]. While applying IIoT systems in various smart city use cases such as intelligent energy, it includes

intelligent management systems in buildings. The system consists of three main layers: the data integration layer, prediction models, and action plan recommendations. It also includes using the streamy system based on Phyton semantic service to create Optimus ontology. As a result, cross-domain data is integrated for work conduction as per weekly and daily plans [51]. It also provides data integration facilities in energy production, data of buildings, energy prices, end-user attitude, and weather information that helps make actionable decisions. The IIoT system also provides personalized information for each building set-up in the city, which helps decision-makers frame policies related to reconstruction efficiently [52]. For example, the intelligent information system for monitoring and verification of energy management in cities (ISEMIC) has been introduced by the governing body in Croatia to support the intelligent management of public buildings in the country. ISEMIC is based on three-layer structures that exercise energy and water consumption control using anomalies and multiple regression analysis.

On the other hand, the effective use of ML could be witnessed in the traffic flow prediction. ML plays a vital role in enhancing route guidance and intelligent transport management process. As a result, there is relief from traffic congestion, lowering air pollution, and establishing secured traffic conditions. The Traffic Flow Prediction includes using several digital and ML-based devices such as mobile gGPS, sensors, radars, crowdsourcing, and cameras that help manage the traffic and transfer data from different traffic posts in real-time [53]. The application of ML and IoT is included in the traffic optimization process by using mobile crowd-sensing for intelligent transportation systems. The system provides information about congested routes and alerts individuals to use alternative routes to reach the desired destination [54]. ML and IIoT applications can also be witnessed in-vehicle parking arrangements. It includes an intelligent IoT-based signboard that provides information about free parking slots available in the parking space. It includes using SVM, a Markov random field (MRF) algorithm, and ultrasonic sensors to check the availability of vacant parking space in the parking space. The information through sensors is conveyed to the parking manager with the help of a Wi-Fi module and a cloud-based server [55]. To promote urban planning, IoT-based applications such as vehicle to vehicle (V2V) communication framework and M2M communication are used to strengthen the infrastructure aspects of smart cities. For example, by using GPS, vehicles like cars will be aware of their position and exchange information related to speed, movement, and location with the server [56]. In another case, a combined hardware and software system is used for monitoring the bus fleet so that there is an enhancement in the public transport user experience. In this system, RFID tags are used to recognize the bus, while incident responses are used to count the passengers on the bus. GPS is used to track the location of the bus, and a cloud-based TI CC3200 microcontroller is used to connect the liquid crystal display (LCD) present at each bus stop. The LCDs information about the routes, real-time position, and availability of seats in the bus to the individuals at the bus stop. The mobile application of the feature provides relevant bus information to passengers through smartphones. Thus, by using modern technologies, there is streamlining and systemizing of the transportation process that provides rich experiences to the users [57].

To promote smart city characteristics, smart street lights (SSL) have been developed with the help of ML and IIoT applications to reduce energy consumption. SSL is built with different intelligent devices and applications such as light sensors, GPS trackers, an IR sensor, and a wireless communication module that help the lights adjust their light frequency [58]. As a result, the intelligent lights make changes such as increasing light intensity in crowded areas and reducing light intensity in sparsely populated regions.

The GPS helps perform light maintenance activity by monitoring the lamps, identifying the defective lamps, and alerting the maintenance team in real-time [59]. Intelligent IIoT based applicants can also be used to detect and prevent accidents. It includes using the continuous hidden Markov model (cHMM) method based on feed forward – neural network (FF-NN) sensors, a regression tree, and the k-nearest neighbor (kNN) algorithms. On the other hand, the DRAM method has also been developed that helps in detecting accidents with the help of image data. It includes the Adaboost application through which the driver's consciousness is assessed with the help of images. It helps prevent accidents by analysing the awareness levels of the driver [60]. Thus, it can be said that the application of IIoT systems in various smart city use cases such as intelligent energy, smart transportation, urban planning, and smart city characteristics help in enhancing the city

functionaries. It also allows the governing body to provide quality services to the users.

5.Taxonomy of ML Algorithms

In addition to a variety of ML techniques for IIoT-based automated devices include categorizing the learner into two sections that are eager learners' lazy learners. Lazy learners save the data and analyse the data as the data arrives, utilizing case-based reasoning. On the other hand, the eager learners train data before receiving information based on the hypothesis using decision tree, naive Bayes, and ANNs. While focusing on the kNN it is used based on the lazy learning algorithm in which the data is stored in the form of n-dimensional space. In this process, when unknown data is received, it signals the closest neighbours to evaluate the data by using the Equation 1.

$$w = \frac{1}{d(x_q, x_i)^2} \quad (1)$$

On the other hand, in the decision tree process, there is the use of regression algorithms and models for the formation of the tree structure. There is a complete and exhaustive process in which the decision-making process is classified into different sequences at a time. The sequencing of the training data is executed until the termination condition is achieved. The entire process is carried out by forming branches that reflect anomalies and outliers [61].

Naive Bayes is based on Bayes theorem and is a probabilistic classifier shown in Equation 2. It includes independent conditionality, uncomplicated assumptions, and expression for the data classification.

$$P(X|C_i) = \prod_{k=l}^{n} P(x_1|C_i) \times P(x_2|C_i) \times \ldots \times P(x_n|C_i) \quad (2)$$

This process achieved the optimized posterior levels using P (Ci/X). The use of the Naive Bayes application helps in reducing cost related to class distribution and provides efficient outcomes. However, the use of applications gets restricted owing to zero probability issues. The use of an ANN is based on using the set of interconnected input and output units which is shown in *Figure 7.*

The process includes using different network structures such as feed-forward, convolutional, and recurrent to create synchronized networks. However, the implementation of the appropriate architecture depends upon the application model. The feed-forward model processes the image application to better convolution networks [62].

The feature extraction algorithms include two essential aspects feature selection and feature extraction. In the ML feature selection method, data is processed by targeting the data and cleaning. Once the data is processed, the feature section and extraction process are conducted using different feature selection techniques shown in *Figure 8.*

This selection process is based on applying two schools of thought, such as why feature selection in ML and application of Feature learning in ML.

In *Figure 9*, the first school emphasizes why feature selection should be included in the ML by focusing on Navies' theoretical features. The other school focuses explicitly on exploring domains, analysing computational resources, and the curse of dimensionality to conduction of feature selection with ML applications. As a result, there is a selection of features by organizing a complete feature set in which there is the identification of valuable features and extraction of information from the selected feature sets.

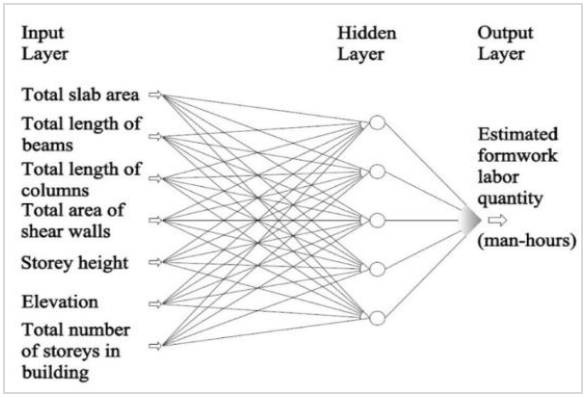


Figure 7 Artificial neural network

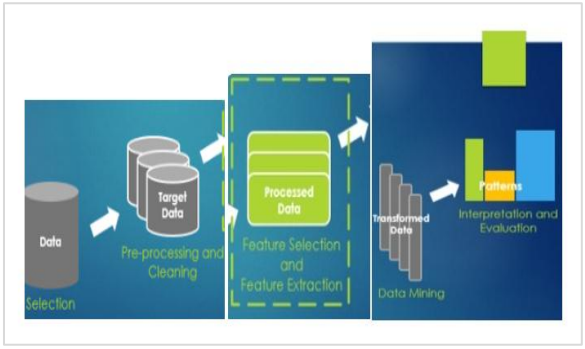


Figure 8 Feature Extraction Algorithms

Therefore, it is evident that in the ML algorithms for intelligent IIoT systems, the selection of features is an essential factor as it enables to improve the efficiency of the training algorithm in computational time and accuracy aspects shown in *Figure 10*. It also facilitates users working on issues and adopting a problem-solving mechanism with high dimension features. It helps in attaining relevancy and optimality aspects.

