

Current Perspectives on Internet of Things Security and Intelligent Threat Detection

Dr Prathviraj Singh Rathore

Assistant Professor, Department of Computer Sciences and Applications

Mandsaur University, Mandsaur

prathviraj.rathore@meu.edu.in

Corresponding Author: * Prathviraj Singh Rathore (prathviraj.rathore@meu.edu.in)

Received: 5 August 2026 | **Revised:** 10 August 2026 | **Accepted:** 25 August 2026

Abstract—The IoT has revolutionised computing by facilitating the seamless communication of interconnected devices in several industries, including transportation, healthcare, smart cities, and industrial automation. The large-scale deployment of IoT networks has however created a wide range of security and privacy issues, as devices are resource-limited, have diverse architectures, and are facing new types of cyber threats. This review paper provides a general overview of the latest insights into IoT security and intelligent threat detection. It covers the basic security requirements, common vulnerabilities and key attack strategies for IoT environments. Additionally, the paper explores traditional security solutions as well as the latest developments in Malware Detection, Distributed Denial-of-Service (DDoS) attacks, Botnets and Anomalous network behaviour by utilising Machine Learning (ML) and Deep Learning (DL). The algorithms, applications, advantages and disadvantages of intelligent threat detection techniques are highlighted for comparative analysis. The review also presents the summary of the most common public datasets and metrics used for evaluating the performance of different solutions in the field of IoT security studies. Finally, the focus is on key research challenges, emerging technologies, and future directions to support the development of robust, scalable, and intelligent IoT security solutions to address the ever-changing nature of cyber threats.

Keywords—Internet of Things (IoT), Intelligent Threat Detection, Cyber Threats, Machine Learning, Deep Learning, Security.

I. INTRODUCTION

The world's digital technology has revolutionized the systems of today by allowing connected devices, constant data sharing, and intelligent services. But, more connectivity also means more vulnerabilities, so there is a need for security mechanisms to be effective against the new cyber threats. The Internet of Things (IoT) is a large network of physical objects that are connected to the Internet and contain sensors, software, and various technologies that allow them to interact with each other and with central systems [1]. This communication enables the seamless collection and analysis of information in real time, which can lead to intelligent automation in various industries such as healthcare,

transportation, agriculture, and energy management, among others. In smart cities, for example, the technologies of IoT are employed to improve traffic efficiency, energy use, public safety, and even the efficient management of waste. These capabilities represent significant efficiencies and conveniences, but they also pose an important risk: security of these devices. The very attributes that make IoT devices appealing—such as the ability to collect and transmit sensitive data—also render them susceptible to cyber threats. Every device that is plugged into the Internet increases the digital attack surface and provides more potential points of entry for bad guys. A compromised device can serve as an entry gateway for attackers, enabling them to infiltrate entire networks, steal sensitive data, or disrupt critical infrastructure [2][3].

This research offers a multi-dimensional view of IoT security, offering a unified framework for analysis rather than focusing on any single aspect like architecture, attack models or detection techniques in isolation. The paper also proposes a four-dimensional attack classification for attack vector, target, attack method, and attack impact to deepen the understanding of the IoT threat. Moreover, this survey is not just a descriptive review but also an analytical one that shows strengths, weaknesses, and trade-offs of the IoT architectures, communication protocols, and ML-based detection approaches. This holistic view sets this book apart from earlier work and contributes to the design of secure IoT solutions [4][5].

Security solutions that work well with the trust levels of IoT sensors and integrate smoothly with network topology, smart devices, and processing systems are necessary to address vulnerabilities in the Internet of Things (IoT). Finding Internet of Things (IoT) devices across various interactions, classifying them, and associating them with media access control (MAC) addresses without hardware modifications is a significant difficulty. The use of learning frameworks to solve such challenges has the potential to enhance the management of cyber-physical systems using MAC designs. Applications of the Internet of Things (IoT) range from smart homes to vital infrastructure, and they have been propelled by the exponential proliferation of wireless sensor devices [6][7]. To

train ML and DL algorithms, datasets should ideally contain real-time IoT system data. However, due to IoT data complexity, datasets are commonly created by collecting different traffic types and attack signatures. These datasets support the training and evaluation of ML and DL algorithms for effective attack detection. Feature extraction, data cleaning, and data conditioning are also important for preparing datasets. Ensuring that datasets accurately represent real-world IoT environments is essential for achieving reliable and effective AI-based detection results[8].

