Indiana Journal of Multidisciplinary Research
Abbreviated Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.21567512

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Research Article

Volume-06|Issue-04|2026

Industrial Internet of Things (IIoT) Security: A Survey on Integrated Intrusion Detection and Cryptographic Approaches

Anil Kumar K N[1] and Dr. Siddartha B K[2]

[1]Research Scholar, Department of Computer Science and Engineering BGS Institute of Technology, Adichunchanagiri University, BG Nagara, Karnataka, India
[2]Professor & Head, Department of Information Science and Engineering, BGS Institute of Technology, Adichunchanagiri University, BG Nagara, Karnataka, India

Article History
Received: 05.05.2026
Accepted: 22.06.2026
Published: 25.07.2026

Citation
Kumar, A. K. N. & Siddartha, B. K. (2026). Industrial Internet of Things (IIoT) Security: A Survey on Integrated Intrusion Detection and Cryptographic Approaches. *Indiana Journal of Multidisciplinary Research, 6*(4), 129-137.

Abstract: The Industrial Internet of Things (IIoT) is revolutionizing industrial automation by integrating intelligent devices, advanced analytics, and decentralized control into manufacturing and critical infrastructure systems. However, the increased interconnectivity and heterogeneity of IIoT environments introduce significant security vulnerabilities, necessitating robust protective mechanisms. This survey presents a comprehensive review of recent advances in IIoT security, with a dual focus on intrusion detection systems (IDS) and cryptographic techniques. It examines the limitations of traditional IDS approaches in detecting novel threats and highlights the growing role of machine learning and deep learning models in adaptive threat detection. Concurrently, the paper explores lightweight cryptographic frameworks that address the resource constraints of IIoT deployments while ensuring confidentiality, integrity, and authentication. The integration of these two domains—detection and protection—is emphasized as a promising pathway toward resilient IIoT security architectures. By analyzing existing testbeds, experimental frameworks, and real-world applications, this survey identifies key research gaps, emerging trends, and future directions for developing scalable, secure, and intelligent IIoT systems.

Keywords: IIoT Security, Intrusion Detection Systems, Lightweight Cryptography, Machine Learning, Resilient Security Architectures

INTRODUCTION

The Internet of Things (IoT) is a way of using smart gadgets that can talk to each other via the internet. IoT settings are made up of a lot of smart devices that can send, receive, analyze, and gather data from each other. These smart gadgets that are all connected to each other allow us to keep an eye on any environment and regulate any setting with great accuracy. By 2025, the entire economic effect of IoT technology is expected to be $11.1 trillion per year [1]. Most of the IoT systems that have been made thus far are for consumers, but this has made it possible for the technology to be used in numerous industrial settings, giving rise to what is known as IIoT technology [2]. The industrial internet, or IIoT, is a way of using smart devices that are connected to each other in an industrial setting to connect industrial parts like actuators, sensors, controllers, and intelligent control systems. This is done for data analysis and process optimization to speed up execution, cut costs, and manage the industrial environment in real time [3].

Some people call the Internet of Things (IoT) "the infrastructure of the information society." IoT is the set of technologies that connect physical things to computers and networks. It makes sense that IoT technology have been used in a number of diverse fields, including healthcare, the military, and industrial automation. This article is about Industrial IoT (IIoT), which is the use of IoT technology in industrial automation settings such enhanced process automation and factory automation [4]. IIoT systems are usually used in tough and complicated settings, unlike IoT systems made for consumer use. They also have strict requirements for reliability, timing performance (like latency and jitter), energy efficiency, and security to improve manufacturing quality and productivity and avoid potentially disastrous outcomes. A newer trend in sophisticated industrial automation is to use IIoT technology to connect factories that depend on each other. This makes it possible to offer decentralized, collaborative, and often unchangeable and verifiable services, such distributed supply chain management [5].

These special needs for IIoT systems make it hard to build the communication fabric, manage and analyze data, make decisions, and keep both the communication and data infrastructure safe.