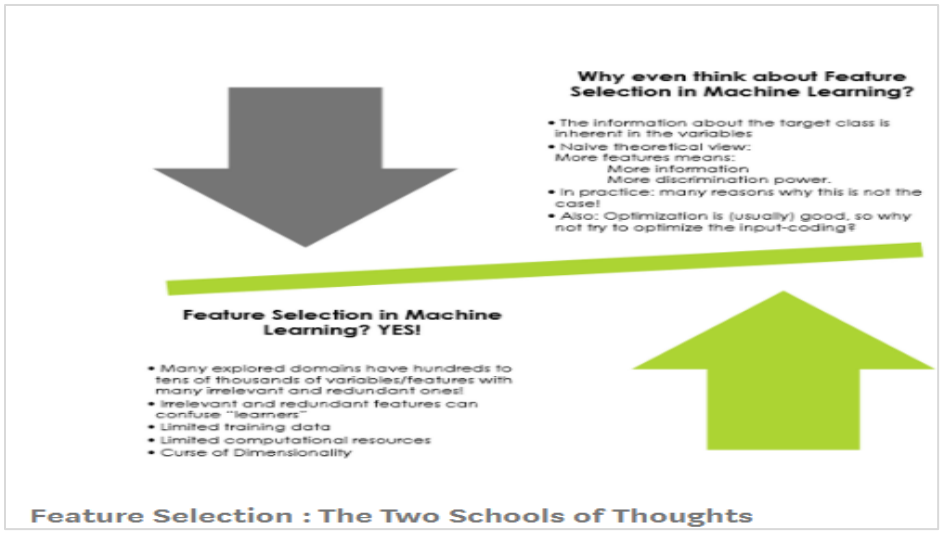


Figure 9 Feature selection (The two schools of thoughts)

Clustering is an unsubstantiated ML task that is organized using clustering algorithms. The clustering algorithm is used when there is an exploration of facts from anonymous data. It helps in earthquake analysis, detecting insurance frauds, customer segmentation, city planning, and classifying books in the library. For example, a centroid-based algorithm, K-means clustering, is used in ML algorithms for IIoT-based intelligent systems.

The K-means clustering process classifies data and minimizes variance points. On the other hand, DBSCAN is based on density-based spatial clustering of the application so that there is a separation between outliers and high-density clusters.

Figure 10 Feature Selection

Algorithm 1: Centroid Based Clustering Algorithm

for k=1 to K do
μk Ω some random location randomly initializes mean for kth cluster
end for
repeat
for n = 1 to N do
$\boldsymbol{r_{nk} \leftarrow argmin_k \parallel x_n - \mu_k \parallel^2}$E-step: assign n-th data point to the closest centre
end for
for k = 1 to K do
$\boldsymbol{\mu_k \leftarrow MEAN_k(x_n, r_{nk})}$ M-step: re-estimate means of cluster k with 2.2
end for
until converged
return r (return cluster assignments)

While focusing on ML algorithms for IIoT-based smart systems includes neural networks that help analyse data using learning algorithms. The ML-based neural network includes different algorithms such as regression algorithms, support vector, ensemble method, and ANN algorithms.

The regression model is a statistical ML model that establishes an association between the variables. The association between the variables provides information about other such mimics in the data.

Thus, by a continual process of observance, there are fewer errors along with the function. On the other hand, the support vector is associated with groups of points located in the dimensional plane. The creation of groups is executed with the help of a hyperplane. It helps separate the groups with a margin and is helpful in human ribonucleic acid (RNA) splicing [63].

The ensemble method is based on neural networks used to supervise the weak learning algorithms. It is a combination technique that helps in reducing variance, overfitting, and providing better outcomes. Additionally, the ANN algorithms are based on human-like neural networks. The different neural networks are connected to attain new data input from each connecting unit in this process. It also includes using other applications such as deep learning, which contributes to forming complex neural networks. Thus, it can be said that the use of different ML algorithms for IIoT-based innovative systems helps in acquiring relevant information from each data set effectively [64].

Algorithm 2. DBSCAN Algorithm

```
DBSCAN (dt, ep, Mpt) {
#dt=Dataset, eps=epsilon, #Mpt=MinPoints
# cluster index
E= 1
for each unvisited point d in dataset {
        mark d as visited
        # Findneighbours
Neighbours S = find the neighbouring points
of d
            if |S|>=Mpt:
S = S U S'
            if d' is not a member of any
cluster:
                    add d' to cluster E
}
```

6.Research trends and open issues

6.1IoT data characteristics

Due to the high level of heterogeneity in IoT, the different IoT characteristics usability and application get restricted by privacy and security issues. There are issues related to maintaining quality and trust for information transferred through shared models. There are issues related to the exchange of data securely between the consumers and IoT devices. For example, there is an issue related to privacy protection and management in the application system [65]. Cryptographic data storage and data aggregation issues in the service support the IoT layer, while cross-domain data security handling issues are faced in the network layer of IoT.

Additionally, cost issues are also faced at the user end in the form of the high price of the connecting components. IoT is based on technologies that establish connections between physical objects and the internet. However, to connect the objects with the network, connecting devices such as sensing, tracking, and control mechanisms are required, increasing the users' cost. Interoperability is the most common issue that is faced while implementing IoT devices. It also causes issues related to protocols and encodings, which create issues in supporting the applications. Data management is an essential characteristic of IoT technology, as with the advancements in technology, there is an increase in the volume of data sets. As the data sets are becoming more complex, IoT applications need to be advanced to deal with them properly to extract valuable information. The users also face device-level energy issues, creating issues in the large-scale adoption of IoT devices. There are energy constraints and interoperability issues that restrict the use of IoT devices [66].

6.2IoT applications

The primary issue with the IoT application is associated with security threats. The issues such as scan and takeover are associated with IoT because of which there is poor encryption of IoT devices. Due to limited hardware and complex algorithm, there is poor password protection. As a result, the hackers can enter and take over the system, creating security breach issues. Distributed denial of service (DDoS) is another issue faced while implementing the IoT devices into the company processes. In the case of massive traffic, the IoT application cannot handle the system and goes down. Under such conditions, when the system is connected to the internet, it gives opportunities to hackers to attack the system from multiple sources. Spam attack is familiar with IoT applications if there is no placement of a sound security system with an IoT device.

Moreover, most IoT devices have low capacities of resources which creates issues in encrypting communication over different layers of the security mechanisms. It limits IoT applications' working as the spyware based on message interceptors reading the data and modifying it as per their requirement. Thus, a security threat is created that restricts the use of IoT applications [67]. An injection attack is another cyber-attack that is encountered by IoT

applications. In injection attacks such as structured query language (SQL) and extended markup language (XML), there is the addition of an additional request to the prevailing one because the data gets compromised. It creates security threats and increases the risks of the infringement of data. 3pp libraries are another issue IoT applications face when included in the business process. 3pp libraries are highly vulnerable and enter the system through updates and upgrades. Thus, it is suggested that while updating the system, secured 3pp must be used so that there is the prevention of attacks.

