IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# A COMPREHENSIVE REVIEW FOR IOT SECURITY: EXISTING CHALLENGES, RESEARCH POTENTIALS, AND FUTURE DIRECTIONS

[1]R.Poongodi, [2]Dr.A.Faritha banu

[1]Assistant Professor, [2] Assistant Professor,

[1]Department of Computer Technology,

[1]Karpagam Academy of Higher Education, Coimbatore, India.

***Abstract:*** The "Internet of Things" (IoT) is a network of computers that can work and interact with each other without needing a person to do anything. It is one of the most fascinating areas of computing right now since it can be used in so many different fields, including cities, homes, wearable tech, vital infrastructure, hospitals, and transportation. IoT technology brings advantages like little human intervention, being cheap, and being easy to set up. However, its extensive use also brings up problems with security and scalability. In order to demonstrate how frequent vulnerabilities are in software-based IoT background and the risks they represent to significant applications, new IoT security events are analyzed in this study. So, it is necessary to examine new security modules based on Machine Learning (ML) and Intrusion Detection (ID) software based on Deep Learning (DL), considering them as flexible pieces that can be added to IoT system topologies.

***Index Terms*** - IoT Protocol, Architecture, Security Attacks, Security Threats, IoT architecture.

## I. INTRODUCTION

The IoT looks into how various items, such as industrial systems, smart sensors, autonomous vehicles, machines, and terminals, could work together. It can also be referred to as a network of physical objects or things that are connected but have limited capabilities for data storage, computation, and communication [1]. These gadgets can exchange, analyse, and gather data because they feature software, network connectivity, and embedded electronics (such as sensors and actuators). We use IoT on a regular basis. Smart meters, IP cameras, smoke detectors, adapters, refrigerators, air conditioners, ovens, and temperature sensors are examples of smart devices. Additionally, accelerometers, radio-frequency identification (RFID) devices, heartbeat monitors, IoT in automobiles, sensors in rooms, etc were sophisticated gadgets that are included in it.

The IoT is bringing about new services and applications in areas including personal health care, household appliances, important agricultural infrastructure, and the military [2]. Intel says that IoT includes a huge number of smart sensors and devices that are making the web a smarter, more connected place. IoT nodes include sensors, actuators, and communication interfaces, but they don't have the computational power or flexibility that IDS agents normally have in traditional IP systems.

IoT networks are composed of numerous devices that are intricately connected to one another.

Because it has a big surface that can be attacked, it is extremely harder to design and keep a strong security system for them. Additionally, it is important to keep in mind that IoT devices are unprotected in an unidentified location. As a result, the data stored or generated by that device can be easily obtained

by an attacker. The IoT gadgets don't have a lot of power because their batteries limit how much they can use. This also makes it harder for them to store and analyze data [3].

In the IoT, security is utmost important, especially in areas where systems are important for the safety of people and communities. Three fundamental security policies are termed as the Confidentiality, Integrity, and Availability (CIA) triad. These security rules work for both the Internet and the IoT. If any of these basic needs are not met, it will affect the person or group in some way [4].

