International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I12P211

Volume 70 Issue 12, 99-108, December 2022

Review Article

A Survey of Security Issues in IIoT and Fault Identification using Predictive Analysis in Industry 4.0

G. Anitha[1], Abirami Manoharan[2], Hariprasath Manoharan[3], P. Ganesan[4]

[1]*Department of Electronics and Communication Engineering, RMD. Engineering College, Chennai, Tamil Nadu.*
[2,4]*Department of Electrical and Electronics Engineering, Government College of Engineering, Srirangam, Trichy, Tamil Nadu.*
[3]*Department of Electronics and Communication Engineering, Panimalar Engineering College, Poonamallee, Tamil Nadu.*

[1]*Corresponding Author : anirajkan@gmail.com*

Received: 02 June 2022 Revised: 16 August 2022 Accepted: 29 November 2022 Published: 24 December 2022

Abstract *- Machine intelligence (ML) and Artificial intelligence (AI) advancements affect a variety of research professions. These primary contributors would have been difficult to attain in the past by employing conventional optimization techniques. Manufacturers benefit significantly from increased automation technology, which is one manufacturing where artificial intelligence and machine learning may offer a range of choices. The Industrial Iot has intensified demand in Industry 4.0. (IIoT), which enables a superior wireless network for actual plant data processing and analysis. A detailed analysis of the essential functions, including fault diagnosis, forecast, and protection in manufacturing 4.0, is investigated in this study, as the safety of computer learning-based methods for these operations. In addition, the human element as contractors or labourers in the Industry 4.0 environment is a significant source of worry and underlined genuine concerns in these sectors to inspire additional research.*

Keywords *- Defect detection, Forecast, Industrial IoT, Machine learning, and Safety.*

1. Introduction

It aspires to create an intelligent production of goods and, as a result, advanced manufacturing with tight customer and competitor partner connectivity. With the rise of IIoT, Industry 4.0 is a set of data that emphasizes automating and linking all physical processes across the board. [3]. Manufacturing 4.0 is an advancement above Industry 3.0. The equipment was then provided with detectors and remote access, and it was connected to a central processing system (CPS) that could understand the whole production process and make intelligent decisions. **Figure 1** depicts IoT/IIoT designs that include machinery, tools, connections, services, and software [4]. The technology works in a closed loop to create personalized and customized things that fit the needs of final consumers. Assessment, Connectivity, Processing, and Application Layer are the four levels that make up this system. Sensors of various types, RFID printers, surveillance equipment, GPS technologies, and other equipment make up this installation. These gadgets may be exacerbated by equipment such as automated guided vehicles (AGVs), material handling, automated machines, and so on in an industrial context. The current research aims to analyze and compile numerous reputable papers discussing various strategies for doing predictive analytics on IIoT data. The goal is to perform a systematic and complete investigation of different methodologies to allow analytics on high-quality telemetry data.

2. Industrial Internet of Things (IIoT)

The Internet of Things (IoT) alters the world through sensor information, motors, processors, and machines to exchange data and present innovative services [11]. It has a broad the spectrum of uses, including smart homes, smart cities, smart grids, farming, smart buildings, transport networks, and e-Health [12]. Industrial businesses or corporations utilize IoT technology to connect devices intelligently with various industrial uses. The phrase IIoT is frequently used to differentiate these technologies from generic IoT applications [13], [14]. As shown in **Figure 2**, the Smart Manufacturing Collaboration established a baseline design for IIoT that includes three levels: edge, gateway, and corporate. This same edge tier uses information from edge devices via border portals. It sends it to the platform layer, which supports financial services, information services, and research. Furthermore, the operational tier provides end-user interaction and leverages business processes [15]. Software and decision-making assistance programs IoT devices may leverage integrated smart sensors to minimize the quantity of data sent and hence processing requirements of the platform and business tiers. Depending on the conditions, such compact systems include pre-processing techniques that validate, linearize, magnify, filter or correct the actual control voltage. Sensor fusion can be used in IoT devices with several sensor units to provide resilience or a merged assessment of collecting data, such as in image processing applications [16].