To fulfil the strict performance standards of IIoT solutions, it is essential to come up with new ways to manage resources, make decisions and analyze data, and secure security. But to make sure these methods are proper and see how well they work, they need a full testing infrastructure. Researchers usually use a controlled experimental setting called a testbed to do

***Corresponding Author:** Anil Kumar K N

well-defined experiments, test new technologies, see how well systems work, and make sure solutions work before they are used in the real world. For IIoT, testbeds can be physical setups that contain a network of sensors, actuators, and devices that are all connected to each other to make an industrial ecosystem [6]. Physical testbeds are very realistic and closely resemble real-world IIoT situations and problems. But it may be expensive and hard to set up and keep up with physical testbeds, especially when they are used on a wide scale. Another option is to use virtual or cloud-based testbeds to test IIoT systems with simulations. This cuts costs and makes the solutions more flexible and scalable. There may also be hybrid testbeds, which are a mix of physical and virtual testbeds. These testbeds create a flexible and adaptive environment that combines actual hardware with virtual components [7].

The Internet of Things (IoT) is a technology that makes it easier for objects to talk to each other and share data via the Internet. It means connecting common gadgets to the Internet so they can talk to one other and share data easily. The Industrial Internet of Things (IIoT) builds on this basis and brings similar features to the industrial sector. It improves production processes, increases productivity, and makes sophisticated analytics possible by connecting smart sensors and machines. Smart devices and sensors are used in IIoT to gather information from industrial equipment and processes. This information is then evaluated to improve operations, forecast when repair will be needed, and cut down on downtime. Sadly, many industrial machines are not built with current security features because the focus is on having them work well and last a long time, which makes them quite easy to break into. Also, the openness of IoT design makes this problem worse, which raises big security issues in the IIoT. Recently, using machine learning and deep learning-based intrusion detection technologies on IIoT has helped fix security problems that were already there. First, intrusion detection systems (IDSs) keep an eye on and evaluate what devices are doing to find possible security holes. When an assault on a device is found, steps may be done right once to lessen the threat and keep the system safe. Second, IDSs keep an eye on things all the time and find threats in real time, which makes industrial networks safer and more resilient overall. However, a major flaw in existing IIoT-oriented IDSs is that they assume that all forms of threats that are tested also show up in the training set [8]. This assumption doesn't work for IIoT, which is always changing and where new attacks are likely to happen in an open environment. Also, standard classifiers don't do a good job of finding assaults that have never been seen before, and they often misclassify them as known attack types, which makes the rate of erroneous classifications go up. This constraint makes IDSs less useful in open IIoT systems, where being able to find new threats is very important. Because of this, it is very vital to use identification models that can move from closed to open IIoT settings. These models can find unknown threats more accurately.

Researchers may analyze the strengths and shortcomings of different IIoT testbeds and see how well they function in a full study. This comparison helps people learn about the best ways to construct IIoT testbeds and the problems that come up when they do. A detailed literature review may also be a useful tool for teaching students and professionals about IIoT testbeds, why they are important, and what role they play in IIoT research and development. It's important to remember that the term "IIoT" covers a lot of different uses and situations. This article, on the other hand, is mostly about the connection part of IIoT testbeds, which includes all the parts that make data transfer and networking possible in the systems that have been set up. This encompasses things like transmission devices, communication protocols, network designs, and resource management [9]. The Industrial Internet of Things (IIoT) has made factories much more efficient by connecting sensors, actuators, and smart devices. But increased interconnectedness also opens up serious security holes that put the integrity, privacy, and availability of data and systems at risk. As IIoT settings increase, they are more likely to be hit by cyberattacks like SQL injection, illegal access, and data breaches. These assaults can stop operations and put critical information at risk. Existing security measures frequently don't do a good job of protecting against the wide range of IIoT threats that are always changing. Many old intrusion detection systems can't find application-level assaults like SQL injection or aren't flexible enough to respond to new threats right away. Also, most cryptographic methods used to make sure data is safe are quite resource-intensive, thus they don't work well on IIoT devices that don't have a lot of power. Also, many existing authentication methods use only one factor, which isn't enough to keep communication safe across scattered IIoT networks. Because of this, there is a strong demand for a full and light security architecture that is made to deal with the specific problems of IIoT [10].

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

***Corresponding Author:** Anil Kumar K N

approaches are inefficient and incapable of handling the capacity constraints of large-scale IIoT big data [11].

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 [12].

Industrial IoT (IIoT), the focus of this article, is the application of IoT technologies in industrial automation environments, including advanced process automation and factory automation. Compared with IoT systems designed for consumer applications, IIoT systems are usually deployed in harsh and complex environments, and have stringent dependability, timing performance (e.g., latency and jitter), energy-efficiency and security requirements to optimize manufacturing quality and productivity, and to avoid potentially catastrophic consequences. A more recent trend in advanced industrial automation is to connect interdependent factories together through IIoT technologies to provide decentralized, collaborative and sometimes immutable and verifiable services (e.g., distributed supply chain management). These unique requirements on IIoT systems pose many challenges in their communication fabric design, distributed data management, analysis and decision making, and security protection for both the communication and data infrastructure [13].