6.3IoT data analytics algorithms

IoT data analysis methods are primarily linked to data structures integrating data formats, an imbalance of size and speed, IoT and edge analytics, and AI. Most sensors that transmit and record information do not gather valuable data structures. However, serious incidents do happen which are adequately predicated in prescriptive phases owing to classic time series challenges. There are issues related to combining multiple data formats as it is difficult to establish an association between senor data and unstructured data. For example, dark data is created because of unstructured data in different datasets. The other major issue with IoT data analytic algorithms is balancing the different environments such as cloud, server-based network, data center, and hybrid cloud. As a result, transferring data from one environment to another consumes much time, which creates discrepancies in the data transfer process [68]. For instance, transferring data with one terabyte capacity over a network with 10 Gbps capability takes more than 13 minutes. It creates issues in batch processing and real-time analysis of facts. Most IoT-enabled devices are located at different locations such as floors, homes, retail stores, and farm fields [69]. The variability in the implementation of the IoT devices and network services leads to the processing of 40% of IoT data at the edge. As a result, supplementary applications such as fog computing are required to support the IoT device algorithm to store, record securely, and transmit information. The integration of IoT and AI is yet to be discovered so that the benefits of both applications can be reaped together. AI is based on current statistical models that help handle the prediction values. Thus, integrating AI with IoT will enhance the ability of IoT devices to detect fraud, project demand, forecast churn, and analyse customer attitudes. A complete list of abbreviations is shown in *Appendix I.*

7.Comparative analysis

In the future, IoT may be used in much more diverse domains such as credential management, IoT, service-oriented architecture (SOA) software, connectivity, network infrastructure, algorithms and software, peripherals, exploration, and search engines, and much more [70]. The significant finding of the research is that edge computing plays a significant role in the extension of IoT applications and enhances IoT's ability to carry out instant processing activity. By focusing on the prevailing standards and solutions, edge IoT helps develop an advanced featured IoT architecture capable of identifying the requirement and selecting criteria for the development of edge ecosystem [71]. The deployment of the IoT application in healthcare helps develop the EH-IoT system that enhances the working of the entire medical and drug sector by synchronizing the healthcare ecosystem with IoT cloud and local edge devices [72]. However, the major issue with developing such a coordinated system is the lack of functional and operational standards. Due to a lack of standards and protocols, there is a development of a gap between the architectural functions and operations. It has led to the introduction of a new module based on the continuous analytics as a service (CAaaS) scheme so that there is a reduction in the security issues at the time of implementation of the elliptic curve cryptosystem [73]. The study in [74] provided a single platform for an industrial communications unit to handle the demerits of COVID-19 industry pandemics. Research in [75] the study highlighted the advantages of the IIoT in functioning the operating models and new businesses by developing a faster response to customer demands and meeting augmented flexibility needs.

The research in [76] focuses on addressing the efficacy and security issues users face when IIoT and blockchain applications. It includes using the developed deep reinforcement learning (DRL)-based optimization framework that helps meet the high throughput requirements by using secured networks. The DRL framework's significant benefit is that it helps develop a methodology through which scalability, decentralization, latency, and security can be reduced. It also helps enhance the scalability of the blockchain systems so that there is the decentralization of the system errors. The use of an open-source ML framework helps develop a learning model by using supporting languages such as Python, Lua, C, C++, and MATLAB. It also used to support platforms such as Windows, Linux, Android, iOS,

Ubuntu, and Google and maintained Microsoft Research, H2O, Ronan, and Google to develop profound speech, image recognition, and reinforcement learning. It includes the use of the PyTorch ML framework along with Python (supporting language), Linux (supporting platform), and Koray and Soumith (maintainer) to scale the production of models [77].

QARNA helps in the quality management use case by increasing the sensor-based supervision activities. It includes ML models such as Linear regression, ANN, M5Rules, radial basis function (RBF) network, bagging, and support vector regression to estimate dataset and attainment of accurate data. Apart from this, the IIoT platform and QARMA algorithm also help in the creation of CPS, data routing and pre-processing (DR&PP), edge data processor engine (E-DPE), data storage, and data bus [78]. There is a development of a distributed software-defined networking (SDN) architecture so that there was a development of configuration between the switches and controllers. It includes statically configured control architecture that helped develop network information base (NIB) and enhance network-wide views. Dynamically configured control architecture development balanced the uneven load distributors and controllers. The study proposed a blockchain based consensus protocol in distributed software defined industrial internet of things (SDIIoT) that helps develop synchronized network-wide views. It improved simulation outcomes and measured the trust features of the node [79].

The study in [80] identified that different model structures had different accuracy levels, such as transfer learning with an entire dataset showed an accuracy of 98.6%, while distributed transfer learning with a small dataset showed accuracy levels of 99.1%. The deep learning technique helps analyse the performance of the different algorithms and allows them to show optimized efficacy in regression, classification, and prediction. The transfer learning aptitude was also analysed in the study that highlighted the use of transfer learning techniques and attainment of relevant facts about problem space in terms of small datasets, large datasets, centralized, and distributed datasets. It included the use of a T-less industrial dataset to obtain faster outcomes.

The study [81] highlights the advantages of the IIoT in the functioning of the operating models and new business by focusing on developing a faster response to customer demands and meeting augmented flexibility needs. The study highlights the use of deep reinforcement learning in improving the convergence performance of algorithms. It includes adopting the access class barring (ACB) scheme to optimize the uplink transmission process. The study emphasizes that there must be a development of IIoT enabled devices to multi-objective optimization of the different performance metrics.

Research [82] has developed and implemented three kinds of chain codes on the industrial edge gateways as a vital architecture component. Furthermore, we have developed a credit-based Raft consensus method, which can choose ordering nodes dynamically to ensure quick and reliable credit calculation consensus. Research in [83] suggested using phase space embedding and sparse self-encoder to transform static and dynamic features. Experimental findings indicate that the proposed network and phase space embedding (PSE) can obtain superior outcomes with a few label applications, i.e., 15.12%. The findings also indicate that accuracy may be enhanced by reducing the number of label requests or the computing complexity required to conduct a fusion at the decision level. The more condensed comparison is shown in *Table 4*.

Table 4 Comparative analysis

S. No.	Author (year)	Aim	Research Methodology	Merits	Demerits	Findings	Research gap
1.	[84] (2023)	Suggest a three-level networking paradigm for networking that is built on decentralized sensor self-networking and cloud-based server platforms	The method allows for real-time evaluation of industrial field data as well as visualization in a variety of dimensions, stages, and granularities.	Solves problem of low reliability and cost effective	This scheme is exposed to some particular scenarios	The system is capable of storing and processing crucial information in real time, minimize the transfer and retention of data costs, and increase data transmission reliability and efficacy.	More algorithms and experiments may be designed for other scenarios