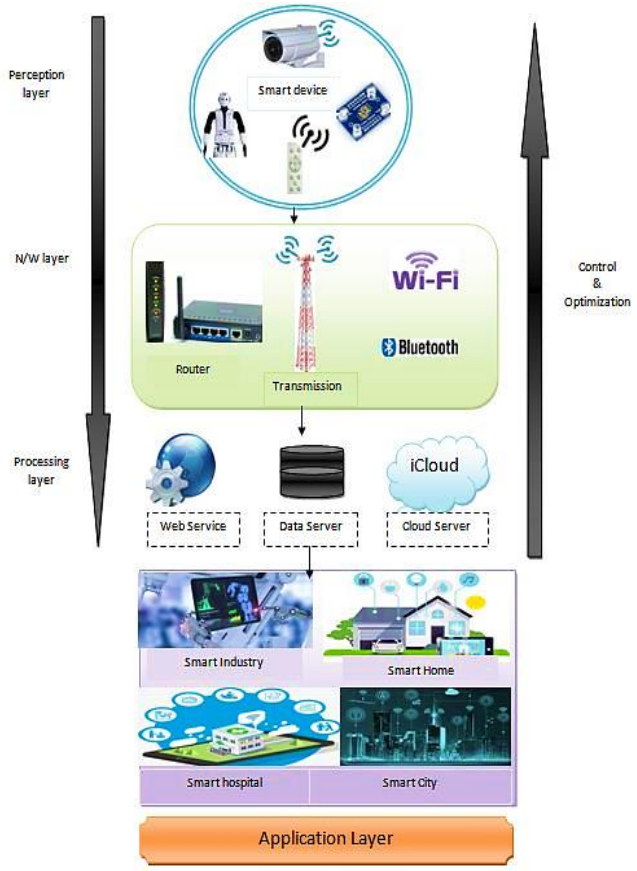

Fig. 1 Generalized IoT/IIoT System Architecture

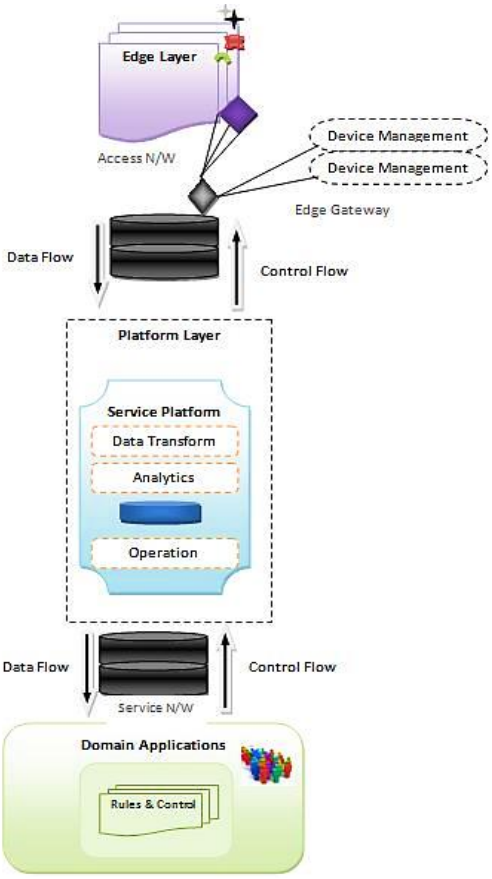

Fig. 2 Three-Layer Industrial IoT System Architecture
a system that specifies how real and digital things interact with other

Industries 4.0 is a German effort aimed at improving the manufacturing industry's profitability and adaptability by increasing cognitive, Communication, and coordination between manufacturing and logistical operations [1], [21], [22]. The Reference Architecture Design Industries 4.0 (RAMI 4.0) and the I4.0 Element are the two most significant Industries 4.0 standardization outcomes. RAMI 4.0 is a common three-dimensional framework that organizes and connects all aspects and IT modules. The I4.0 Module, on either extreme, would be a single.

The IIoT focuses on embedded machines and their connectivity to generate massive volumes of data, as seen In Figure 3. Big data, on either extreme, offers platforms of information dissemination and computing intelligence to aid IIoT information analysis and visualization [25], [52]. Operations should become more effective and versatile due to adopting Industries 4.0 concepts in the manufacturing sector, taking advantage of the growing transparency. Conventional technologies, on either extreme, struggle to store and evaluate the providing accessibility as it becomes extensive and complicated. As a result, there is widespread agreement that data analysis and IIoT capabilities are inextricably linked and should advance in tandem [26].

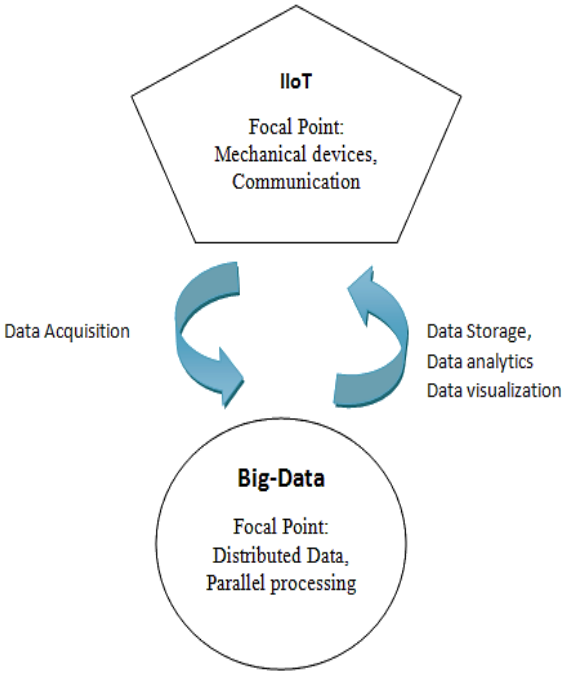

Fig. 3 Interrelation between IIoT & Big-Data

Table 1. IoT-related features of a few cloud platforms

IoT approaches	IoT AWS	Watson IoT	Azure IoT Suite	IoT SAP	Mind Sphere	Bosch IoT Suite	Thing Worx
IoT Networks	+	+	+	+	+	+	+
Technology for Interconnection	+	+	+	+	+	+	+
IIoT software	+	+	+	+	+	+	+
IIoT connection	-	-	-	-	+	+	-
Cloud Computing	+	+	+	+	+	-	-

No Data Accessible Mythology: (+) Assisted, (-) Not Supported, or No Data Available