The Industrial Internet of Things (IIoT) represents a transformative evolution of traditional industrial systems, integrating intelligent sensors, actuators, and data analytics platforms to optimize operational efficiency, enhance automation, and enable predictive maintenance. By embedding interconnected smart devices within industrial environments, IIoT systems facilitate real-time monitoring, decentralized control, and advanced decision-making processes across sectors such as manufacturing, energy, and logistics [14].

Despite these advancements, the increased connectivity and heterogeneity inherent to IIoT introduce significant security vulnerabilities. Unlike consumer-oriented IoT applications, industrial systems often operate in mission-critical and safety-sensitive environments, where a successful cyberattack can result in severe financial losses, compromised safety, and operational disruptions. These concerns are exacerbated by the extended lifespan of industrial equipment, much of which lacks built-in security mechanisms, and the open nature of network architectures that are prone to exploitation [15].

Challenges

To mitigate these risks, two fundamental areas of research have emerged at the forefront of IIoT security: **attack detection** and **cryptographic protection**. Intrusion Detection Systems (IDSs), particularly those powered by machine learning and deep learning algorithms, are being increasingly deployed to identify anomalous behaviors and previously unseen threats within industrial networks. However, conventional IDS models often assume that all types of attacks encountered during testing were also present during training—a flawed assumption in dynamic IIoT environments. This limits their ability to detect novel threats and increases false positive rates, ultimately undermining their reliability.

Complementing detection mechanisms, cryptographic techniques offer foundational security guarantees such as confidentiality, integrity, and authentication. Yet, traditional cryptographic schemes may not scale well in resource-constrained IIoT settings, where real-time performance and energy efficiency are critical. Therefore, integrating lightweight cryptographic protocols and advanced access control strategies—such as attribute-based encryption (ABE)—has become vital to secure communication and data exchange within IIoT infrastructures.

This survey explores the integration of attack detection methodologies and cryptographic solutions in IIoT, providing a comprehensive review of existing frameworks, highlighting their strengths and limitations, and identifying emerging trends and open research challenges. In particular, it emphasizes the need for hybrid approaches that can synergistically combine anomaly detection and adaptive encryption to address evolving threats while maintaining system performance and reliability.

Scalability and Heterogeneity of IIoT Networks: IIoT infrastructures consist of diverse devices with varying computing capabilities, communication protocols, and operational requirements. This heterogeneity complicates the design of unified security solutions. Moreover, as networks scale, maintaining consistent performance and ensuring synchronized security updates across distributed nodes becomes increasingly difficult.

Detection of Unknown and Zero-Day Attacks: Many existing intrusion detection systems (IDSs) rely on supervised learning models that are trained on labeled

***Corresponding Author:** Anil Kumar K N

datasets. However, these models struggle to detect zero-day attacks or anomalies not present in the training data. This limitation is particularly critical in IIoT environments where new threats can emerge rapidly.

Resource Constraints in Edge Devices: IIoT nodes often operate under strict limitations in terms of power, processing capacity, and memory. Conventional cryptographic techniques and deep learning models are frequently too resource-intensive to be deployed on such constrained devices, leading to a need for lightweight and optimized security algorithms.

Latency-Sensitive Decision Making: Real-time process control in industrial settings requires rapid detection and mitigation of security breaches. High-latency IDSs or encryption schemes can delay critical responses, potentially leading to operational disruptions or safety hazards.

Secure and Efficient Communication: Ensuring the confidentiality and integrity of data exchanged among IIoT nodes is vital. However, the use of heavy cryptographic mechanisms can introduce communication overhead and reduce throughput. Balancing security with communication efficiency is a persistent challenge.

Lack of Standardized Testbeds and Datasets: Benchmarking the performance of security mechanisms in IIoT remains difficult due to the absence of standardized testbeds and realistic datasets. Most existing datasets are either synthetic or limited in scope, reducing the generalizability of trained models.

Interoperability with Legacy Systems: Many industrial environments still rely on legacy equipment lacking built-in security features. Integrating modern security frameworks with such systems requires adaptive and backward-compatible approaches that do not disrupt operations.