This paper is organized as follows: Section II introduces Internet of Things Security Fundamentals. Section III Intelligent threat detection. Section IV: Threat Detection Methods Using Artificial Intelligence Recent literature is reviewed in Section V, and the paper's conclusion and possible future study areas are outlined in Section VI.

II. INTERNET OF THINGS SECURITY FUNDAMENTALS

The Internet of Things (IoT) is an ecosystem of interconnected physical objects, or “things,” that communicate with each other, sense and react to their environment, and share data via the Internet in the way that the human world does. In a variety of application areas, such as healthcare, smart cities, industrial automation, agriculture, and transportation, IoT devices interact with one another and cloud or edge computing platforms to enable intelligent monitoring, automation, and decision-making [9].

A. Components of Iot

The IoT is composed of four basic elements, Sensors / Devices, Connectivity, Data Processing and User Interface, as depicted in Fig. 1. These components work together to collect data, transmit it over communication networks, process it, and present meaningful results to end users.

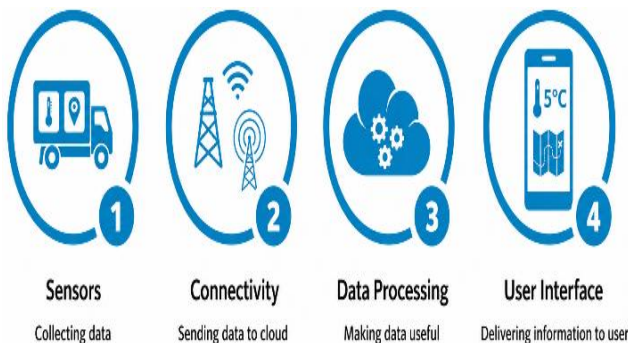


Fig. 1. Main Components of an IoT System

- **Sensors/Devices:** One essential element that enables to get real-time data from surroundings is sensors or other devices. A gadget may contain different kinds of sensors that do more than just sense.
- **Connectivity:** A cloud infrastructure receives all of the gathered data. A variety of communication channels should be used to link the sensors to the cloud. These communication channels include Bluetooth, WI-FI, WAN, satellite or mobile networks, etc.
- **Data Processing:** The program processes the data after it has been captured and transferred to the cloud [10]. This procedure can be as simple as taking a temperature reading on appliances like air conditioners or heaters. But occasionally, it may also be quite

complicated, such as when utilizing computer vision on video to detect things.

- **User Interface:** The end-user must have access to the information in some manner, which can be accomplished by sending them notifications via email or text message or setting off alarms on their phones. An interface that actively monitors their IoT system may occasionally be required by the user [11].

B. Iot Architecture

IoT designs often have several layers, each of which has a distinct function within the IoT system [12]. These systems use cloud, edge, and fog computing concepts to strike a balance between centralized control and distributed computation. as seen in Fig. 2.