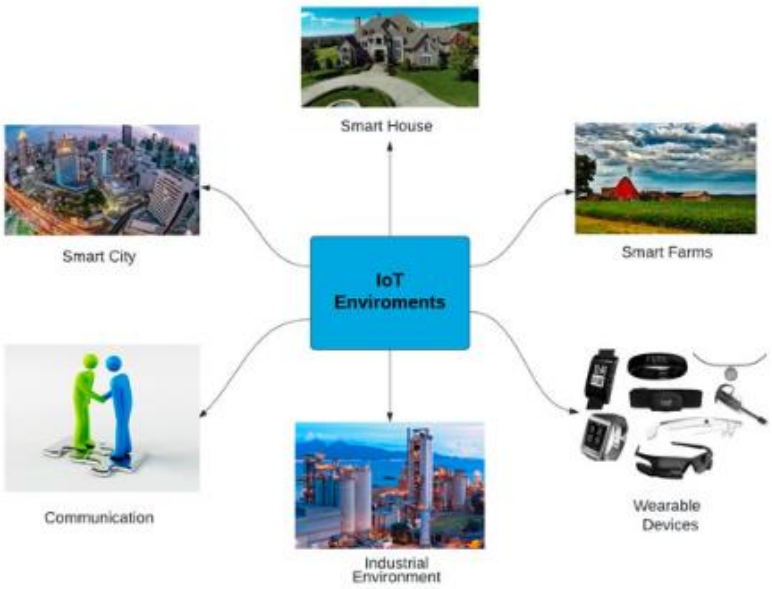


**Figure 1: IoT infrastructure**

Here, Figure 1 illustrates how the IoT infrastructure is made up of interconnected components. Data flow and control are made possible by this architecture. A wide range of devices, including medical and industrial equipment, wearables, and smart thermostats are included in this IoT. IoT devices offer advantages like convenience, effectiveness, and data-driven insights, but they also come with technological difficulties, security flaws, and privacy issues. Balancing advantages and downsides are crucial for prudent use of IoT technologies. IoT has numerous uses in healthcare, banking, education, government, and other industries [5]. Sensors, actuators, devices, a gateway, and a cloud server make up a typical IoT system. Data is gathered by sensors and sent to the cloud for processing and storage. For additional improvement, fog computing and edge computing might be utilised. With the support of endpoint devices, data is accessed by the end users, enables monitoring sensors and executing operational commands.

Despite their tiny size and compatibility, IoT devices confront resource constraints and security problems. Various communication methods are utilized for efficient data sharing. IoT devices use multiple communication channels and methods to exchange data efficiently.

The use of wireless-connected sensors is addressed by WSN, a subset of the IoT. It makes it possible to regulate physical sensing domains like transportation and healthcare in real time. A multi-layer design is now required since the IoT makes it easier for several heterogeneous devices to connect to one another. However, due to the authors' divergent opinions, the number of suggested architectures has not yet converged to a single model. The perception layer, network layer, and application layer are the 3 layers of a basic model [6].

Below are brief descriptions of each tier:

i. **Application Layer -** Data from IoT devices is processed, examined, and acted upon at the application layer. It consists of software, services, and apps that leverage data from IoT devices to do operations, provide users with information, and assist users in making wise decisions. Smart homes, industrial automation, and healthcare are just a few of the many applications for which this layer can be modified. Security concerns including DoS attacks, which can be software assaults, injection attacks, tampering, and scripting attacks are also included in this layer.

ii. **Network Layer -** Data transfer between IoT devices and the network is made possible by the network layer. In order to manage and process intelligent events in the IoT, objects must be able to communicate with connected devices through the network layer [69]. Receiving important digital data is the aim of this layer. A range of communication technologies, including WiFi, Bluetooth, WiMax, Zigbee, GSM, and 5G [70], must be used with protocols like IPv4, IPv6, and MQTT are used. Data is extracted from the perception layer via this integration and sent to middleware-layer processing systems. The IoT sensors produce a lot of data, efficient middleware management is necessary. In this tier, cloud computing is essential [8].

iii. **Perception Layer -** An essential connection between the IoT and the real world is the IoT perception layer. This layer consists of sensor nodes with varying wireless communication capabilities and resource limitations, forming a self-organising network system. This layer sends data from "objects" to a gateway or sink by physically connecting to them. This layer contains a range of devices that are used to gather information about things and their surroundings, such as sensors, RFID readers, cameras, and cellphones. It is important to note, nevertheless, that this layer is vulnerable to serious security problems.

Any behaviour, whether intentional or not, that threatens the security of data and/or computer systems is referred to as a security attack [7]. This includes replaying or interrupting data to create new data, copying data, assessing traffic, and changing original data.

**Physical attacks**: A physical attack happens when attackers acquire direct access to hardware devices and modify or break them to steal data or disrupt operations. IoT devices are often located in open or remote places, which makes these kinds of attacks more common.

**Software attacks**: Software assaults look for weak spots in operating systems, programs, or firmware so they can get in without permission or destroy systems.

**Network attacks**: Network attacks aim at the communication paths between devices to steal, change, or stop data that is being sent.

**Encryption attacks**: Encryption attacks attempt to break or bypass cryptographic systems to access protected data.

Some of the most prevalent applications for IoT devices are listed below:

i. Transportation: IoT is widely employed in smart cars that drive themselves. This might help with traffic control, finding locations where accidents are likely to happen, and figuring out the best speed for cars to go to save gas. By looking at the information from GPS, CCTVs, weather sensors, and other sources. The ML/DL algorithm may produce accurate predictions. Transportation would become safer and more effective as a result [9].

ii. Agriculture: IoT devices can be used in agriculture to gather real-time data that helps farmers identify and address climate and soil defects at the right time. These instruments can tell you how much moisture is in the soil, how hot it is outside, what the weather is like, and how humid it is. This information can be used to set up automatic watering, find diseases early on, check soil quality, and more.

iii. Healthcare: IoT devices are made to keep a careful eye on a patient's health, find problems early on, and quickly let the right people know. But it's really important to secure patients' information, and simultaneously, the medical authorities need to be able to get to the data right away without any problems. It is especially helpful when medical professionals need to be alerted right away

in an emergency when routine visits might not work. Therefore, all of the aforementioned requirements must be satisfied, but consider that IoT devices are not very powerful [10].