Decentralized and Federated Learning Challenges: While federated learning is promising for privacy-preserving intrusion detection, it introduces its own challenges, including model convergence, communication overhead, and vulnerability to poisoning attacks in decentralized environments.

Dynamic and Evolving Threat Landscape: The threat environment in IIoT is continuously evolving, requiring adaptive security systems that can learn from new patterns and autonomously update their defense strategies without manual intervention.

Privacy Preservation and Compliance: With increasing regulatory requirements on data privacy (e.g., GDPR), IIoT systems must not only be secure but also privacy-compliant. Designing IDS and cryptographic protocols that process minimal data while ensuring accountability is both necessary and difficult.

Motivation and contribution

The quick adoption of Industrial Internet of Things (IIoT) technology has changed industrial automation by making it possible for devices, systems, and activities to connect to each other without any problems. But this increasing interconnectedness also makes important infrastructures more vulnerable to a wide range of cyber assaults. Traditional security measures were made for static, isolated environments; therefore they don't always work well in IIoT ecosystems, which are dynamic, distributed, and data-heavy. Also, even while intrusion detection and cryptography approaches have both showed potential on their own, they can't protect IIoT systems well enough from complex, changing threats when used alone. This makes it necessary to look at integrated methods that combine smart attack detection with strong cryptographic defenses. To fill in the gaps in our present knowledge, evaluate how well current solutions perform, and point future research in the direction of constructing durable, scalable, and secure IIoT frameworks, it is important to undertake a full study of these methods.

- **Comprehensive Review**: This survey provides a detailed analysis of recent advancements in attack detection and cryptographic techniques specifically tailored for IIoT systems, covering both traditional and AI-driven approaches.
- **Integrated Perspective**: It highlights the need for synergistic integration of intrusion detection systems (IDS) and lightweight cryptographic methods, offering insights into their combined effectiveness in addressing IIoT-specific security challenges.
- **Research Directions**: The paper identifies key limitations in current solutions and outlines open research challenges, serving as a roadmap for future work aimed at enhancing the security and resilience of IIoT infrastructures.

Related work

[16] looked at the problems and research questions that come up while managing data in I-IoT. They also did a case study on a big petrochemical facility. Also, they used auction-based methods to solve the problem of allocating computing resources, while [17] dealt with the trust difficulties that come up when allocating resources. Also, some study has used new communication tools like 5G and software-defined networking (SDN) for I-IoT [19], [20].

[21] created a system for intrusion detection in Industrial IoT contexts that uses federated learning and blockchain together. Their method spreads model training among edge devices, and blockchain immutability makes sure that the data stays safe. The solution had a high detection rate and a lot less communication overhead, which

***Corresponding Author:** Anil Kumar K N

solved the problems of privacy and scalability in IIoT networks. This experiment also revealed that the system was better able to handle poisoning attempts and collusion among nodes, which made people more confident in collaborative detection. The evaluation was done using standard datasets and real-life IIoT situations.

[22] built a security module for IIoT devices that uses Physical Unclonable Functions (PUFs) and hybrid cryptographic methods. Their technology, which is built on FPGA platforms, stops cloning and illegal access to important data from sensors and actuators. Lightweight cryptography makes sure that the software works with IIoT hardware that doesn't have a lot of resources. Tests showed that the module was safe from common risks including replay attacks and man-in-the-middle assaults. This strategy works especially well for older systems that require protection added on.

[23] came up with a hybrid security architecture for SDN-enabled IIoT networks that combines blockchain support with deep learning-based intrusion detection. Their convolutional neural network (CNN) model finds dangers in real time, and blockchain keeps a record of network transactions that can't be changed. This two-layer protection lowers the dangers of things like changing rules and changing the flow. The framework worked well on the CICIDS dataset and worked in a simulated manufacturing network.

[24] showed how to use combinational neural networks to build a federated transfer learning system that makes it easier to find intrusions in IIoT settings. The system keeps data private between nodes that are spread out over a large area by only exchanging model parameters. The method cuts down on the requirement for a lot of local data and can handle new sorts of attacks through transfer learning. The technique was more accurate and had less latency than centralized models on a range of IIoT testbeds. It looks like it may be useful for finding threats in large industrial networks throughout the world.

[25] did a research comparing several machine learning classifiers to see which ones were best at finding cyberattacks in IIoT networks that operate with huge data. They used real-world datasets to evaluate algorithms like SVM, Random Forest, and XGBoost and found that they were able to predict known attack patterns with over 99% accuracy. The study showed how feature engineering and class balance may affect how well a model works. It also stressed how important it is for edge-based deployment to be computationally efficient. The results give us a starting point for choosing models for IIoT infiltration scenarios.