S. No.	Author (year)	Aim	Research Methodology	Merits	Demerits	Findings	Research gap
2.	[85] (2023)	BA-CPIC is an improved blockchain-assisted certificateless public integrity verification technique that might be used in a viable industrial cloud storage system.	Smart contract and Ethereum blockchain	Users' identity privacy is protected when they employ outsourced data retention and blockchain-assisted verification of integrity services.		It is offered equivalent security analysis using the certificateless security paradigm, which eliminates both the inherent problems of key escrow and cumbersome certificate administration.	
3.	[86] (2023)	Carried out a thorough review on cloud computing based cyber intelligent control operating system (ICIOS)	IEC61499 programming method and replaced tbe obsolete programmable logic controller (PLC)	Adapts industrial automation		ICIOS has been introduced	
4.	[87] (2023)	This work tries to summarize the evolution of intelligent multi-fault diagnosis and condition monitoring techniques in a systematic and wide manner.	AI based technologies, vibration analysis, IoT technologies, cloud computing	This article presents a brief overview of the research and development of intelligent, autonomous, and online fault detection systems based on the use of IoT, cloud computing, and AI approaches for predictive maintenance of mechanical systems.	More domains could be added to make the review more systematic	This article presents a brief overview of the research and development of intelligent, autonomous, and online fault detection systems based on the use of IoT, cloud computing, and AI approaches for predictive management of machinery.	For future study, several frequency domain and time domain features may be used, and vibration analog electrical signals can be turned into discrete data.
5.	[88] (2023)	This work presents a unique way to real-time detection of intrusions in ICS by combining cloud-based technology and big-data approaches.	Data fusion was used to merge various sources of data, leading in increased intrusion detection precision and efficacy.	When compared to previous solutions, obtains greater accuracy rates and displays improved efficiency in identifying intrusions.		Using the Multi-Layer Perceptron Classifier (MLPC), we achieved 99.98% accuracy in multiclass classification and 99.97% accuracy in binary categorization and can handle over 125,543 events in a single millisecond.	To further improve the distribution of attacks, deep learning techniques can be incorporated to generate more consistent and robust system.
6.	[89] (2023)	Auto-encoder and Long Short-Term Memory (LSTM) based ensemble deep learning model to identify unusual activities	To distinguish abnormal data from usual data, a combined deep learning model is used, comprised of LSTM AE to develop patterns of gathered data and a DT model to collect data outcomes.	Anomalies and outlier prediction, reduced complexity, and improved performance	-	The suggested model is tested on two independent real-world IIoT datasets, where it achieves a 0.997 accuracy rate.	-
7.	[90] (2022)	Using the eXtremely Gradient Boosting model, this study suggests an IDS for IIoT asymmetric data sets.	Built an XGBoost model to improve manipulation of imbalanced dataset	Overcame the problem of imbalanced and multiclass data processing	Not tuned for general data sets of security	obtained F1 score of 99.99% and 99.87 % in both data sets	To test the proposed model for specific application

S. No.	Author (year)	Aim	Research Methodology	Merits	Demerits	Findings	Research gap
8.	[91] (2022)	The purpose of this article is to discuss how to implement expedient privacy in an IIoT MIMOME networking environment.	The first step is to establish a closed-form formulation for the asymptotic regularised instantaneous privacy rate in an IIoT network system.	This approach can mitigate any adverse impact of the Eavesdropper's location while maintaining privacy.	Other real-world and theoretical applications are not explored.	explores the construction of optimum jamming parameters by presenting a method called Optimal Counter-Eavesdropping Channel Approximation (OPCECA) for addressing eavesdrop attacks in the IIoT	necessitates an examination of the OPCECA model's many conceptual and other real-world uses.
9.	[92] (2022)	offer a scalable management solution for on-device apps across scattered IoT nodes.	utilized TD to tag dispersed IoT devices, whose data, like interfaces, can be represented conceptually, allowing IoT devices to be accessible as internet resources.	This technique lets users administer IoT objects and artifacts horizontally through all sectors.	A semantic model must be constructed for each device, which may be inefficient given the various IoT modules engaged.	suggested a unique strategy for addressing diversity issues in the IIoT based on the standardized W3C TD, semantic modelling of objects, and KG.	Our recommended vocabularies are focused on our understanding. They must be continuously upgraded to ensure accuracy, quality, and widespread acceptability.
10.	[93] (2022)	to offer a strategy for improving the estimate of feature importance in data collected during the early phases of ransomware outbreaks.	The technique integrates an improved minimal Redundancy maximum Relevance (EmRmR) with the Term Frequency-Inverse Document Frequency (TF-IDF) weights to sift out runtime noise.	The suggested approach can determine if a specific characteristic in the relevant collection is significant or not.		The findings demonstrate the efficacy of the suggested approach, which achieves high classification accuracy with a low number of false positives.	to evaluate the technique's efficacy on a variety of datasets derived from Industrial IoT
11.	[70] (2021)	Provides a single platform for an industrial communications unit to handle the demerits of COVID-19 industry pandemics.	address the SDN with NFV services and utilize the SDN-based IoT framework	better throughput and response time with minor data failure	lack of data confidentiality and security	Suggested the framework, using NFV-based SDNs, for multi-controller execution IoT-SDN to manage an industrial automation system during the propagation of SARS-COV-2 virus.	can distributed data handling Blockchain technology and more security in the existing architecture.
12.	[71] (2021)	designed an efficient and extensible intelligent living authentication system.	developed and build a CA system based on microservices and fog schemes.	Addressing both high reliability and reduced latency.	•limited the physical activity. •health risks.	•adoption of an authentication scheme in the form of an OPNET Modeler. •introduction of virtual fog (VFOG) for IoT that helps in identifying various attacks by developing an authentication scheme.	does not consider the scheme leverages fog computing and microservices as the significant barriers
13.	[74] (2021)	The study's main objective is to identify the significance of deep transfer learning in the industrial network.	Performance comparison, classical CNN-based approach with other techniques with large datasets.	• Improving the design of scenarios and algorithms	Low latency and reduced power consumption	The study identified that different model structures had different accuracy levels, such as Transfer Learning with full dataset showed an accuracy of 98.6%, while Distributed transfer learning with a small dataset showed accuracy levels of 99.1%.	The research gap identified in the study was related to the complex interaction between CPS and IIoT systems.

S. No.	Author (year)	Aim	Research Methodology	Merits	Demerits	Findings	Research gap
14.	[75] (2021)	The primary purpose of this research is to study the development of new commercial and operational models, together with industry 4.0 and AI/ML, within the industrial digital model.	Hypothesis development	Flexibility	Interoperability issue	The study highlights the advantages of the IIoT in functioning the operating models and new businesses by focusing on developing a faster response to customer demands and meeting augmented flexibility needs.	The research gap is related to the lack of studies in the business application segment.
15.	[81] (2021)	The primary motive of this study is to ascertain the role of MLfor Massive IIoT.	Few-shot learning, case study	Solve MDP problems	High Communication Overheads	The study highlights the use of Deep Reinforcement Learning in improving the convergence performance of algorithms. It includes adopting the ACB scheme to optimize the uplink transmission process.	The research gap is related to the shortage of data about MLand IIoT applications in critical service requirements.
16.	[94] (2021)	presented a new 5G-enabled IIoT access control framework based on blockchain consortium to achieve effective and trustworthy access control.	design a two-step credit-based Raft consensus mechanism	lower consensus cost, high throughput, lesser hardware consumption	unoptimized data storage	new access control architecture for 5G-enabled IIoT based on the community blockchain. The system includes three kinds of chain codes implemented on industrial edge gateways.	Do not emphasize optimizing the blockchain node's data storage for IIoT.
17.	[95] (2021)	presented a sophisticated autonomous verifiable system for the building of a reliable, security-by-contract (SxC), secure IIoT ecosystem	Deploy blockchains as a verifiable and irreversible library to save these Network Manifests, which have been signed and verified by the device or industry authority under SxC-based innovative agreements	Improves adaptability, consistency, and explanations of behaviour.	data privacy and security	developed a system to understand expected MUD security and compliance contract behaviour patterns for each IoT device and verify policy	The data obtained from various devices and suppliers vary significantly and make unified administration a vital issue.
18.	[96] (2021)	Suggest the use of sparse autoencoder (SAE), long-short term memory (LSTM), and PSE to supervise an active learner.	An active malware detection learning framework utilizes PSE, SAE, and LSTM with action-value functions.	secure and resilient IIoT systems that are evident in contrast to previous studies	this research does not consider multi-class classification	Proposed using LSTM as an active learning process to identify harmful apps in industrial IoT environments with action-value function.	to explore the efficacy of the suggested technique to detect different malware software types.
19.	[79] (2021)	This article presents a new industrial environmental task processing system supported by Network-in-Box (NIB).	Because of the completion period of functioning machines, Q-learning-based efficiency assessments are carried out for various operational machinery states.	Greater efficiency in forecasting machines and timely completion of assigned and discharged tasks.		This paper offers a new industrial employment management framework with NIB paradigm integration.	
20.	[77] (2021)	to suggest a hybrid Blockchain method to ensure the safety of multi-national IIoT with multi-country offices.	Providing a transparent interaction among communicating entities via blockchain	DoS and DDoS threat detection, message modification threat, and identification delay.	cost overhead and data falsification are not considered	proposed a secure Blockchain IIoT method. The suggested method uses IoT devices to autonomously manage the whole business, such as data gathering, analysis, product distribution, and employees' location traceability	deployment of private cloud for data protection