iv. Smart Homes: IoT lets home appliances make smart and reasonable choices. For instance, air conditioners may change the temperature on their own based on the weather, and gates can open on their own based on face recognition. The air conditioner needs to keep an eye on the temperature and humidity inside and outside the house all the time. It should also be able to respond to changes in the environment.

v. Supply Chain: IoT can be added to the manufacturing and transfer of things and making it more adaptable. You can keep track of the goods at every step of the production and delivery process, all the way to the customer. To make the right choices for improving the customer experience and making the best use of resources, you need to be able to analyze data well.

vi. Commerce domain: Facilitates faster and more effective commerce operations for both physical storefronts and online retailers. IoT devices can be deployed at sales terminals to automatically track inventories and allow customers to make purchases. One example of a device in the commerce realm is a square card reader.

The remaining part of this work is structured in this manner: The IoT components, architectures, protocols, and difficulties were reviewed in Section 2. A research gap for IoT systems was presented in Section 3. Section 4 discusses the analysis of used datasets, evaluation metrics in the IoT system, and associated IoT survey works before concluding this study.

## II. LITERATURE REVIEW

A hierarchical blockchain (BC)-based federated learning (FL) system was introduced by Sarhan et al. [2022] [11]. A secure and privacy-preserved collaborative IoT ID is facilitated by this system. The cyber threat intelligence was transmitted over inter-organizational IoT networks, and the significance of this transmission is highlighted and demonstrated. A hierarchical FL design is used in the suggested ML-based ID system (IDS) to protect the organization's data and the learning process. The smart contract will verify that the operations were completed successfully, and the transactions (model updates) and procedures will occur on a safe BC. This approach was tested and shown that it works by putting it into action and using a crucial IoT data set to see how well it detects intrusions. The result is a well-designed ML-based IDS that can find several bad actions while keeping information private.

An AI-powered edge computing strategy for IIoT was presented by Zhao et al. [2022] [12]. Then, a novel software-defined industry control architecture was developed. This implementation may support in enhancing the adaptability and security of IIoT edge systems.
Industrial modelling and virtualisation technologies are used in the design to keep the hardware and software of industrial devices apart. This helps with the industrial data privacy issue and increases the adaptability and programmability of IIoT edge systems. In AI-driven IIoT, cutting-edge edge computing technique known as "dispersed computing" is used. Thus, real-time efficiency and resource utilisation are enhanced. The networking and computing of AI-driven industrial applications were enhanced by the multi objective optimisation scheduling technique. Here, the suggested computing solution makes use of a multiobjective optimisation scheduling technique. The simulation establishes the efficacy of the suggested approach.

In ML IoT-based intelligent systems, new systems, security, innovative approaches, and susceptibilities were analyzed by a method suggetsed by El-Sofany et al [2024] [13]. A vital component of technology in improving IoT security is this recommended method. The pros and restrictions of using ML in an IoT context are described in the paper. It offers an ML-based security framework that separately resolves emerging security problems associated with the IoT sector. By developing a ML-based method for identifying cyberattacks on IoT devices, this study had a significant impact. Using 7 ML methods to find the most accurate classifiers, researchers have created an AI-based reaction agent to identify IoT network intrusions. The suggested method attains a 99.9% accuracy (ACC) rate, a 99.8% detection average, a 99.9 F1 score, and a perfect AUC score of 1, and it executes better than others.

With the utilization of lightweight neural network (NN), differential privacy (DP), and homomorphic encryption (HE), privacy-preserving FL architecture was developed by Puviarasu and Sudha [2026] [14].

The suggested model had 1,191,264 occurrences and 47 attributes when it was evaluated on the IoT ID Dataset from Kaggle. Its overall ACC was 93.5%, its precision (PRE) was 94.2%, its recall (Sensitivity) was 93.4%, and its F1-score was 94.2%. This study examined the detection time, which ranged from 90 to 130 ms, and found no differences between the attacks. For DoS attacks, the model's accuracy was 94.1%, for DDoS assaults it was 92.5%, and for Mirai attacks it was 93.6%. Additionally, its ACC for malware and web-based threats was higher than 85%. A trade-off between privacy and performance was shown by DP tests. Increasing the privacy budget parameter from 0.5 to 20.0 reduced processing time from 150 ms to 121 ms and increased ACC levels by 2.6% to 94.0%, as demonstrated by outcomes. When switching from no encryption to complete HE, the experiments also showed that its computation times increased (from 120 ms to 200 ms), their ACC slightly decreased (from 94.1% to 93.5%). According to device-level testing, the model exhibits strong performance on both powerful and low-end processors, maintaining a high ACC. With restricted hardware (0.5 GHz CPU, 128 MB memory), the model achieved above 91% ACC. With an inference time of 110 ms, the performance increased to 94.5% ACC when tested on more potent processors. The experiments verified that the accuracy of the model is maintained even in the presence of heterogeneous sensor data. This demonstrates that the concept works well in a heterogeneous IT environment. With only a minor decline in ACC (<0.8%), audit techniques further increased compliance from 0% to 99%. The results show that in resource-constrained IoT networks, privacy-preserving ID may be successfully implemented with real-time ID, high detection rates, and privacy assurances.