3. Security Attacks in IoT

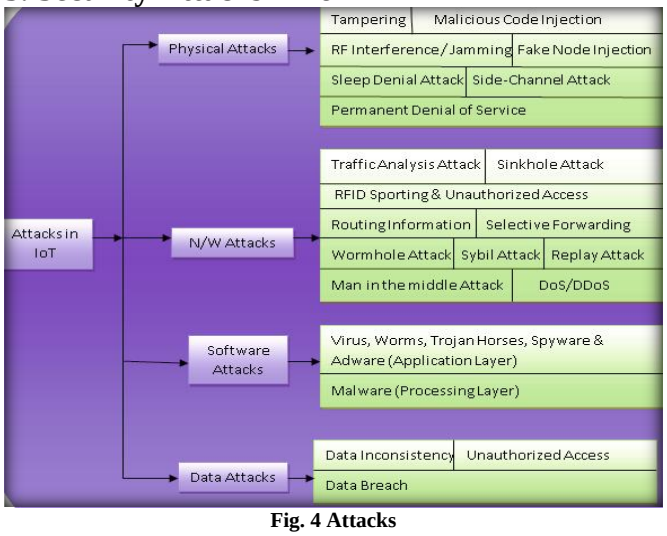

Fig. 4 Attacks

4. Fault Detection

Due to the autonomous and self-optimized equipment maintenance and the quantity of information recorded in actual, problem identification and analysis is a critical and challenging procedure in Industry 4.0. Currently, diagnostic applications for the testing phase involve producing information in authentic contexts, leading to poor diagnostic performance and requiring professionals to complete numerous error-handling cycles. In addition, physical inquiry to determine defects results in longer repair times of many days or even weeks. In Machine learning (ML) approaches, massive surveillance programs' massive data should be evaluated in real-time to identify aberrant operations and defects appropriately. Data gathering, computational modelling for extracting features, and fault classification are the three primary phases in defect identification and treatment.

To add to the prediction performance proposed framework, Deep learning techniques are used to analyze the information and execute the defeat diagnosis categorization. Manufacturing procedures for automobiles' higher-flow headlights and wire components were studied using this technology. Figure 4 also shows a variety of AI/ML systems for defect detection, forecast, and management. These topics are thoroughly examined in the following sections, emphasizing the impact of ML-based methods.

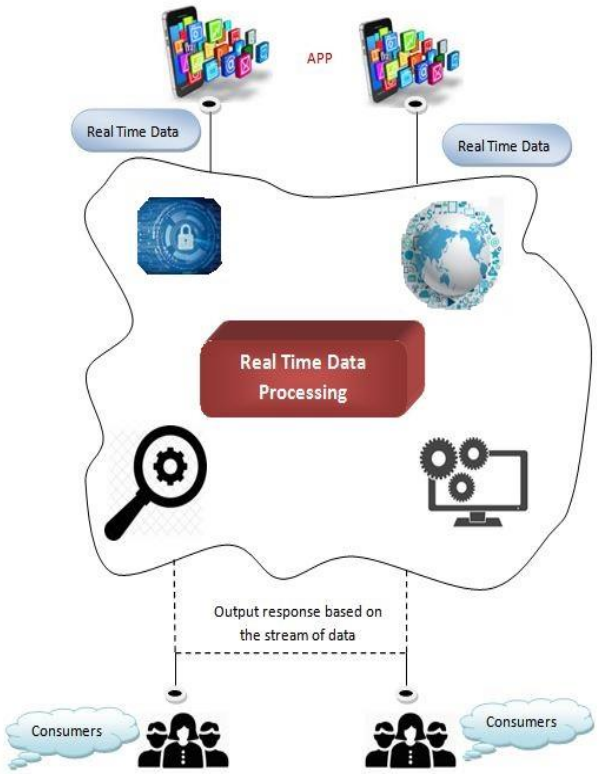

Fig. 5 Real-time data processing and Analytics

5. Related Works

The term "Internet of Things" (IoT) refers to future virtual networks. There are two distinct groups. Wearable technologies, smart home appliances, and connected products are part of the "Customer IoT." Connected smart electricity, production, healthcare, and transportation are part of the "Manufacturing IoT." The Customer IoT or the Industrial IoT is more dissimilar than comparable in technology. Since it is more understandable to most people, the Customer receives more interest. Consumer networks often link only a few points to the cloud, such as a watch or a thermostat. Usually, reliability is not a big deal. Most technologies are "Greenfield," which means they have no current facilities or decentralized architecture to contemplate. A slew of interesting modern innovations on the horizon will transform daily living. On the other hand, the Customer IoT is a natural network development from human-operated machines to mechanized items surrounding humans [1].

Industrial Internet-of-Things (IIoT) is rapidly expanding and intelligent sensors, equipment, gadgets, and technology are increasingly deployed and integrated through wireless connections. Industrial practices would improve dramatically due to this combined hardware-software strategy, resulting in industrial intelligence for more efficient production. Recent advancements in its big processing and analysis are necessary to discover and utilize hidden valuable and vital data from the manufacturing method to realize such manufacturing knowledge. However, on either extreme, large-scale broadcasting, which multi-attributes its data from manufacturing techniques, is noisy and contains redundancy. As a result, a proper data treatment method, such as convolution, was required to manage these IIoT data. On the other hand, existing convolution dissection approaches are inefficient and incapable of handling the capacity constraints of large-scale IIoT big data [2].

Essential infrastructure systems are necessary for a society's and the country's smooth economic operation. Safety and adaptability are becoming pressing challenges for critical infrastructures of Web Internet-of-Things (its) / Industrial IoT (IIoT) devices grows, as does the amount of data generated and gathered. Blockchain is a decentralized and private database that includes all types in a hierarchical increasing sequence of blocks. Edge devices bring the cloud's operations closer to the processing activities. Early and scalability issues can be mitigated by combining blockchain and edge computing paradigms [3].

Industrial Internet-of-Things (IIoT) connections, particularly audiovisual IIoT connections, require electricity connectivity to cloud computing, including globally dispersed information services. Changing final demand needs, imbalanced connection fuel economy, asymmetrical or duration connection use, and customer support frequency or latency limit are all substantial challenges [4].