Using the TON_IoT dataset, which shows how things really are in industrial settings, [26] created an intrusion detection system just for IIoT networks. Their technology uses ensemble learning methods to find and categorize different types of attacks, such as DoS and data injection. The framework was able to find things with a high degree of accuracy and a low number of false positives, making it useful in changing IIoT situations. Their work also focused on choosing the right features and how important new datasets are for making models that operate in a variety of situations. The suggested IDS was light enough to be used at the edge, which made it responsive in real time.

[27] did a thorough review of IIoT security concerns and how to protect against them, with an emphasis on edge computing and artificial intelligence. The study put possible threats into groups and found AI-driven remedies for each group. It showed how edge devices may help lower latency and make decisions more accurately. One suggestion was to combine machine learning with security models that are aware of their surroundings. This survey gives researchers a starting point for improving IIoT security designs.

[28] created AIMS, a machine learning-based intrusion detection system that helps protect smart grids against Routing Protocol for Low-Power and Lossy Networks (RPL) attacks. The system uses a stacked ensemble model and a lightweight blockchain to work safely and use less energy. AIMS had better detection rates for rank, wormhole, and Sybil attacks while keeping the computational cost low. Their use of IDS with cryptographic chaining makes sure that logs can't be changed. This mixed method makes power-sensitive IIoT systems more reliable.

Using permissioned blockchain, Arbiter PUFs, and the Elliptic Curve Digital Signature Algorithm (ECDSA), [29] built a safe architecture for smart cities. Their design allows for collaborative anomaly detection while also making sure that identity verification and access restriction are solid. The system does a good job of preventing data tampering and distributed denial-of-service (DDoS) assaults. The simulation results revealed that it had a high throughput and a low latency, which makes it good for real-time IoT situations in cities. This paradigm connects the security of physical devices with cloud analytics that can grow.

[30] suggested an IDS for cyber-physical systems that use fog with Enhanced Chicken Swarm Optimization (ECSO) and recurrent neural networks. Their feature selection method makes categorization more accurate while making the model less complicated. The system was able to detect attacks with more than 99% accuracy on benchmark datasets, suggesting that it can handle new threats. It is made for processing on fog nodes in real time and can work with minimal latency. Their architecture makes sure that it can grow to fit industrial uses with different types of devices.

[31] came up with a hybrid security architecture that uses Software-Defined Networking (SDN) and blockchain to protect IIoT systems against assaults on the control

***Corresponding Author:** Anil Kumar K N

plane. They used Random Subspace Learning with k-Nearest Neighbors (KNN) to find intrusions and added a blockchain-based layer to check for integrity. This two-pronged strategy makes sure that threats are always being dealt with and events are always being logged. The model was quite good at finding things in simulated industrial settings, especially when it came to finding malicious command injections. It shows how SDN programmability and blockchain transparency can work together in the IIoT.

[32]. built an AI-based intrusion detection system to stop False Data Injection (FDI) assaults in smart grid settings. Their technique employs temporal deep learning to find small changes in how energy is used. The model worked quite well on a genuine low-voltage distribution system and didn't take up much processing power. Their method makes industrial energy management systems more reliable. The study shows how important it is to undertake domain-specific feature engineering to make AI-based IDS work better.

[33] came up with Federated-Simple Recurrent Units (Federated-SRUs), an IDS that protects privacy and is designed for Industrial Control Systems in IIoT. Their solution makes it possible to study together safely without exchanging data in one place, which keeps important process information safe. The SRU-based model was better at finding real-time anomalies than regular RNNs. The lightweight design makes it possible to use on small industrial machines. The paper talks about both how accurate detection is and how well it follows the rules in places where data is sensitive.

[34] created a decentralized IDS for big IIoT networks that uses Multi-Agent Reinforcement Learning. Each agent changes to fit the parameters of the local network and works with other agents to find coordinated strikes. The system was able to work with the NSL-KDD dataset with more than 97% accuracy and was able to keep working even when nodes failed. It can handle massive data without any centralized bottlenecks, which makes it scalable. This decentralized learning technique is very useful for connecting factories to each other.