In the IoT-enabled edge-computing background, an Intelligent Deep FL Model for Enhancing Security (IDFLM-ES) was suggested by Albogami [2025] [15]. The unwanted intrusions are detected by this method, and helps in ensuring security in the IoT background. A federated hybrid deep belief network (FHDBN) framework was created by the IDFLM-ES method, as it uses FL on time series data generated by the IoT edge devices to establish that model. Pre-processing procedures in the IDFLM-ES method include data normalisation and feature selection.

(FS) based on golden jackal optimisation (GJO). In order to speed up model convergence and learning, the IDFLM-ES approach additionally learns how to represent features both individually and across distributed databases. Finally, the optimal hyperparameter for the FHDBN model is determined using the dung beetle optimiser (DBO) model. A benchmark database is used to validate the suggested technique's simulation value. When compared to other models, the IDFLM-ES methodology's experimental validation showed a higher ACC rate of 98.24%.

An innovative framework for adaptive edge security was suggested by Halgamuge and Niyato [2025] [16]. This model generates and modifies security policies for Internet of Things edge devices dynamically. The AI-Driven Adaptability Integration, Regulatory Compliance Analysis, Conflict Detection and Resolution, Bias-Aware Risk Assessment, and Dynamic Security Policy were integrated in this model. As the threat landscape, legal requirements, and device statuses change, this approach creates security policies that are unique to each scenario. It classifies important security vulnerabilities in different IoT background and verifies the efficacy of this design using both simulations and real-world implementations. This method makes IoT security policies much more robust and adaptable. The results show how integrating AI and ML may help create secure protocols for IoT ecosystems that are resilient and adaptable. To secure IoT devices from emerging attacks, dynamic and adaptive security frameworks are required. This approach guarantees compliance with legal requirements and maintains the availability and integrity of IoT services for a variety of uses.

A new hybrid approach to post-quantum cryptography (PQC) was created by Elnour [2026] [17], which greatly boosts edge-IoT networks. The suggested model integrates lattice-based techniques, specifically Kyber-786 and Dilithium-III, alongside an AES-GCM layer model. A mathematical analysis of trust and key negotiation also shows how classical and quantum attackers might resist module-LWE and ring-LWE assumptions. The simulation in Python shows that the proposed method enhances throughput by 18.6% and lowers latency by 22.4% compared to standard methods. Also, the hybrid design cuts energy utilization by 41.7% thanks to hardware-accelerated two-polynomial processes and better offloading. The analysis has demonstrated that the suggested solution meets the requirements for confidentiality, integrity, and authenticity, incurring an overhead of less than 7.3 ms per transaction. Furthermore, PQC may be used in both IoT and consumer environments without sacrificing responsiveness and energy efficiency.

For accurate ID in IoT networks, a Hybrid Stacked DL (HSDL) architecture was created by Leon-Granizo et al. [2026] [18] . The suggested structure combines Stacked (LSTM) Long Short-Term Memory (SLSTM) networks to identify long-term temporal correlations in sequential traffic patterns with Vectorised Convolutional NN (VCNN) for enhanced feature extraction. Data processing is enhanced and retains efficiency through the deployment of a Spark-based pretreatment pipeline. In large-scale situations, this enables real-time adaptation. A bio-inspired metaheuristic named Harris Hawks Optimisation (HHO) adjusts hyperparameters. Then, Deep LSTM and HHO (DLSTM-HHO) supports in improving detection efficiency, accuracy and generalisation. The N-BaIoT, UNSW-NB15, and UNSW-IoT-Botnet benchmark datasets were used for extensive evaluations. The outcomes demonstrate how effectively the suggested framework performs. The HSDL framework outperformed conventional baselines like CNN and LSTM with a maximum accuracy of 99.89%. In comparison to LSTM (95%), LSTM-RNN (83%), DNN (79%), and Naïve Bayes (78%), the DLSTM-HHO variation achieved 99% ACC. The HSDL design may provide reliable and resource-efficient ID, reducing false positives (FP), and it was demonstrated by the outcomes. Edge-deployable, real-time, scaled IoT threat monitoring is made possible by this architecture.