The Industrial Internet of Things (IIoT) has opened the possibility of creating digitalized manufacturing systems. The Radio-Frequency Identification (RFID) approach, A key technology of the IIoT, is object recognition, which allows industrial members to recognize objects and anchor generalized linear out data for them. They can also use the cloud service to communicate IoT data, allowing for information sharing and supporting important manufacturing choices. However, collecting IoT files in the database demands an access control technique to safeguard vital firm data. On the other hand, traditional encryption and access control approach to time series IoT data are inefficient and cause data loss.

Conventional sign encryption techniques with equality checking are designed for a single cryptosystem. Therefore, they are inadequate for the complex heterogeneous Industrial Internet of Things network (IIoT). Because of the fast rise of IoT techniques, many critical technologies, including consortium virtually smart factories, are now accessible. However, the significant convergence of industry 4.0 with business networks in the IIoT networks exposes the industrial world to considerable cyber-risks. Traditional IT safety fails to prevent cyber attacks over IIoT networks due to a significant security perimeter, enterprise multilayer protocols, restricted maintenance possibilities, different communications architectures, and a prominent trust demarcation. Moreover, for crucial response time commitments, recent secure technologies such as safe DNP 3.0 (Distributed Network Protocol) are confined to weak hash functions [6].

IIoT manufacturing is an important research area that evolved from IoT. The Internet of Things (IoT) links industrial machines to the Internet, develops data collection, sharing, and analytic tools, or improves operations and procedures to reduce costs and enhance output. Information technology in the IIoT can drastically reduce judgment delay, conserve available bandwidth, and maintain privacy to some level. This report summarizes the current state of network edge development in the IIoT[7].

First, IIoT and cloud technology ideas are addressed, followed by a detailed discussion and summary of cloud computing technology. Then, a future framework is given from the standpoint of computing power, and its technological advancement in networking, job scheduling, storage systems and processing, safety, and standardization was examined [8].

Using electronic objects, the IIoT is predicted to give a possible chance to change the manufacturing effectiveness of the already-in-place industrial infrastructure. However, information integrity is a significant concern due to the shady character of communications networks. Furthermore, the security, connectivity, and diversity of equipment present serious issues regarding IIoT applications, as existing authentication methods for the IIoT ecosystem are vulnerable to privacy violations and cannot ensure communication security in heterogeneous industrial facilities. To tackle these issues, this study offers proxy re-signature as a private information authentication method for heterogeneous networks in the IIoT. The suggested technique allows for heterogeneous connection among ID-based and CL-based cryptosystems and meets several safety requirements. A random oracle model's modified Algorithmic Diffie-Hellman (eCDH) postulate was used to be implemented in an IIoT environment [9].

The Internet of Things (IoT) framework has a crucial application within industrial areas. Moreover, IIoT, also known as Industry 4.0, promises to transform manufacturing by combining massive numbers of advanced wearable sensors with new internet technology like cloud calculation

or surveillance intelligence. However, IIoT was accompanied by an increased level of interconnection that presents the potential for both the enterprises that embrace it and cyber criminals. Furthermore, IoT security is currently one of the most significant roadblocks to the mainstream deployment of IIoT technology. Understandably, such issues have resulted in a massive increase in existing papers [10].

Industrial Internet of Things, a unique manufacturing connection might be connected (IIoT). Manufacture IIoT and various wireless considerations for sensing devices are essential. The IIoT sensor keeps track of the state of manufacturing devices and systems. As a result, the most critical concerns are dependability and safety. It brings up many old and new risks linked with the industrial economy. Viruses, threats, and assaults could affect its devices in various ways. Consequently, an effective protection plan is needed to keep the millions of youth devices secure from these threats.

Furthermore, IIoT devices with limited resources have not been created with adequate security mechanisms. Consequently, cloud, fog, and edge-based IIoT have gotten a lot of interest in the research community in recent years. Computationally heavy functions like security, database management, strategic planning, and monitoring were handled by a robust computer infrastructure in the cloud or fog. A hash signature is used to verify the device's authenticity. An accurate detector aggregation strategy focused on the level (N) separation of the group (D). Resource management utilizing SoftMax deep neural network (DNN) is presented to reduce latency and network bandwidth of IIoT devices. SoftMax-DNN classifies all demands arriving from the cluster members for effective resource allocation based on storage, processing, and connectivity demands. The suggested architecture outperforms the competition regarding power usage, delay, and safety strength [11].

The Internet of Things (IoT) could boost productivity and effectiveness by enabling sophisticated, remote monitoring. Still, it also raises the risk of cyberattacks. Recently, challenges to IoT systems or the need to mitigate risk have been a hot topic. Therefore, reliable Intrusion Detection Systems (IDSs) must be created for IoT applications. In addition, an up-to-date or appropriate IoT dataset for training and validation.

Furthermore, IDS-enabled IoT devices have few benchmark IoT as well as IIoT datasets to evaluate. This work addresses this issue by proposing novel IoT/IIoT datasets with underlying data that includes a label characteristic showing normal and malicious categories and a typed feature to identify the issues. The suggested database, dubbed TON IoT, contains Telemetry, data from its/services of youth, as well as Functioning Application and patterns from an IoT network, all of which were accumulated from a reasonable approximation of an intermediate network at the UNSW Canberra's Cyber Range and IoT Labs (Australia). This paper also discusses the suggested dataset tracking data for its/youth services and the services and their characteristics. TON provides several missing benefits in previous data sets: It includes a wide range of standard and attack events for various IoT services and heterogeneous data sources. [12]. To assess the uncertainty of the reduced energy muon flux, a high-volume scintillator sensor was applied to monitor the terrestrial halting muon rate under various locations, altitudes, protection, and climate circumstances. A year's worth of study was performed under various situations. This information could then be compared to cosmic ray muon computations to calculate the soft error rate owing to direct muon ionization [13].