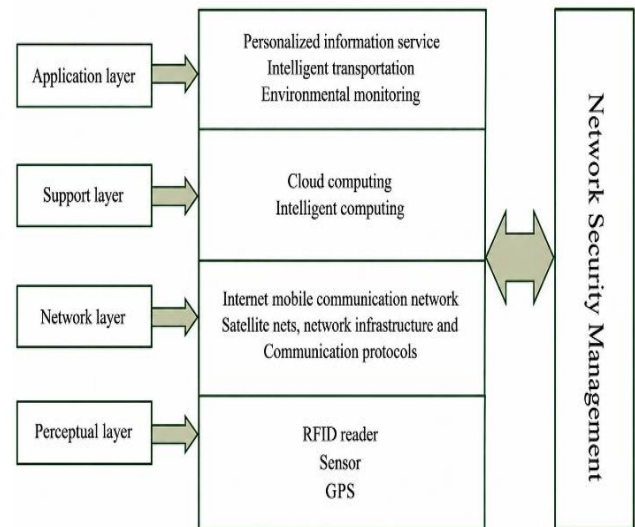


Fig. 2. IoT Architecture

- **Perceptual Layer:** This fundamental layer, also known as the recognition layer, uses physical equipment to collect all kinds of data and recognize the outside environment.
- **Network Layer:** The network layer is the second layer of the security architecture. Data from the preceding layer is collected by this layer [13]. This is in charge of processing the data gathered from sensor cataloging and polymerization, as well as the reliable broadcast of data and information from the preceding layer.
- **Support Layer:** The security architecture's third layer is this one. Establish a solid foundation for the application layer in this layer. The majority of intelligent computing power comes from the grid and cloud computing [14].
- **Application layer:** The highest layer in the security architecture is this one. This layer provides tailored services according to user requirements. The application layer facilitates consumers' access to the internet of things (IoT) via a television, mobile device, personal computer, etc.

C. Core Characteristics and Security Considerations in Iot

IoT systems are characterized with security requirements and properties that are different from the traditional computing environment. The widespread use of heterogeneous devices together with the continuous exchange of data raises serious concerns on the secure and reliable operation. Therefore, understanding the fundamental

characteristics of IoT alongside essential security requirements such as confidentiality and authentication is crucial for designing resilient and trustworthy IoT systems.

- **Independence:** Every day, the quantity of devices rises. Consequently, a lot less human engagement is required.
- **Model Training on Labeled Threat Data:** Supervised learning models learn from historical data by
- **Diversity:** More types of IoT devices work closely with the physical state and are designed for certain tasks. Their equipment, structure, and process requirements are therefore unique.
- **Confidentiality:** Privacy and confidentiality are synonymous. It ensures that the correct individuals may obtain sensitive information while preventing it from getting to the wrong persons [15]. The people who are authorized to view the data must have access.
- **Authentication:** A process that makes use of confirmation that an entity's stated attribute is accurate. Verifying that a trademark or feature that gives the appearance of being real is indeed authentic is known as authentication.

D. Security Challenges Facing Iot

The defense of Internet of Things devices against intrusions is known as IoT security. Although many company owners are aware that they must use antivirus software to secure their phones and laptops, the security concerns associated with IoT devices are less widely understood, and their protection is far too frequently disregarded.

- **Data Integrity:** Billions of devices come under the umbrella of an interlinked ecosystem that is connected through IoT[16]. Manipulating even a single data point result in manipulation of the entire data which is exchanged and shared back and forth from the sensor to the main server.
- **Encryption Capabilities:** Data encryption and decryption is a continuous process. The IoT network's sensors still lack the capability to process. Brute force attempts can be prevented by firewalls and segregating the devices into separate networks.
- **Privacy Issues:** IoT is all about the exchange of data among various platforms, devices, and consumers. The smart devices gather data for a number of reasons, like, improving efficiency and experience[17], decision making, providing better service, etc.; thus, the end point of data shall be completely secured and safeguarded.
- **Common Framework:** There is an absence of a common framework and so all the manufacturers have to manage the security and retain the privacy on their own.
- **Automation:** Eventually, enterprises have to deal with more and more number of IoT devices. This enormous amount of user data can be difficult to manage.

III. INTELLIGENT THREAT DETECTION

Intelligent Threat Detection is a state-of-the-art cybersecurity method that detects harmful activity and possible security risks by constantly monitoring system activities, network traffic, and Internet of Things (IoT) devices. Instead of using signatures, it can detect known and

unknown attacks from patterns and anomalies in real time. It promises to make IoT environments more secure, with more accurate detection, fewer false alarms, and faster threat response and mitigation.

A. Types of Intelligent Threat Detection in IoT

There are different types of detection in IoT in Intelligent threat like Anomaly-Based Detection, Signature-Based Detection, Hybrid-Based Detection and Behavior-Based Detection.