A novel Security and Congestion-Aware Data Transmission (SCADT) model was suggested by Shwethashree et al. [2026] [19]. Congestion-aware cluster-head (CH) selection with reputation-based trust evaluation are integrated in this suggested model. This may facilitate secure and effective communication. This paper resolves the issue of inadequate attack and breach detection in IoT-Edge environments, which compromises throughput and reliability when attack frequencies are high. SENSORIA and CloudSim were used to test SCADT in situations where 10%, 20%, 30%, and 40% of the data was under assault. With an average of 47.5% more breach identification, 50.5% more threat detection, and 45.2% more throughput than NATURE, the data demonstrate that SCADT consistently outperforms NATURE and RG-ACA. SCADT outperforms RG-ACA by 12.3% in breach detection, 11.8% in threat detection, and 12.5% in throughput. These results show that SCADT works well to improve security while keeping network speed high. This shows that it is new and strong enough to work well for IoT-Edge communication even when there are problems.

FLiForest, a unique approach for identifying abnormalities on the IoT edge that combines FL with the isolation forest (iForest) technology, was created by Xiang et al. [2026] [20]. This method outlines a three-step process that includes data collection and sampling, model training, and data testing in order to collaboratively train an iForest between clients and edge servers. FLiForest enhances data privacy and reduces computational cost by facilitating decentralized model training among IoT devices—all without requiring the sharing of multimedia data. Then, evaluating the performance of this approach with the modern anomaly detection techniques by doing extensive tests on a variety of multimedia datasets. This highlights this technique's strength in protecting data privacy and security, as well as its higher detection accuracy.

**Table 1: Comparative table for existing methods in IoT security**

| Authors | Methods/Application | Merits | Demerits |
|---|---|---|---|
| Sarhan et al [2022] [11] | IoT network security | Makes ensuring that learning is private and that models can be shared safely. | A lot of processing power is needed and the architecture is complicated. |
| Zhao et al [2022] [12] | Multiobjective optimization scheduling algorithm | Makes a better use of resources and offering solutions that are fair. | Requires more processing time |
| El-Sofany et al [2024] [13] | ML – algorithms | By ACC and performance time, it executes well. | For real-time applications, execution time is critical. |
| Puviarasu and Sudha [2026] [14] | Privacy-preserving FL model | Used in privacy guarantees in resource-constrained IoT networks. | Encryption and secure aggregation are two privacy approaches that need more computing power. |

| | | | |
|---|---|---|---|
| Albogami [2025] [15] | IDFLM-ES | Sensitive data stays on local devices instead of being transferred to a central server, which makes privacy protection better. | The network gets busier when a lot of local devices talk to the central server. |
| Halgamuge and Niyato [2025] [16] | Adaptive edge security framework | promotes data privacy, lowers latency, and improves real-time threat detection | It faces challenges such as limited edge device resources. |
| Elnour [2026] [17] | Hybrid post-quantum cryptography (PQC) | Consumer environments without sacrificing responsiveness and energy efficiency | Consumes more processing power |
| Leon-Granizo et al [2026] [18] | Hybrid Stacked Deep Learning framework | Improves real-time threat detection. | Complicated deployment on edge devices with limited resources |
| Shwethashree et al [2026] [19] | SCADT framework | Success in delivering improved safety measures while preserving outstanding network efficiency | Increases system complexity |

## III. RESEARCH GAP

Even though IoT systems that work with Edge security are growing quickly, there are still some research gaps that need to be filled in order to make sure that IoT-edge environments are safe. Many of the security systems that use today require large computing ability, which makes them unsuitable for resource-contrained IoT device that are positioned at the edge. Many current IDS have trouble finding attacks in real time while keeping latency low. Also, keeping robust privacy protection is still hard, especially with new methods like Federated Learning. It's also harder to defend systems because there aren't any common security standards for connecting IoT devices, edge nodes, and cloud infrastructure. Also, edge nodes are open to physical manipulation and sophisticated cyberattacks, and when security models are used on big IoT networks, they might cause problems with scalability. So, we need to build security frameworks that are light, scalable, and smart so that they can safeguard IoT-edge systems well while also making sure that resources are used well and data privacy is strong.

### Machine Learning in IoT

In order to analyse the vast amounts of data produced by IoT devices and create algorithms that recognise patterns in behaviour, ML and DL are crucial [16].
ML enhances the security of the IoT by enabling intelligent detection of cyber threats such as intrusion, malware, and anomalies through algorithms like Decision Trees (DT), SVM, and NN. It improves real-time monitoring, accuracy, and automation, especially in edge and distributed environments.