With the rise of Machine Intelligence (AI) and Internet of Things (IoT) approaches aggressive attempts to mislead Deep Neural Networks (DNNs) used in Industrial IoT (it) implementations are becoming more common. Due to the skewed learning algorithm or weak underlying algorithms, aggressive assaults that make subtle changes to inputs might have disastrous repercussions. Although the current techniques show promise in guarding against malicious assaults, most of them should only deal with a limited number of known attacks, making it difficult to implement large-scale IIoT devices [14].

Recognition algorithms function better in controlled circumstances and decline with lighting, facial expression, and stance changes. For feature extraction, attempts have been devoted to investigating other face technologies such as infrared (IR) and 3-D. Studies show that fusing several face paradigms improves compared to single-modal feature extraction. It assesses the classification using thorough descriptions of relevant research and table summaries. The benefits and drawbacks of each face recognition methodology are examined. Furthermore, image datasets and technology assessments were discussed [15].

In current years, the Industrial Internet of Things (IIoT) was grown quickly. In IIoT, a private blockchain with decentralization, adaptable regulations, and robust data management could be used to collect and process data and address security concerns. The durability of blockchain, on the other hand, limits it. As a result, this article presents an improved optimization technique on Two Arch2 to enhance sustainability and decentralization while lowering blockchain latency and expense. A multi-objective blockchain-enabled framework is designed by incorporating private blockchain theory while simultaneously maintaining the abovementioned four purposes. This model is then solved using an updated Two Arch2 technique. The modified technology can significantly optimize for different indicators, according to the experiment results [16]. The

network architecture based on feature technology is currently viewed as essential for real-time surveillance and automation systems of power generation and transmission and developments in remote system connectivity technologies [17].

The most fundamental unit for digitalization and investment decisions is virtualization technology (VM). This same research on VM electricity monitoring is crucial to lowering network infrastructure electricity consumption [18]. PEC was an innovative approach to the IIoT, where SDN provided reduced delay operations or massive adaptive attempts to address the IIoT.[19]. The IoT has become highly prevalent and pervasive in people's lives recently. E-health, Home Automation, Industrial IoT, and Smart Farming are only some fields where devices with various functionalities are combined and used. Industrial IoT (IIoT) is gaining popularity across these areas because it allows users to connect externally and operate embedded sensors. The user only needs to get basic information generated by detecting gadgets during manufacturing. Furthermore, these data are usually transferred across an unprotected route, posing a data protection issue in the Industrial IoT[20]. Depending on the conditions, such compact systems include pre-processing techniques that validate, linearize, magnify, filter or correct the actual control voltage [21]. Sensor fusion can be used in IoT devices with several sensor units to provide resilience or a merged assessment of collecting data, such as in image processing applications [22].

Table 2. Indicative Differences Between IoT And IIoT in Selected Aspects

Elements of Interest	IoT	IIoT
Concentration	Personal information and valuables are safeguarded.	Production disruption mitigation and security
Principles	Transparency, reliability, and accessibility	Accessibility, Reliability, and Accountability
Consequences of Equipment Damage	There are no severe effects.	Operational disruption, influence on manufacturing, and possible physical risks
Response to a danger	Termination or cleanup may be necessary.	Operational service
Strategy Implementation or Installations	There are no notable causes of considerable disruptions in treatment time.	The installation must be arranged and completed in unavailability, which might cause the structure to be postponed for an extended period.
The computer's lifespan	Technology improvements occur on a somewhat regular basis.	Equipment with sturdy construction (over 15 years)
Implementation circumstances	Typical surroundings	a hostile atmosphere (temperature, vibration, etc.)

Table 3. Comparison of Survey papers

Citation	Fault Detection Setting	Objective
[2][13][50]	Automated detection for circuit boards	On the outer side level, address security holes, assaults, and effective remedies.
[16][8][49]	Missing syndromes due to fragmented repair logs	Explain identification and authentication systems and sheet safety issues and challenges.
[15][3][48]	Imbalanced data sets	Illustrate layer-by-layer risks, trust evaluation difficulties, modulation schemes, and BS metric-based analysis of significant system vulnerabilities.
[1][17][47]	Imbalanced data sets and concept drifts	A four-category classification of contemporary security issues is provided. Then, examine probable assaults that fit that criterion; In terms of process installations, talk about security problems.
[4][19][46]	Imbalanced data sets of semiconductor production	Describe telecommunication and internet protocols, levels of security challenges, and security products for each.
[45][6][22]	Wide range of data types	Sort security flaws into categories. Draw attention to problems, current remedies, and unsolved study objectives
[44][5][23]	Lack of prior knowledge and diagnosis experience, as well as the use of unsupervised learning	Evaluate traditional or innovative technological techniques for different IoT-related security mechanisms; evaluate the regulatory standards of six primary IoT systems.
[43][10]	Measured vibration data from wind generators are used.	Examine security problems such as privacy, faith, authentication, and remote access in a test case on industrial automation.