[35] showed DeepLG SecNet, a layered deep learning architecture that uses LSTM and Gated Secure Networks to protect IIoT systems from cyberattacks. The framework has an optimization module that tweaks model parameters to make it better at finding intrusions. DeepLG SecNet was more than 98% accurate on several datasets, such as NSL-KDD and BoT-IoT. Its modular architecture lets it work with existing industrial systems without any problems. The system is set up to work best at both finding things and doing calculations quickly.

[36] looked at how to combine edge computing with IIoT security. It focused on making lightweight, ECC-based mutual authentication protocols. These protocols make guarantee that machine-to-machine (M2M) communication is safe and are intended for edge nodes with minimal resources. The suggested approach is safe against popular cyberattacks like impersonation and replay. Formal and experimental tests back up its efficacy. This study further forward safe real-time cooperation in industrial edge-cloud ecosystems, which is becoming more important for applications that need to be done quickly. Another recent paper looked at cybersecurity threats and responses in IIoT, focusing on how to find anomalies.

[37] It used AI to sort common attack vectors into groups and connect them to current ways to stop them. The authors pointed out some important outstanding questions, such as how to make systems more resistant to attacks, how to make datasets more reliable, and how to limit real-time detection. The evaluation encourages the use of adaptive anomaly detection systems that change when new threat patterns appear. It also advises that benchmark datasets should be standardized to make it easier to compare models.

[38] suggested a deep learning-based intrusion detection system that uses convolutional neural networks (CNNs) to find geographical relationships in IIoT traffic data. The algorithm was able to generalize well across different sorts of assaults, especially when it came to finding behaviors that had never been observed before. Compared to typical classifiers, it cut down on false positives by a large amount. The model was tested on the TON_IoT and BoT-IoT datasets, and it showed a lot of promise for use in many types of industrial settings.

[39] published a comprehensive analysis of the literature that looked at improvements in AI-driven IDS, with an emphasis on training efficiency and easy implementation. The review looked at how model pruning, quantization, and federated learning affected the speed and accuracy of detection. It came to the conclusion that hybrid training-deployment methodologies are necessary for scalability in the real world. The study also talked about how important cryptographic primitives are for keeping model communication and update propagation safe in federated environments. A study in [40] suggested an ensemble AI-based way to find coordinated and covert intrusions in IIoT systems. The hybrid model got more than 99% accuracy on complicated, unbalanced datasets by using decision trees, support vector machines, and deep learning. The system is meant to be used in industrial plants that are spread out and include a lot of different types of equipment. This study adds to proactive threat response systems in industrial automation by making systems more resilient through smart detection.

***Corresponding Author:** Anil Kumar K N

Ref	Method	Advantages	Disadvantages	Research Gap
[21]	Federated learning + blockchain for IDS	Preserves privacy, reduces communication overhead, resists poisoning	High complexity in coordination and training	Scalability in real-time federated deployment
[22]	PUF-based hardware security with lightweight cryptography	Resists cloning, low overhead, suitable for legacy systems	Hardware dependency, limited generalizability	Integration with AI-based detection systems
[23]	CNN-based IDS + blockchain on SDN	Real-time detection, immutable audit trail	High resource requirements, SDN integration complexity	Generalization to diverse IIoT network topologies
[24]	Federated transfer learning with combination neural networks	Privacy-preserving, adapts to unseen attacks	Requires careful parameter tuning	Performance under adversarial data distribution
[25]	Comparative study of ML classifiers	High accuracy (>99%) on known threats	Limited to static datasets, not real-time	Real-time deployment under constrained hardware
[26]	Ensemble learning on TON-IoT for IDS	Low false positives, robust to diverse attacks	Feature engineering dependent	Dataset bias and lack of transferability
[27]	AI-driven edge-based security analysis	Threat categorization, latency reduction	Edge resource limitations	Joint edge-cloud cooperative detection
[28]	Ensemble IDS + lightweight blockchain (AIMS)	Energy-efficient, high detection of RPL attacks	Limited to smart grids	Generalization to broader IIoT domains
[29]	ECDSA + Arbiter PUF + permissioned blockchain	Strong identity/authentication, high throughput	High initial configuration cost	Interoperability with standard IIoT protocols
[32]	Temporal DL for False Data Injection detection	Domain-specific optimization, low overhead	Limited to smart grid	Portability across industrial verticals
[33]	Federated-SRU IDS for ICS	Real-time, low-latency, privacy-preserving	Complex synchronization	Resource-aware federated security design
[34]	Multi-agent RL-based decentralized IDS	Scalable, fault-tolerant, adapts locally	Complex training, potential convergence issues	Cross-agent coordination optimization
[35]	DeepLG, SecNet: LSTM + Gated Secure Network	Modular, >98% accuracy, fast inference	High memory cost during training	Support for real-time adaptive intrusion scenarios