S. No.	Author (year)	Aim	Research Methodology	Merits	Demerits	Findings	Research gap
21.	[78] (2020)	The study's primary objective is to evaluate the effect on the IIoT of open-source learning frameworks.	Experimentation and implementation of MLmodels in industrial domains.	It helps in developing the environment of the learning model.	High dependency on network	Suggested five open-source ML developmental framework models. The research also demonstrates data production in IoT environments and MLframework deployment.	The research gap of the study is that it is related to industry-specific issues such as customer behaviour and price optimization.
22.	[97] (2020)	The critical role of this study is to evaluate the function of ML for IIoT Applications.	QARMA algorithms, quantitative mining	QARMA algorithms provide good outcomes for RUL prediction.	Limited to off-the-shelf supervised learning algorithms	Provided an Industrial IoT platform that allows data and data flows from various heterogeneous sources to be collected and consumed on the floor. The platform follows the architectural paradigm of edge/cloud and can enable edge analysis and cloud analysis.	The research gap is that QARMA cannot be used when a lack of sensor data is.
23.	[80] (2020)	to analyse the utility of MLand deep learning algorithms on IIoT	Literature analysis	Improve existing processes and augmented infrastructure	Security, interoperability, real-time response, and future-readiness issues	Presented an in-depth overview of deep learning and MLmethods. This article also investigated the instances of ML and IoT information.	The research gap of the study is that it does not consider the exponential data growth conditions because of which there is a creation of issues in the identification learning algorithms.
24.	[73] (2020)	Analysed the function of the indoor location ML method for IIoT that uses Ultra-Wide Bandwidth (UWB) System.	the transmitted signal is analysed with the help of the UWB system. It also includes a channel model that helps in evaluating the UWB pulse experience.	gains localization accuracy. Possess excellent LoS and NLoS focusing precision.	cannot work in different environments when there is a plotting of different pre-processed data sets.	r UWB IPS system based on ML algorithms and NB principles to determine the area under the curve (AUC). It also helps enhance the localization accuracy levels that help reduce the distance between the anchors and increase tags.	The research gap identified in the study is related to the differences in the plotting of LoS and NLoS environments.
25.	[72] (2019)	to study edge computing for the IoT by surveying e-healthcare case studies.	The EH-IoT deployment uses: •Apache Edgent engine •an embedded hardware-based sensing unit, and IoT-based cloud repository.	•temperature controlling of medication. •detection of adverse medical incidents. •promotes the conduction of physical activity and its monitoring.	lack of IoT protocols and standardization and security and privacy threats	enhanced the working of the entire medical and drug sector by synchronizing the healthcare ecosystem with IoT cloud and local edge devices.	latency issues, low asset performance, security issues, poor processing speed, optimization issues, and high downtime
26.	[76] (2019)	Determined efficiency improvement for Blockchain-Enabled IIoT platforms via a deep reinforcement learning approach.	Blockchain-enabled IIoT system, transactional throughput to measure system's scalability.	•Development of DRL-based performance optimization framework	Latency and security issues	addresses the efficacy and security issues and designed a modulable blockchain system that helps in integrating the algorithms with the DRL technique.	The research gap identified in the research is related to considering limited consensus algorithms.

S. No.	Author (year)	Aim	Research Methodology	Merits	Demerits	Findings	Research gap
27.	[82] (2018)	This research is primarily conducted to evaluate the application of a Duelling Deep Q-learning method in the IIoT based on blockchain software.	System model, network model, Trust Feature Model, Computation Model	•Improves the throughput of the Blockchain system	Limited to network size	Proposed blockchain-based consensus protocol in distributed SDIIoT that helps develop synchronized network-wide views improved simulation outcomes and measured the trust features of the node.	The significant research gap identified in the study was related to the limited capacities of industrial devices.
28.	[83] (2016)	Presented a data-driven IIoT kernel-based method to anticipate missing QoS using kernel least mean squares (KLMS).	Pearson correlation coefficient (PCC) is used to find the relevant QoS values, and KLMS analyses the hidden relationships.	•Developing a data-driven scheme will allow a fine selection of qualified web services.	The scheme is limited to IIoT based on kernel least mean square (KLMS) and does not respond well in the absence of the proposed system.	It will help develop personalized IIoT applications based on cloud computing technologies. By using the scheme, there will be better prediction accuracy and a reduction in data redundancies	The research gap is that the KLMS algorithm applies only known QoS entries.

8.Conclusion and future work

IIoT is based on embedded technologies that help organizations to extend their application to vast levels by making use of innovative technologies such as ML, OT, M2M, and ICS. We examined that IIoT is based on several IoT taxonomies such as fog computing, edge computing, cloud computing, and distributed computing through the research. The different taxonomies help create an adequate IoT environment for the flow and transmission of information. We examined the application of IIoT systems in various smart city use cases such as smart energy, smart transportation, urban planning, and smart city characteristics. The use of different IIoT systems helps enhance the working of smart cities by developing infrastructure and organizing transportation activities. We examined the facts related to ML algorithms for IIoT-based innovative systems based on ML classifiers, regression algorithms, feature extraction algorithms, clustering, and neural networks. The different ML algorithms helped increase the IIoT application's efficacy by storing, recording, and transferring data. For example, the use of the K-means clustering process helped in classifying data and minimizing variance points. We discussed significant challenges and issues associated with IIoT systems and found that the significant issues with the implementation of IoT-enabled devices are associated with privacy and security issues. The other factors such as lack of skilled labour and high cost of installing and mending also impacted its application adversely.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare relevant to this article's content.

Author's contribution statement

Nabeela Hasan: Investigation, paper collection, prepared original draft, data collection, conceptualization, result interpretation, analysis of collected papers and study conception. **Mansaf Alam:** Design, supervision, investigated limitations of study and manuscript preparation.

References

[1] Iqbal R, Maniak T, Doctor F, Karyotis C. Fault detection and isolation in industrial processes using deep learning approaches. IEEE Transactions on Industrial Informatics. 2019; 15(5):3077-84.

[2] Shevchik SA, Masinelli G, Kenel C, Leinenbach C, Wasmer K. Deep learning for in situ and real-time quality monitoring in additive manufacturing using acoustic emission. IEEE Transactions on Industrial Informatics. 2019; 15(9):5194-203.