[53][8][21]	Machine spindle monitoring	Assess privacy concerns in the emerging Internet of Things; highlight critical obstacles.
[41][9][24]	Use of noisy mechanical data	Analyze IoT architecture, security concepts, and PETs; investigate the issue of data protection at each of these levels.
[7][40]	Bearing and fracture size assessment using observed with increasing signals	To evaluate the security problems of IoT systems, divide them into six categories.
[12][39]	Signal properties that evolve and prompt detection accuracy	Describe five manufacturing industries where IoT is being used and existing related research.
[38][6][25]	Failures in the gearbox of mechanical equipment	Examine crucial innovations and the labour that goes with them for the evolution of Manufacturing 4.0.
[37][11]	Automatic range adjustment of the CLR scheduler	Conduct surveys on the Digital Manufacturing concept.
[20][36]	An automotive assembly line's use of inter-spatiotemporal data	Explain significant features or obstacles involved in the development of BIoT implementations; identify major BIoT frameworks
[51][13]	Transmitter properties that change over time and early detection accuracy	Describe the advantages and drawbacks of incorporating blockchain solutions into IoT systems.
[34][21]	Machine spindle monitoring	Evaluate and compare the capabilities of numerous previous BIoT frameworks.
[52][23][33]	Bearing and defect thickness assessment using vibration acceleration indicators	Extend the current research to accommodate BIoT purposes via improving blockchain database systems and consensus algorithms.
[25][32]	Original signal signals from wind generators are used.	Examine the security needs for developing IoT or IIoT systems based on blockchains.
[29][31]	Lack of prior knowledge and analytical experience, as well as the use of unsupervised learning	Compare the benefits of specific blockchain-based IoT systems to the criteria; Examine the practicalities of incorporating blockchain into the Internet of Things.
[30][26]	Automatic range adjustment of the CLR scheduler	Create a five-category threat classification for blockchain IoT technologies; Compare and contrast safe blockchain approaches in security plans.
[28]	Lack of existing understanding and diagnosis knowledge, as well as the use of large datasets	Classify key IoT device risks via assault components and map them to one or more levels of the design; Examine defenses. Developments in IIoT safety studies are considered. Research project on IIoT implementations, focusing on security-related work; IoT and IIoT appropriately designed technologies built on the blockchain; Create a taxonomy of security research topics for IoT and IIoT; Discuss potential research topics.

6. Conclusion

This document highlights recent IIoT information security. Data confidentiality, security, CPS stability, key authentication for device coupling, and device administration emphasized existing problems and reviewed prior IoT security approaches and various sharing.

Because it differs in specifications and capabilities, IoT security methods must be updated or reinvented for IIoT applications.

It clearly examined the issues posed by the rising linkages among previously separated ICS devices and other connections and the corresponding solutions for the security problems unique to manufacturing technologies.

It still requires significant enhancements to fulfil the high expectations of IIoT vital infrastructure operations in terms of safety and high availability—Intelligence IoT-based solution for detecting or diagnosing faults in household equipment.

The technology can analyze the acquired data, detect errors, or inform the user of the circumstance.

To improve IIoT system security, examine the security considerations of different manufacturing platforms, consider relevant difficulties, and then build effective methods to safeguard its processes.

References

[1] Schneider, S, "The Industrial Internet of Things (IIoT) Applications and Taxonomy," *Internet of Things and Data Analytics Handbook*, pp. 41-81, 2017. *Crossref,* http://dx.doi.org/10.1002/9781119173601.ch3

[2] Xiaokang Wang et al., "ADTT: A Highly Efficient Distributed Tensor-Train Decomposition Method for IIoT Big Data," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1573-1582, 2021. *Crossref,* https://doi.org/10.1109/TII.2020.2967768

[3] Y. Wu, H. -N. Dai, and H. Wang, "Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2300-2317, 2021. *Crossref,* https://doi.org/10.1109/JIOT.2020.3025916

[4] Dingde Jiang et al., "An Energy-Efficient Networking Approach in Cloud Services for IIoT Networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 928-941, 2020. *Crossref,* https://doi.org/10.1109/JSAC.2020.2980919

[5] Saiyu Qi et al., "Efficient Data Access Control with Fine-Grained Data Protection in Cloud-Assisted IIoT," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2886-2899, 2021. *Crossref,* https://doi.org/10.1109/JIOT.2020.3020979

[6] Hu Xiong et al., "Heterogeneous Encryption with Equality Test for IIoT Environment," *IEEE Internet of Things Journal*, vol. 8, no. 21, 2021. *Crossref,* https://doi.org/10.1109/JIOT.2020.3008955

[7] Mohammad Mehedi Hassan et al., "An Adaptive Trust Boundary Protection for IIoT Networks Using the Deep-Learning Feature-Extraction-Based Semisupervised Model," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2860-2870, 2021. *Crossref,* https://doi.org/10.1109/TII.2020.3015026

[8] Tie Qiu et al., "Edge Computing in the Industrial Internet of Things: Architecture, Advances, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2462-2488, 2020. *Crossref,* https://doi.org/10.1109/COMST.2020.3009103

[9] Hu Xiong et al., "Efficient and Privacy-Preserving Authentication Protocol for Heterogeneous Systems in IIoT," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11713-11724, 2020. *Crossref,* https://doi.org/10.1109/JIOT.2020.2999510

[10] Koen Tange et al., "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489-2520, 2020. *Crossref,* https://doi.org/10.1109/COMST.2020.3011208

[11] Abuhasel, K. A., and Khan, M. A, "A Secure Industrial Internet of Things (IIoT) Framework for Resource Management in Intelligent Manufacturing," *IEEE Access*, vol. 8, pp. 117354-117364, 2020. *Crossref,* https://doi.org/10.1109/ACCESS.2020.3004711