RESEARCH GAP

1. **Inadequate Detection of Unknown and Zero-Day Threats**: Most existing IDS models are trained on static datasets and assume that all attack types are known during training. This limits their ability to detect novel or zero-day attacks in dynamic IIoT environments, where threat signatures evolve rapidly.
2. **Lack of Integration Between Detection and Protection Mechanisms**: Intrusion detection and cryptographic mechanisms are often developed independently. Few solutions combine adaptive IDS with lightweight encryption in a cohesive framework, leaving systems vulnerable at the interface between detection and response.
3. **Limited Support for Resource-Constrained Devices**: Many proposed security solutions do not adequately consider the computational and energy limitations of IIoT edge devices. This restricts the applicability of deep learning models and standard encryption protocols in real-world industrial environments.
4. **Absence of Standardized and Realistic Benchmark Datasets**: The evaluation of IDS performance is hindered by the lack of comprehensive and standardized IIoT datasets that reflect real-world traffic, attack scenarios, and device heterogeneity. This impedes reproducibility and comparative assessment.
5. **Insufficient Exploration of Federated and Decentralized Learning in IIoT**: While federated learning offers privacy-preserving benefits, challenges such as convergence efficiency, communication overhead, and robustness against

***Corresponding Author:** Anil Kumar K N

adversarial poisoning in IIoT contexts remain underexplored.

6. **Scalability and Interoperability in Large-Scale Industrial Networks**: Current solutions often fail to scale across complex IIoT ecosystems with heterogeneous devices and legacy infrastructure. Research is needed on scalable architectures that can ensure interoperability and real-time synchronization.
7. **Lack of Context-Aware and Adaptive Security Frameworks**: Current IIoT security mechanisms often lack the ability to dynamically adjust their operations based on contextual factors such as device behavior, operational state, network conditions, or threat intelligence. Developing adaptive, context-aware security frameworks is essential for achieving real-time resilience against sophisticated and evolving cyber threats in industrial environments.

CONCLUSION

The rapid evolution of the Industrial Internet of Things (IIoT) has brought significant advancements in industrial automation, enabling real-time data exchange, intelligent control, and predictive maintenance. However, this progress has also introduced a complex landscape of cybersecurity challenges due to the open, heterogeneous, and resource-constrained nature of IIoT environments. This survey reviewed recent developments in two primary domains of IIoT security: intrusion detection systems (IDS) and cryptographic mechanisms. Our analysis underscores that while machine learning and deep learning-based IDS frameworks offer promising capabilities in identifying anomalies and previously unseen attacks, their effectiveness is limited by static training datasets and high false positive rates. Similarly, although traditional cryptographic solutions provide strong security guarantees, they often fall short in IIoT settings due to computational overhead and lack of scalability. To address these limitations, integrated approaches that combine adaptive intrusion detection with lightweight, context-aware cryptographic protocols are essential. Hybrid testbeds and federated learning architectures also emerge as key enablers for evaluating and deploying such solutions in realistic industrial scenarios. Future research should focus on building resilient, low-latency, and privacy-preserving security frameworks that can dynamically adapt to evolving threats. Standardized benchmarking datasets, real-time evaluation platforms, and interdisciplinary collaboration will be critical for advancing the state-of-the-art in IIoT security. Ultimately, the convergence of intelligent detection and efficient protection mechanisms will be pivotal in securing next-generation industrial systems and fostering trust in connected manufacturing infrastructures.

REFERENCES

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
3. Zhou, K., Liu, T., & Zhou, L. (2015). *Industry 4.0: Towards future industrial opportunities and challenges*. In *Proceedings of the 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*.
4. Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.
5. McKinsey Global Institute. (2015). *The Internet of Things: Mapping the value beyond the hype*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
6. Industrial Internet Consortium. (2017). *Industrial Internet Reference Architecture*.
7. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431–440.
8. Lu, Y., & Xu, X. (2019). Resource virtualization and service selection in manufacturing cloud. *Journal of Manufacturing Systems, 43*, 310–318.
9. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646.
10. Ray, P. P. (2016). A survey on Internet of Things architectures. *Journal of King Saud University – Computer and Information Sciences*.
11. Cheng, J., Chen, W., Tao, F., & Lin, C. L. (2018). Industrial IoT in 5G environment towards smart manufacturing. *Journal of Industrial Information Integration, 10*, 10–19.
12. Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of IoT. *International Journal of Computer Applications, 111*(7), 1–6.
13. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks, 57*(10), 2266–2279.
14. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in the Internet of Things. *IEEE Internet of Things Journal, 4*(5), 1250–1258.
15. Wang, Y., & Jones, K. (2019). IoT-based testbed for industrial control system cybersecurity research. *Journal of Information Security and Applications, 45*, 102–112.
16. Poorazad, H., et al. (2022). A hybrid deep learning and blockchain-based architecture for secure IIoT communication. *IEEE Access, 10*, 23812–23825.