[3] Li Y, Carabelli S, Fadda E, Manerba D, Tadei R, Terzo O. Machine learning and optimization for production rescheduling in industry 4.0. The International Journal of Advanced Manufacturing Technology. 2020; 110:2445-63.

[4] Hossain MS, Al-hammadi M, Muhammad G. Automatic fruit classification using deep learning for industrial applications. IEEE Transactions on Industrial Informatics. 2018; 15(2):1027-34.

[5] Munirathinam S. Industry 4.0: industrial internet of things (IIOT). In advances in computers 2020 (pp. 129-64). Elsevier.

[6] Aceto G, Persico V, Pescapé A. A survey on information and communication technologies for industry 4.0: state-of-the-art, taxonomies, perspectives, and challenges. IEEE Communications Surveys & Tutorials. 2019; 21(4):3467-501.

[7] Ray PP. A survey of IoT cloud platforms. Future Computing and Informatics Journal. 2016; 1(1-2):35-46.
[8] Wan J, Li J, Imran M, Li D. A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Transactions on Industrial Informatics. 2019; 15(6):3652-60.
[9] Mohammed N, Chen R, Fung BC, Yu PS. Differentially private data release for data mining. In proceedings of the 17th international conference on knowledge discovery and data mining 2011 (pp. 493-501). ACM.
[10] Hasan N, Alam M. Evolution and insight in industrial internet of things (IIoT): importance and impact. Trust-Based Communication Systems for Internet of Things Applications. 2022:159-93.
[11] https://webstore.ansi.org/preview-pages/ISA/preview_S_990001_2007.pdf. Accessed 11 May 2023.
[12] Boyes H, Hallaq B, Cunningham J, Watson T. The industrial internet of things (IIoT): an analysis framework. Computers in Industry. 2018; 101:1-2.
[13] Da XL, He W, Li S. Internet of things in industries: a survey. IEEE Transactions on Industrial Informatics. 2014; 10(4):2233-43.
[14] Liao Y, Loures ED, Deschamps F. Industrial internet of things: a systematic literature review and insights. IEEE Internet of Things Journal. 2018; 5(6):4515-25.
[15] Piccarozzi M, Aquilani B, Gatti C. Industry 4.0 in management studies: a systematic literature review. Sustainability. 2018; 10(10):1-24.
[16] Raza S, Faheem M, Guenes M. Industrial wireless sensor and actuator networks in industry 4.0: exploring requirements, protocols, and challenges-a MAC survey. International Journal of Communication Systems. 2019; 32(15):e4074.
[17] Leminen S, Rajahonka M, Wendelin R, Westerlund M. Industrial internet of things business models in the machine-to-machine context. Industrial Marketing Management. 2020; 84:298-311.
[18] Zolanvari M, Teixeira MA, Gupta L, Khan KM, Jain R. Machine learning-based network vulnerability analysis of industrial internet of things. IEEE Internet of Things Journal. 2019; 6(4):6822-34.
[19] Mistry I, Tanwar S, Tyagi S, Kumar N. Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges. Mechanical Systems and Signal Processing. 2020; 135:106382.
[20] Khan WZ, Rehman MH, Zangoti HM, Afzal MK, Armi N, Salah K. Industrial internet of things: recent advances, enabling technologies and open challenges. Computers & Electrical Engineering. 2020; 81:106522.
[21] Ur RMH, Yaqoob I, Salah K, Imran M, Jayaraman PP, Perera C. The role of big data analytics in industrial internet of things. Future Generation Computer Systems. 2019; 99:247-59.
[22] Heer T, Garcia-morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K. Security challenges in the IP-based internet of things. Wireless Personal Communications. 2011; 61:527-42.
[23] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013; 29(7):1645-60.
[24] Cole PH, Ranasinghe DC. Networked RFID systems and lightweight cryptography. 2008.
[25] Pöhls HC, Angelakis V, Suppan S, Fischer K, Oikonomou G, Tragos EZ, et al. RERUM: building a reliable IoT upon privacy-and security-enabled smart objects. In wireless communications and networking conference workshops 2014 (pp. 122-7). IEEE.
[26] Sadeghi AR, Wachsmann C, Waidner M. Security and privacy challenges in industrial internet of things. In proceedings of the 52nd annual design automation conference 2015 (pp. 1-6). ACM.
[27] Atamli AW, Martin A. Threat-based security analysis for the internet of things. In international workshop on secure internet of things 2014 (pp. 35-43). IEEE.
[28] Zhang ZK, Cho MC, Wang CW, Hsu CW, Chen CK, Shieh S. IoT security: ongoing challenges and research opportunities. In 7th international conference on service-oriented computing and applications 2014 (pp. 230-4). IEEE.
[29] Arends R, Austein R, Larson M, Massey D, Rose S. DNS security introduction and requirements. 2005.
[30] http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf. Accessed 30 October 2023.
[31] Shahid R. Lightweight security solutions for the internet of things (Doctoral Thesis). UMI Order Number: ID Code: 5548. Mälardalen University. 2013.
[32] Ziegeldorf JH, Morchon OG, Wehrle K. Privacy in the internet of things: threats and challenges. Security and Communication Networks. 2014; 7(12):2728-42.
[33] Qureshi AS, Khan A, Shamim N, Durad MH. Intrusion detection using deep sparse auto-encoder and self-taught learning. Neural Computing and Applications. 2020; 32:3135-47.
[34] Lanckriet GR, Ghaoui LE, Bhattacharyya C, Jordan MI. A robust minimax approach to classification. Journal of Machine Learning Research. 2002; 3:555-82.
[35] Xu H, Caramanis C, Mannor S. Robust regression and lasso. Advances in Neural Information Processing Systems. 2008.
[36] Paschali M, Conjeti S, Navarro F, Navab N. Generalizability vs. robustness: adversarial examples for medical imaging. International conference on medical image computing and computer-assisted intervention 2018 (pp. 493-501). Springer.
[37] Tang C, Li W, Wang P, Wang L. Online human action recognition based on incremental learning of weighted covariance descriptors. Information Sciences. 2018; 467:219-37.
[38] Ristin M, Guillaumin M, Gall J, Van GL. Incremental learning of random forests for large-scale image