[12] Abdullah Alsaedi et al., "TON_Iot Telemetry Dataset: A New Generation Dataset of IOT and IIoT for Data-Driven Intrusion Detection Systems," *IEEE Access*, vol. 8, pp. 165130-165150, 2020. *Crossref, Crossref,* https://doi.org/10.1109/ACCESS.2020.3022862

[13] Ewart W. Blackmore et al., "Terrestrial Muon Flux Measurement at Low Energies for Soft Error Studies," *IEEE Transactions on Nuclear Science*, vol. 62, no. 6, pp. 2792-2796, 2015. *Crossref,* https://doi.org/10.1109/TNS.2015.2498103

[14] Yunfei Song et al., "Fda3: Federated Defense Against Adversarial Attacks for Cloud-Based IIoT Applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, 2021, *Crossref,* https://doi.org/10.1109/TII.2020.3005969

[15] Hailing Zhou et al., "Recent Advances on Single Modal and Multimodal Face Recognition: A Survey," *IEEE Transactions on Human-Machine Systems*, vol. 44, no. 6, pp. 701-716, 2014. *Crossref,* http://dx.doi.org/10.1109/THMS.2014.2340578

[16] Bin Cao et al., "A Many-Objective Optimization Model of Industrial Internet of Things Based on Private Blockchain," *IEEE Network*, vol. 34, no. 5, pp. 78-83, 2020. *Crossref,* http://dx.doi.org/10.1109/THMS.2014.2340578

[17] Zhengwei Xu et al., "Adaptive DE Algorithm for Novel Energy Control Framework Based on Edge Computing in IIoT Applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5118-5127, 2021. *Crossref,* https://doi.org/10.1109/TII.2020.3007644

[18] Chonglin Gu, Hejiao Huang,, and Xiaohua Jia, "Power Metering for a Virtual Machine in Cloud Computing Challenges and Opportunities," *IEEE Access*, vol. 2, pp. 1106-1116, 2014. *Crossref,* https://doi.org/10.1109/ACCESS.2014.2358992

[19] Ying Gao et al., "Blockchain-Based IIoT Data Sharing Framework for SDN-Enabled Pervasive Edge Computing," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5041-5049, 2020. *Crossref,* https://doi.org/10.1109/TII.2020.3012508

[20] R. Vinoth et al., "Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3801-3811, 2021. *Crossref,* https://doi.org/10.1109/JIOT.2020.3024703

[21] Rongbo Zhu et al., "ERDT: Energy-Efficient Reliable Decision Transmission for Intelligent, Cooperative Spectrum Sensing in Industrial IoT," *IEEE Access*, vol. 3, pp. 2366-2378, 2015. *Crossref,* https://doi.org/10.1109/ACCESS.2015.2501644

[22] Sajid, A., Abbas, H., and Saleem, K, "Cloud-Assisted Iot-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," *IEEE Access*, vol. 4, pp. 1375-1384, 2016. *Crossref,* https://doi.org/10.1109/ACCESS.2016.2549047

[23] Saad Mubeen et al., "Delay Mitigation in Offloaded Cloud Controllers in Industrial IoT," *IEEE Access*, vol. 5, pp. 4418-4430, 2017. *Crossref,* https://doi.org/10.1109/ACCESS.2017.2682499

[24] Charbel El Kaed et al., "SRE: Semantic Rules Engine for the Industrial Internet-of-Things Gateways," *IEEE Transactions on Industrial Informatics*, vol.14, no. 2, pp. 715-724, 2017. *Crossref,* https://doi.org/10.48550/arXiv.1710.09627

[25] Delsing, J, "Local Cloud Internet of Things Automation: Technology and Business Model Features of Distributed Internet of Things Automation Solutions," *IEEE Industrial Electronics Magazine*, vol. 11, no. 4, pp. 8-21, 2017. *Crossref,* https://doi.org/10.1109/MIE.2017.2759342

[26] George, G, and Thampi, S. M, "A Graph-Based Security Framework for Securing Industrial IoT Networks From Vulnerability Exploitations," *IEEE Access*, vol. 6, pp. 43586-43601, 2018. *Crossref,* https://doi.org/10.1109/ACCESS.2018.2863244

[27] Neha Priya, "Cybersecurity Considerations for Industrial IoT in Critical Infrastructure Sector," *International Journal of Computer and Organization Trends*, vol. 12, no. 1, pp. 27-36, 2022. *Crossref,* https://doi.org/10.14445/22492593/IJCOT-V12I1P306

[28] Hansong Xu et al., "A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective," *IEEE Access*, vol. 6, pp. 78238-78259, 2018. *Crossref,* https://doi.org/10.1109/ACCESS.2018.2884906

[29] Chun-Cheng Lin et al., "Concept Drifts Detection and Adaption in Significant Imbalance Industrial IoT Data Using an Ensemble Learning Method of Offline Classifiers," *IEEE Access*, vol. 7, pp. 56198-56207, 2019. *Crossref,* https://doi.org/10.1109/ACCESS.2019.2912631

[30] Helin Yang et al., "Learning-Based Energy-Efficient Resource Management by Heterogeneous RF/VLC for Ultra-Reliable Low-Latency Industrial IoT Networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5565-5576, 2020. *Crossref,* https://doi.org/10.1109/TII.2019.2933867

[31] Francesca Meneghello et al., "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182-8201, 2019. *Crossref,* https://doi.org/10.1109/JIOT.2019.2935189