***Corresponding Author:** Anil Kumar K N

17. Amael, et al. (2021). Securing Industrial IoT with PUFs and lightweight cryptography on FPGA platforms. *Microprocessors and Microsystems, 82*.
18. Alotaibi, M. (2022). Edge-AI driven security for IIoT: A review. *Journal of Information Security and Applications, 65*, 103135.
19. Rajesh, S., et al. (2022). Federated transfer learning with combinational neural networks for IIoT intrusion detection. *IEEE Transactions on Industrial Informatics, 18*(3), 2015–2026.
20. Alshathri, K., et al. (2021). Ensemble-based IDS for Industrial IoT using the TON_IoT dataset. *Future Generation Computer Systems, 115*, 322–336.
21. Savitha, T., & Basarkod, G. (2021). AIMS: Energy-efficient machine learning-based intrusion detection system for RPL attacks in smart grids. *Sustainable Computing: Informatics and Systems, 30*.
22. Babu, M., et al. (2021). Secure smart city architecture using Arbiter PUFs, ECDSA, and permissioned blockchain. *Sensors, 21*(9).
23. Derhab, R., et al. (2021). A hybrid SDN and blockchain architecture for IIoT security. *Computer Networks, 198*.
24. Radoglou-Grammatikis, D., et al. (2021). AI-enabled detection of false data injection attacks in smart grids. *Electric Power Systems Research, 189*.
25. Khan, et al. (2022). Federated-SRU: A lightweight privacy-preserving intrusion detection system for Industrial Control Systems. *IEEE Internet of Things Journal, 9*(7), 5401–5413.
26. Louati, R., et al. (2022). Multi-agent reinforcement learning-based decentralized intrusion detection system for IIoT. *Ad Hoc Networks, 130*.
27. Nanjappan, S., et al. (2021). DeepLG SecNet: Layered deep learning architecture for IIoT security. *Journal of Network and Computer Applications, 178*.
28. Su, Y., et al. (2021). Big data management challenges in IIoT: A case study from the petrochemical industry. *IEEE Transactions on Industrial Informatics, 17*(4), 2756–2765.
29. Sun, Y., et al. (2021). Auction-based computing resource allocation in IIoT. *Journal of Parallel and Distributed Computing, 158*, 1–13.
30. Alohali, X., et al. (2021). ECSO and RNN-based intrusion detection system for cyber-physical fog systems. *Journal of Cybersecurity and Privacy, 1*(3), 401–420.
31. Wang, Z., et al. (2024). ECC-based lightweight mutual authentication for IIoT edge-cloud systems. *Sensors, 24*(2).
32. Zhang, S., et al. (2024). AI-driven anomaly detection frameworks for IIoT cybersecurity. *Cluster Computing, 27*, 95–110.
33. Sharma, et al. (2023). Deep CNN-based intrusion detection system for IIoT using spatial-temporal traffic patterns. *Neurocomputing, 500*.
34. Liu, H., et al. (2025). AI-enhanced intrusion detection system with model pruning and federated learning for scalable IIoT security. *Discover Internet of Things, 1*.
35. Su, Y., et al. (2021). Managing big data in IIoT: Challenges and case study in petrochemical plants. *IEEE Transactions on Industrial Informatics, 17*(4), 2756–2765.
36. Sun, Y., et al. (2021). Auction-based resource allocation for edge computing in IIoT environments. *Journal of Parallel and Distributed Computing, 158*, 1–13.
37. Zhang, X., et al. (2024). Secure M2M authentication in IIoT via lightweight ECC protocols. *Sensors, 24*(2).
38. Sharma, et al. (2024). AI-based threat classification and anomaly mapping in IIoT. *Cybersecurity Journal, 3*(1), 1–16.

***Corresponding Author:** Anil Kumar K N