ML in IoT security has **limitations**, including dependence on large labeled datasets, high computational cost, and difficulty in deployment on resource-constrained devices. Its efficacy in practical situations is further diminished by problems including overfitting, explainability challenges, privacy concerns, and susceptibility to adversarial attacks.
Supervised Learning: Accurately identifies and categorizes known IoT security risks using labeled data.

Unsupervised Learning: Finds anomalies in unlabeled IoT data to identify unknown assaults.

Reinforcement learning: Through interaction with the IoT environment and feedback, it learns the best security measures in real time.

**Deep Learning in IoT**

IoT security makes extensive application of DL techniques to detect and stop a variety of cyberthreats, including malware, intrusions, and denial-of-service attacks. DL models are very effective in dynamic and heterogeneous situations because they can automatically learn complicated patterns from massive IoT data, unlike standard ML methods. Models like as CNN, Recurrent NN (RNN), and LSTM networks are often utilized for anomaly and ID in IoT networks. In order to identify questionable activity, these models can instantly examine sensor data, network traffic, and device behavior [18].

**Security Challenges in IoT**

Applications including the IoV, healthcare IoT, IIoT, and smart city IoT are revolutionising important facets of standard of living, hospitals, manufacturing, and smart city in the quickly developing IoT landscape. However, there are serious security, privacy, and trust issues brought about by the extensive use of connected devices in these sectors. Concerns regarding the CIA of data are raised as these IoT devices collect and analyze enormous volumes of personal information, making them susceptible to a variety of security risks. IoT applications frequently gather sensitive or personal data that could be exploited if disclosed, so privacy protection is crucial. Furthermore, reliable connectivity and the avoidance of data manipulation depend on trust between IoT entities. The main obstacles that are particular to each application highlight the necessity of thorough security measures, privacy protections, and trust management procedures that are adapted to the particular needs of each IoT domain.

## IV. DATASET AND EVALUATION METRICS

In the fast-paced world of cybersecurity today, comprehensive and representative data is crucial to the analysis and development of IDS. These datasets are crucial standards for creating and evaluating artificial intelligence (AI) that can identify and respond to various risks [17].

**Dataset Usage for IDS in IoT Networks**

IDS designed for IoT networks mainly rely on publicly accessible datasets. The purpose of this study is to examine the present level of DDoS attack intensities, IoT device-related problems, and the limitations of the available datasets.

**Table 3: Dataset usage in articles**

| References & Year | ML/DL Frameworks | Dataset | Efficiency |
|---|---|---|---|
| Afrah Gueriani et al. (2024) | CNN and LSTM | CICIoT2023 | High precision |
| Saadat Izadi & Mahmood Ahmadi (2026) | Mobile Net Federated learning | ToN-IoT | Reduced latency |
| Izadi & Ahmadi (2026) | Meta Federated Learning | BoT-IoT | Improved accuracy |
| Ikbarieh et al. (2025) | Random Forest + LLM | CICIoT2023 + Edge-IIoTset | Strong attack detection |

| | framework | | |
|---|---|---|---|

**Evaluation of metrics used in IoT security**

In many different sectors, including performance, security, and quality assessments, a number of crucial metrics are employed to evaluate the efficacy of frameworks. By calculating the percentage of accurate forecasts to all cases, ACC evaluates the accuracy of forecasts. The framework's potential to lower FP is demonstrated by PRE, which gauges the accuracy of positive predictions. Sensitivity, another name for recall, evaluates the framework's capability to determine all pertinent instances while taking the rate of false negatives (FN) into consideration.

The harmonic mean of PRE and sensitivity yields the F1-Score. When FP and FN are considered, the T is F1-score offers a balanced evaluation. The fraction of incorrect positive predictions among TN is measured by the FP Rate (FPR). For applications like medical diagnostics and fraud detection, FPR is essential. The model's capacity to find all pertinent cases is demonstrated by both Detection Rate (DR) and TP Rate. For security and threat detection systems, TPR is crucial. At last, Detection Accuracy provides a complete understanding of a system's efficiency by assessing both positive and negative cases. These metrics are essential for streamlining processes and enhancing decision-making in many different fields. Table 3 illustrates the used metrics in IoT.