classification. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2015; 38(3):490-503.
[39] Du H, Teng S, Yang M, Zhu Q. Intrusion detection system based on improved SVM incremental learning. In international conference on artificial intelligence and computational intelligence 2009 (pp. 23-8). IEEE.
[40] Miorandi D, Sicari S, De PF, Chlamtac I. Internet of things: vision, applications and research challenges. Ad Hoc Networks. 2012; 10(7):1497-516.
[41] Alkhabbas F, Spalazzese R, Davidsson P. Characterizing internet of things systems through taxonomies: a systematic mapping study. Internet of Things. 2019; 7:100084.
[42] Wang Y, Li J, Wang HH. Cluster and cloud computing framework for scientific metrology in flow control. Cluster Computing. 2019; 22:1189-98.
[43] Mukherjee M, Shu L, Wang D. Survey of fog computing: fundamental, network applications, and research challenges. IEEE Communications Surveys & Tutorials. 2018; 20(3):1826-57.
[44] Yu W, Liang F, He X, Hatcher WG, Lu C, Lin J, et al. A survey on the edge computing for the internet of things. IEEE Access. 2017; 6:6900-19.
[45] Satyanarayanan M. The emergence of edge computing. Computer. 2017; 50(1):30-9.
[46] Stergiou C, Psannis KE, Kim BG, Gupta B. Secure integration of IoT and cloud computing. Future Generation Computer Systems. 2018; 78:964-75.
[47] Yang C, Huang Q, Li Z, Liu K, Hu F. Big data and cloud computing: innovation opportunities and challenges. International Journal of Digital Earth. 2017; 10(1):13-53.
[48] Li S, Maddah-ali MA, Yu Q, Avestimehr AS. A fundamental tradeoff between computation and communication in distributed computing. IEEE Transactions on Information Theory. 2017; 64(1):109-28.
[49] El-sayed H, Sankar S, Prasad M, Puthal D, Gupta A, Mohanty M, et al. Edge of things: the big picture on the integration of edge, IoT and the cloud in a distributed computing environment. IEEE Access. 2017; 6:1706-17.
[50] Kanawaday A, Sane A. Machine learning for predictive maintenance of industrial machines using IoT sensor data. In 8th international conference on software engineering and service science 2017 (pp. 87-90). IEEE.
[51] Hammi B, Khatoun R, Zeadally S, Fayad A, Khoukhi L. IoT technologies for smart cities. IET Networks. 2018; 7(1):1-3.
[52] Marinakis V, Doukas H. An advanced IoT-based system for intelligent energy management in buildings. Sensors. 2018; 18(2):1-16.
[53] Paul A, Chilamkurti N, Daniel A, Rho S. Chapter 8-big data collision analysis framework. Intelligent Vehicular Networks and Communications. 2017: 177-84.
[54] Distefano S, Merlino G, Puliafito A, Cerotti D, Dautov R. Crowdsourcing and stigmergic approaches for (Swarm) intelligent transportation systems. In human centered computing: third international conference, HCC 2017, Kazan, Russia, Revised Selected Papers 3 2018 (pp. 616-26). Springer International Publishing.
[55] Zantalis F, Koulouras G, Karabetsos S, Kandris D. A review of machine learning and IoT in smart transportation. Future Internet. 2019; 11(4):1-23.
[56] Chowdhury DN, Agarwal N, Laha AB, Mukherjee A. A vehicle-to-vehicle communication system using IoT approach. In second international conference on electronics, communication and aerospace technology 2018 (pp. 915-9). IEEE.
[57] Geetha S, Cicilia D. IoT enabled intelligent bus transportation system. In 2nd international conference on communication and electronics systems 2017 (pp. 7-11). IEEE.
[58] Hasan N, Alam M. Envisaging industrial perspective demand response using machine learning. In proceedings of data analytics and management: ICDAM 2021, 2022 (pp. 331-42). Springer Singapore.
[59] Nausicaa J. Smart street lighting system using IoT and cloud computing. International Journal for Research in Applied Science & Engineering Technology. 2021; 9(6):5014-18.
[60] Ryder B, Wortmann F. Autonomously detecting and classifying traffic accident hotspots. In proceedings of the international joint conference on pervasive and ubiquitous computing and proceedings, international symposium on wearable computers 2017 (pp. 365-70). ACM.
[61] Rani P, Kumar R, Jain A, Lamba R. Taxonomy of machine learning algorithms and its applications. Journal of Computational and Theoretical Nanoscience. 2020; 17(6):2508-13.
[62] Berrar D. Bayes' theorem and naive Bayes classifier. Encyclopedia of Bioinformatics and Computational Biology: ABC of Bioinformatics. 2018; 403:412.
[63] Setiawan B, Djanali S, Ahmad T. A study on intrusion detection using centroid-based classification. Procedia Computer Science. 2017; 124:672-81.
[64] Sun W, Liu J, Yue Y. AI-enhanced offloading in edge computing: when machine learning meets industrial IoT. IEEE Network. 2019; 33(5):68-74.
[65] Hussain T, Muhammad K, Del SJ, Baik SW, De AVH. Intelligent embedded vision for summarization of multiview videos in IIoT. IEEE Transactions on Industrial Informatics. 2019; 16(4):2592-602.
[66] Oracevic A, Dilek S, Ozdemir S. Security in internet of things: a survey. In international symposium on networks, computers and communications 2017 (pp. 1-6). IEEE.
[67] Patel KK, Patel SM, Scholar P. Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. International Journal of Engineering Science and Computing. 2016; 6(5):6122-31.
[68] Udoh IS, Kotonya G. Developing IoT applications: challenges and frameworks. IET Cyber-Physical Systems: Theory & Applications. 2018; 3(2):65-72.
[69] Mahdavinejad MS, Rezvan M, Barekatain M, Adibi P, Barnaghi P, Sheth AP. Machine learning for internet

of things data analysis: a survey. Digital Communications and Networks. 2018; 4(3):161-75.
[70] Rahman A, Chakraborty C, Anwar A, Karim MR, Islam MJ, Kundu D, et al. SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic. Cluster Computing. 2021:1-8.
[71] Li J, Jin J, Lyu L, Yuan D, Yang Y, Gao L, et al. A fast and scalable authentication scheme in IOT for smart living. Future Generation Computer Systems. 2021; 117:125-37.
[72] Ray PP, Dash D, De D. Edge computing for internet of things: a survey, e-healthcare case study and future direction. Journal of Network and Computer Applications. 2019; 140:1-22.
[73] Che F, Ahmed A, Ahmed QZ, Zaidi SA, Shakir MZ. Machine learning based approach for indoor localization using ultra-wide bandwidth (UWB) system for industrial internet of things (IIoT). In international conference on UK-China emerging technologies 2020 (pp. 1-4). IEEE.
[74] Liu X, Yu W, Liang F, Griffith D, Golmie N. Toward deep transfer learning in industrial internet of things. IEEE Internet of Things Journal. 2021; 8(15):12163-75.
[75] Mateo FW, Redchuk A. The emergence of new business and operating models under the industrial digital paradigm. industrial internet of things, platforms, and artificial intelligence. machine learning. Journal of Mechanics Engineering and Automation. 2021; 11(2):54-60.
[76] Liu M, Yu FR, Teng Y, Leung VC, Song M. Performance optimization for blockchain-enabled industrial Internet of things (IIoT) systems: a deep reinforcement learning approach. IEEE Transactions on Industrial Informatics. 2019; 15(6):3559-70.
[77] Rathee G, Ahmad F, Sandhu R, Kerrache CA, Azad MA. On the design and implementation of a secure blockchain-based hybrid framework for industrial internet-of-things. Information Processing & Management. 2021; 58(3):102526.
[78] Christou IT, Kefalakis N, Zalonis A, Soldatos J. Predictive and explainable machine learning for industrial internet of things applications. In international conference on distributed computing in sensor systems 2020 (pp. 213-8). IEEE.
[79] Velusamy N, Al-turjman F, Kumar R, Ramakrishnan J. A framework for task allocation in IoT-oriented industrial manufacturing systems. Computer Networks. 2021; 190:107971.
[80] Ambika P. Machine learning and deep learning algorithms on the industrial internet of things (IIoT). Advances in Computers. 2020; 117(1):321-38.
[81] Zhou H, She C, Deng Y, Dohler M, Nallanathan A. Machine learning for massive industrial internet of things. IEEE Wireless Communications. 2021; 28(4):81-7.
[82] Qiu C, Yu FR, Yao H, Jiang C, Xu F, Zhao C. Blockchain-based software-defined industrial internet of things: a dueling deep ${Q} $-learning approach. IEEE Internet of Things Journal. 2018; 6(3):4627-39.
[83] Luo X, Liu J, Zhang D, Chang X. A large-scale web QoS prediction scheme for the industrial internet of things based on a kernel machine learning algorithm. Computer Networks. 2016; 101:81-9.
[84] Wang M, Xu CA, Lin Y, Lu Z, Sun J, Gui G. A distributed sensor system based on cloud-edge-end network for industrial internet of things. Future Internet. 2023; 15(5):1-17.
[85] Yang T, Hao W, Yang Q, Wang W. Cloud-edge coordinated traffic anomaly detection for industrial cyber-physical systems. Expert Systems with Applications. 2023:120668.
[86] Su W, Xu G, He Z, Machica IK, Quimno V, Du Y, et al. Cloud-edge computing-based ICICOS framework for industrial automation and artificial intelligence: a survey. Journal of Circuits, Systems and Computers. 2023:2350168.
[87] Maurya M, Panigrahi I, Dash D, Malla C. Intelligent fault diagnostic system for rotating machinery based on IoT with cloud computing and artificial intelligence techniques: a review. Soft Computing. 2023:1-8.
[88] Abid A, Jemili F, Korbaa O. Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques. Cluster Computing. 2023:1-22.
[89] Lu Y, Yang L, Yang SX, Hua Q, Sangaiah AK, Guo T, et al. An intelligent deterministic scheduling method for ultralow latency communication in edge enabled industrial internet of things. IEEE Transactions on Industrial Informatics. 2022; 19(2):1756-67.
[90] Le TT, Oktian YE, Kim H. XGBoost for imbalanced multiclass classification-based industrial internet of things intrusion detection systems. Sustainability. 2022; 14(14):1-21.
[91] Anajemba JH, Iwendi C, Razzak I, Ansere JA, Okpalaoguchi IM. A counter-eavesdropping technique for optimized privacy of wireless industrial IoT communications. IEEE Transactions on Industrial Informatics. 2022; 18(9):6445-54.
[92] Ren H, Anicic D, Runkler TA. Towards semantic management of on-device applications in industrial IoT. ACM Transactions on Internet Technology. 2022; 22(4):1-30.
[93] Ahmed YA, Huda S, Al-rimy BA, Alharbi N, Saeed F, Ghaleb FA, et al. A weighted minimum redundancy maximum relevance technique for ransomware early detection in industrial IoT. Sustainability. 2022; 14(3):1-15.
[94] Feng Y, Zhang W, Luo X, Zhang B. A consortium blockchain-based access control framework with dynamic orderer node selection for 5G-enabled industrial IoT. IEEE Transactions on Industrial Informatics. 2021; 18(4):2840-8.
[95] Krishnan P, Jain K, Achuthan K, Buyya R. Software-defined security-by-contract for blockchain-enabled MUD-aware industrial IoT edge networks. IEEE