[32] Waheb A. Jabbar et al., "Design and Fabrication of Smart Home with the Internet of Things-Enabled Automation System," *IEEE Access*, vol. 7, pp. 144059-144074, 2019. *Crossref,* https://doi.org/10.1109/ACCESS.2019.2942846

[33] Tejasvi Alladi et al., "Blockchain Applications for Industry 4.0 and Industrial IoT: A Review," *IEEE Access*, vol. 7, pp. 176935-176951, 2019. *Crossref,* https://doi.org/10.1109/ACCESS.2019.2956748

[34] Aris S. Lalos et al., "Privacy Preservation in Industrial IoT Via Fast Adaptive Correlation Matrix Completion," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7765-7773, 2020. *Crossref,* https://doi.org/10.1109/TII.2019.2960275

[35] G.Vinobala, and M.Piramu, "Monitoring of Industrial Electrical Equipment Using IoT," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 1, pp. 13-18, 2021. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V8I1P103

[36] Xiaolong Lai et al., "Adaptive Resource Allocation Method Based on Deep Q Network for Industrial Internet of Things," *IEEE Access*, vol. 8, pp. 27426-27434, 2020. *Crossref,* https://doi.org/10.1109/ACCESS.2020.2971228

[37] Jaeyoung Hwang et al., "AUTOCON-IoT: Automated and Scalable Online Conformance Testing for IoT Applications," *IEEE Access*, vol. 8, pp. 43111-43121, 2020. *Crossref,* https://doi.org/10.1109/ACCESS.2020.2976718

[38] Mostafa Haghi et al., "A Flexible and Pervasive IoT-Based Healthcare Platform for Physiological and Environmental Parameters Monitoringm," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5628-5647, 2020. *Crossref,* https://doi.org/10.1109/JIOT.2020.2980432

[39] Massimo Ballerini et al., "NB-IoT Versus Lorawan: An Experimental Evaluation for Industrial Applications," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7802-7811, 2020. *Crossref,* https://doi.org/10.1109/TII.2020.2987423

[40] Lei Xu et al., "Fairness-Aware Throughput Maximization Over Cognitive Heterogeneous NOMA Networks for Industrial Cognitive IoT," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4723-4733, 2020. *Crossref,* https://doi.org/10.1109/TCOMM.2020.2992720

[41] Teklay Gebremichael et al., "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges," *IEEE Access*, vol. 8, pp. 152351-152366, 2020. *Crossref,* https://doi.org/10.1109/ACCESS.2020.3016937

[42] Jaiganesh P M, and DR. B.Meenakshi Sundaram, "IoT Based Power Monitoring System," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 4, pp. 4-7, 2021. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V8I4P102

[43] Abdullah Alsaedi et al., "TON_Iot Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," *IEEE Access*, vol. 8, pp. 165130-165150, 2020. *Crossref,* https://doi.org/10.1109/ACCESS.2020.3022862

[44] Md Liton Hossain et al., "Industrial IoT-Based Condition Monitoring for Wind Energy Conversion System," *CSEE Journal of Power and Energy Systems*, vol. 7, no. 3, pp. 654-664, 2020. *Crossref,* https://doi.org/10.17775/CSEEJPES.2020.00680

[45] Usman Tariq et al., "Context-Aware Autonomous Security Assertion for Industrial IoT," *IEEE Access*, vol. 8, pp. 191785-191794, 2020. *Crossref,* https://doi.org/10.1109/ACCESS.2020.3032436

[46] Anmin Fu et al., "VFL: A Verifiable Federated Learning with Privacy-Preserving for Big Data in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 5, pp. 3316 – 3326, 2022. *Crossref,* https://doi.org/10.1109/TII.2020.3036166

[47] Xiaoding Wang et al., "Enabling Secure Authentication in Industrial IoT with Transfer Learning Empowered Blockchain," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7725-7733, 2021. *Crossref,* https://doi.org/10.1109/TII.2021.3049405

[48] Y. Njah, and M. Cheriet, "Parallel Route Optimization and Service Assurance in Energy-Efficient Software-Defined Industrial IoT Networks," *IEEE Access*, vol. 9, pp. 24682-24696, 2021. *Crossref,* https://doi.org/10.1109/ACCESS.2021.3056931

[49] Yuming Feng et al., "A Consortium Blockchain-Based Access Control Framework with Dynamic Orderer Node Selection for 5G-Enabled Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, 2021. *Crossref,* https://doi.org/10.1109/TII.2021.3078183

[50] Nteziriza Nkerabahizi Josbert et al., "A Framework for Managing Dynamic Routing in Industrial Networks Driven by Software-Defined Networking Technology," *IEEE Access*, vol. 9, pp. 74343-74359, 2021. *Crossref,* https://doi.org/10.1109/ACCESS.2021.3079896

[51] Iqra Qasim et al., "A Model-Driven Mobile HMI Framework (MMHF) for Industrial Control Systems," *IEEE Access*, vol. 8, pp. 10827-10846, 2020. *Crossref,* https://doi.org/10.1109/ACCESS.2020.2965259

[52] Mostafa Uddin et al., "SDN-Based Multi-Protocol Edge Switching for IoT Service Automation," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 12, pp. 2775-2786, 2018. *Crossref,* https://doi.org/10.1109/JSAC.2018.2871325

[53] Tanesh Kumar et al., "Blockedge: Blockchain-Edge Framework for Industrial IoT Networks," *IEEE Access*, vol. 8, pp. 154166-154185, 2020. *Crossref,* https://doi.org/10.1109/ACCESS.2020.3017891