**Table 3: Useful Metrics in IoT**

| Metric | Formula | Common Use Cases |
|---|---|---|
| ACC | $\frac{TP+TN}{TP+TN+FP+FN}$ | Evaluation of general |
| PRE | $\frac{TP}{TP+FP}$ | Fraud detection |
| Sensitivity | $\frac{TP}{TP+FN}$ | ID |
| F1 Score | F1 Score = 2*$\frac{Precision*Recall}{Precision+Recall}$ | Imbalanced datasets in |
| FPR | FPR = $\frac{FP}{FP+TN}$ | Clinical evaluation, |
| FNR | FNR= $\frac{FN}{FN+TP}$ | Security systems, risk |
| AUC-ROC | AUC-ROC = Area under the ROC curve | Classification model |
| DR | Detection Rate = $\frac{TP}{TP+FN}$ | ID, detecting malware |
| False Alarm Rate | FAR = $\frac{FP}{FP+TN}$ | Network security systems |
| Matthew's Correlation Coefficient (MCC) | MCC = $\frac{TP*TN-FP*FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$ | Binary classification in imbalanced |

**Gap Analysis**

The lack of attention on practical applicability and the lack of standardised IDS evaluation techniques are two significant gaps in the current environment. Real-world IoT scenarios are still unpredictable, despite research promising high accuracy rates in controlled conditions. To enable more realistic evaluations of suggested IDS, standardised standards and evaluation criteria that take into account the complexity of IoT contexts are needed.

- Comprehensive IoT-specific datasets.
- Integration of Lightweight frameworks.
- Holistic Evaluation Approaches.

- DL Techniques.
- Privacy and security concerns.

A lack of real-world testing on a variety of IoT devices and resource-intensive model integrations are two obstacles to integrating ML models into IoT security systems. Many benchmark datasets suffer from class imbalance and fail to take into account IoT-specific properties. Reducing computing costs while maintaining high accuracy in detection is critical, as is resolving the shortcomings of specific frameworks, like NB.

The reliance on large-scale datasets raises privacy and security problems, as does the vulnerability to adversarial attacks, making it difficult to identify innovative DDoS operations.

**Conclusion and Future Directions**

In-depth analysis of security concerns at various IoT layers is provided in this survey report along with appropriate solutions. This survey explains many IoT layers: physical, software, network, and encryption, that pose security risks to IoT devices. Applications of IoT are also covered here. People's daily lives are positively impacted by the great network known as the IoT. Also, there are drawbacks as well, like eavesdropping, criminality, DoS, unwanted access to data, node forging, and detecting infiltration. The rapid expansion of the IoT has brought to light serious security issues that call for sophisticated IDS. By implementing advanced solutions and strong security measures, stakeholders may safely use IoT technology, making sure that the IoT ecosystem is strong and safe for future deployments. Large IoT-specific datasets that capture the complexity and varying nature of IoT networks, including a variety of devices, communication patterns, and current cyberthreats, must be the main emphasis of upcoming study. For the application on IoT devices with constrained resources, it is critical to optimise lightweight, energy-efficient IDS models. This means finding the right balance between speed and accuracy of detection. It would be simpler to compare and assess IDS models more precisely if standards and evaluation criteria were established that reflected actual IoT scenarios. Research can be made more coherent by integrating FS and feature extraction processes into a cohesive framework and using evaluation techniques that include accuracy, computational cost, and flexibility overall.

**References**


1. Sadhu, P.K., Yanambaka, V.P. and Abdelgawad, A., 2022. Internet of things: Security and solutions survey. Sensors, 22(19), p.7433.
2. Charfare, Ruwayd Hussain, Aditya Uttam Desai, Nishad Nitin Keni, Aditya Suresh Nambiar, and Mimi Mariam Cherian. "IoT-AI in Healthcare: A Comprehensive Survey of Current Applications and Innovations." International Journal of Robotics & Control Systems 4, no. 3 (2024).
3. Ahmad, Z., Iqbal, S., Ullah, M.O., Naeem, W. and Azam, M., 2024. IoT Security Issues and Challenges. Kashf Journal of Multidisciplinary Research, 1(12), pp.233-253.
4. Fei, W., Ohno, H. and Sampalli, S., 2023. A systematic review of IoT security: Research potential, challenges, and future directions. ACM computing surveys, 56(5), pp.1-40.
5. Dubey, K., Dubey, R., Panedy, S. and Kumar, S., 2024. A review of IoT security: Machine learning and deep learning perspective. Procedia Computer Science, 235, pp.335-346
6. Singh, K. and Neeru, N., 2023. A comprehensive study of the iot attacks on different layers. Journal Punjab Academy of Sciences, 23, pp.140-155.
7. Sagu, A., Gill, N.S., Gulia, P., Alduaiji, N., Shukla, P.K. and Shah, M.A., 2025. Advances to IoT security using a GRU-CNN deep learning model trained on SUCMO algorithm. Scientific Reports, 15(1), p.16485.
8. Zahid, M. and Bharati, T.S., 2026. Leveraging Machine Learning and Deep Learning in IoT Security: A Review. Security and Privacy, 9(1), p.e70144.
9. Zreikat, A.I., AlArnaout, Z., Abadleh, A., Elbasi, E. and Mostafa, N., 2025. The integration of the internet of things (IoT) applications into 5G networks: a review and analysis. Computers, 14(7), p.250.
10. Sizan, N.S., Dey, D., Layek, M.A., Uddin, M.A. and Huh, E.N., 2025. Evaluating blockchain platforms for iot applications in industry 5.0: A comprehensive review. Blockchain: Research and Applications, p.100276.
11. Sarhan, M., Lo, W.W., Layeghy, S. and Portmann, M., 2022. HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. Computers and Electrical Engineering, 103, p.108379.