Transactions on Industrial Informatics. 2021; 18(10):7068-76.
[96] Khowaja SA, Khuwaja P. Q-learning and LSTM based deep active learning strategy for malware defense in industrial IoT applications. Multimedia Tools and Applications. 2021; 80(10):14637-63.
[97] Khan AI, Al-badi A. Open source machine learning frameworks for industrial internet of things. Procedia Computer Science. 2020; 170:571-7.

Nabeela Hasan is presently working as Senior Research Fellow with the Department of Computer Science, Jamia Millia Islamia, New Delhi, India. She has completed MCA from Jamia Millia Islamia, India in 2018, BCA from Banasthali University, Rajasthan in 2013, and she is pursuing Ph.D. in field of IoT and Big Data from Jamia Millia Islamia, New Delhi. She has a rich academics & research experience in various areas of Computer Science. She has published many research articles in reputed journals, conferences and books. Her research area is Big Data Analytics, Machine Learning, Cloud Computing and Industrial Internet of things.
Email: nabeela1910394@st.jmi.ac.in

Dr. Mansaf Alam currently holds the position of Professor in the Department of Computer Science within the Faculty of Natural Sciences at Jamia Millia Islamia, New Delhi-110025. He serves as a Young Faculty Research Fellow at DeitY, Govt. of India, and holds the position of Editor-in-Chief for the Journal of Applied Information Science. Dr. Alam has contributed significantly to the academic field, publishing numerous research articles in reputable international journals and proceedings of esteemed international conferences published by IEEE, Springer, Elsevier Science, and ACM. His research interests encompass a broad spectrum, including Big Data Analytics, Machine Learning & Deep Learning, IoT, Cloud Computing, Cloud Database Management System (CDBMS), Object-Oriented Database System (OODBMS), Bioinformatics, Information Retrieval, and Data Mining. In addition to his research contributions, Dr. Alam actively contributes to the academic community. He serves as a reviewer for various journals of international repute, such as Information Science published by Elsevier Science. Furthermore, he is a member of the program committee for several reputed international conferences and holds positions on the editorial boards of some prestigious international journals in the field of Computer Sciences.
Email: malam2@jmi.ac.in

Appendix I

S. No.	Abbreviation	Description
1	2G/3G/4G	Second/Third/Fourth Generation
2	ACB	Access Class Barring
3	AI	Artificial Intelligence
4	ANN	Artificial Neural Network
5	API	Application Programming Interfaces
6	AR	Augmented Reality
7	B2B	Business-to-Business
8	CA	Certification Authority
9	CAaaS	Continuous Analytics as a Service
10	cHMM	continuous Hidden Markov Model
11	CPS	Cyber Physical Systems
12	CPU	Central Processing Unit
13	DBSCAN	Density-Based Clustering Algorithm
14	DDoS	Distributed Denial of Service
15	DNP	Distributed Network Protocol
16	DNSSEC	Domain Name Service Security Extension
17	DR&PP	Data Routing and Pre-processing
18	DRL	Deep Reinforcement Learning
19	E-DPE	Edge Data Processor Engine
20	FF-NN	Feed Forward- Neural Network
21	GITA	Genetic Indoor Tracking Algorithm
22	GPRS	General Packet Radio Service
23	GPS	Global Positioning System
24	GSM	Global System for Mobile Communication
25	HMI	Human-Machine Interface
26	ICIOS	Intelligent Control Operating System
27	ICS	Industrial Control Systems
28	ICT	Information Communications Technology
29	IDS	Intrusion Detection System
30	IEC	International Electrotechnical Commission
31	IETF	Internet Engineering Task Force
32	ISEMIC	Intelligent Information System for Monitoring and Verification of Energy Management in Cities
33	KLMS	Kernel Least Mean Squares
34	kNN	K Nearest Neighbor
35	LCD	Liquid Crystal Display
36	LASSO	Least Absolute Shrinkage and Selection Operator
37	M2M	Machine-to-Machine
38	MQTT	Message Queuing Telemetry Transport
39	MRF	Markov Random Fields
40	NIB	Network Information Base
41	NLoS	Non-Line-of-Sight
42	OPCECA	Optimal Counter-Eavesdropping Channel Approximation
43	OS	Operating System
44	OT	Operational Technology
45	PCC	Pearson Correlation Coefficient
46	PLC	Programmable Logic Controller
47	PKC	Public-Key Cryptography
48	PSE	Phase Space Embedding

49	QARMA	From Qualcomm ARM Authenticator
50	RBF	Radial Basis Function
51	RNA	Ribonucleic Acid
52	RFC	Request for Comments
53	RFID	Radio Frequency Identification
54	SAE	Sparse Autoencoder
55	SCADA	Supervisory Control and Data Acquisition
56	SDIIoT	Software Defined Industrial Internet of Things
57	SDN	Software-Defined Networking
58	SOA	Service-Oriented Architecture
59	SQL	Structured Query Language
60	SSL	Smart Street Lights
61	SVM	Support Vector Machine
62	SxC	Security-by-Contract
63	TF-IDF	Term Frequency-Inverse Document Frequency
64	UID	Unique Identifier
65	UWB	Ultra-Wide Bandwidth
66	V2V	Vehicle-to-Vehicle
67	VR	Virtual Reality
68	WSAN	Wireless Sensor and Activator Network
69	XML	eXtended Markup Language