12. Zhao, Y., Hu, N., Zhao, Y. and Zhu, Z., 2023. A secure and flexible edge computing scheme for AI-driven industrial IoT. Cluster Computing, 26(1), pp.283-301.
13. El-Sofany, H., El-Seoud, S.A., Karam, O.H. et al. Using machine learning algorithms to enhance IoT system security. Sci Rep 14, 12077 (2024).
14. Puviarasu, A. and Sudha, V.K., 2026. Enhanced IoT security: privacy-preserving federated learning model for accurate, real-time intrusion detection across devices. Ain Shams Engineering Journal, 17(1), p.103866.
15. Albogami, N.N. Intelligent deep federated learning model for enhancing security in internet of things enabled edge computing environment. Sci Rep 15, 4041 (2025).
16. Halgamuge, M.N. and Niyato, D., 2025. Adaptive edge security framework for dynamic IoT security policies in diverse environments. Computers & Security, 148, p.104128.
17. Elnour, A.A.H., 2026. Integrating Post Quantum Cryptography (PQC) for End-to-End Security in Edge and IoT Environments. IEEE Transactions on Consumer Electronics.
18. Leon-Granizo, O., Palacios-Zamora, K., Yagual-Muñoz, O. et al. Intelligent Deep Learning-Based NetFlow Botnet Detection and AI-Powered Malware Classification for IoT Edge Security. SN COMPUT. SCI. 7, 41 (2026).
19. GC, S. and Thimmappa, P.B., 2026. A Novel Multi-layer Architecture for Enhancing IoT-edge Security for Intrusion Detection and Network Performance Optimization. International Journal of Intelligent Engineering & Systems, 19(2).
20. Xiang, H., Zhang, X., Xu, X., Beheshti, A., Qi, L., Hong, Y. and Dou, W., 2026. Federated learning-based anomaly detection with isolation forest in the IoT-edge continuum. ACM Transactions on Multimedia Computing, Communications and Applications, 22(1), pp.1-19.
21. Dubey, K., Dubey, R., Panedy, S. and Kumar, S., 2024. A review of IoT security: Machine learning and deep learning perspective. Procedia Computer Science, 235, pp.335-346.
22. Patil, D.A. and G, S., 2025. A comprehensive survey on securing the social internet of things: protocols, threat mitigation, technological integrations, tools, and performance metrics. Scientific Reports, 15(1), p.40190.
23. Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A., Kamal, T.: A review on internet of things (IoT). Int. J. Comput. Appl. 113(1),1–7 (2015).
24. Rakine et al., "Comprehensive Review of Intrusion Detection Techniques: ML and DL in Different Networks," in IEEE Access, vol. 13, pp. 104345-104367, 2025.
25. Rahman, M.M., Al Shakil, S. and Mustakim, M.R., 2025. A survey on intrusion detection system in IoT networks. Cyber Security and Applications, 3, p.100082.
26. M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020.
27. Singh, S., Sharma, P.K., Moon, S.Y. et al. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Human Comput 15, 1625–1642 (2024).
28. Aparcana-Tasayco, A.J., Deng, X. and Park, J.H., 2025. A systematic review of anomaly detection in IoT security: towards quantum machine learning approach. EPJ Quantum Technology, 12(1), p.112.
29. Alfahaid, A., Alalwany, E., Almars, A.M., Alharbi, F., Atlam, E. and Mahgoub, I., 2025. Machine learning-based security solutions for iot networks: A comprehensive survey. Sensors, 25(11), p.3341.
30. Ali, M., Raza, A., Akram, M.A., Arif, H. and Ali, A., 2025. Enhancing IOT Security: A review of Machine Learning-Driven Approaches to Cyber Threat Detection: Enhancing IOT Security: A review of Machine Learning-Driven Approaches to Cyber Threat Detection. Journal of Informatics and Interactive Technology, 2(1), pp.316-324.