- **Anomaly-Based Detection:** A proactive method in intrusion detection systems that detects abnormal activity in the network by using the deviation from the normal behavior patterns [18]. This approach is not just based on known attack signatures; it is more about identifying irregular patterns that could be indicative of malicious activity.
- **Signature-Based Detection:** A technique for Intrusion Detection Systems that involves using a database of known attack signatures to identify malicious activity in the incoming network traffic. Each signature represents a specific threat type, with unique characteristics of that threat.
- **Hybrid-Based Detection:** The hybrid threat detection paradigm is a notable combination of rule-based and AI-based techniques, which has proven exceptionally powerful in today's cybersecurity ecosystem [19].
- **Behavioral –based Detection:** The behavior-based technique may identify more types of malwares, including ones that haven't been discovered yet. However, since it's too inclusive, it often produces false positives [20].

B. Threat Detection Framework in IoT

Data collected from monitoring tools, endpoints, servers, and routers is the first step in developing a ML threat detection system. Data that is not processed typically has irrelevant characteristics, noise, or missing values [21].

- **Data Collection Layer:** The right sensors in an IoT network may collect data and send it on. It is also possible to relay data on the sensors' operational state at the same time. The primary goals of collecting this data, which is a byproduct of sensor functioning, are security and preventative maintenance [22].
- **Data Preprocessing:** Sensor data may contain noise, missing values, outliers, and redundancy as a result of interference signals, which might cause inaccurate data transfer [23]. Data denoising, missing data imputation, data outlier identification, and data aggregation are some of the data analyzes carried out to address difficulties with data collected by Internet of Things sensors.
- **Feature Engineering:** Feature engineering seeks to optimize data representation so that models may learn important patterns with little noise and irrelevant information [24]. Statistical analysis, computational methods, and domain knowledge are all necessary for this procedure.

C. Datasets Used for Intelligent Threat Detection

Datasets play a crucial role in the development and evaluation of intelligent threat detection systems by providing realistic network traffic and attack scenarios for analysis. They contain both normal and malicious activities, enabling

researchers to assess the effectiveness of threat detection techniques. Publicly available datasets also facilitate performance comparison using standardized benchmarks.

1) KDD Cup 99

The DARPA KDD'99 data set was developed in 1999 utilizing the 1998 dataset, which contained recorded network traffic. For each network connection, it is being pre-processed into 41 features. Types of features found in the KDD'99 dataset are as follows: Basic Features (#1–#9), Content Features (#10–#22), Time based features (#23–#31), and host based features (#32–#41).

2) NSL-KDD

One solution to the problems with the KDD Cup data set is the NSL-KDD dataset, which is based on a subset of the whole KDD Cup'99 dataset [25]. The train set is free of irrelevant records, allowing classifiers to be objective and not favor records with a higher frequency of occurrence.

3) UNSW-NB15

It has 49 characteristics, a range of normal and attacked activities, and a total of 25,40,044 records with class labels, including current attacks. Of the entire number of records, 3,21,283 have been attacked while 2,21,876 have been normal. There are six major types of features in the UNSW-NB15 dataset: basic, flow, time, content, additional generated, and labeled.

4) CICIDS2017

The data set consists of eight distinct sessions that were recorded over the course of five days. After that, the data was extracted into eight separate files, each representing a single session. These files were then prepared for use in ML research using the Comma Separated Values (.csv) format [26].

5) ToN-IoT

The goal of the ToN-IoT dataset is to compile and evaluate IIoT and IoT mixed data sources. It includes heterogeneous data gathered from many sources, such as system network traffic, Windows and Linux system logs, and telemetry data from linked devices [27]. Realistic network components make up the Internet of things.

IV. ARTIFICIAL INTELLIGENCE TECHNIQUES FOR THREAT DETECTION

Detecting, analyzing, and mitigating cyber risks in IoT settings is automated by Intelligent Threat Detection, which uses ML and DL algorithms. Intelligent threat detection is able to see unusual activity and identify both known and unknown threats instantly, in contrast to conventional security systems that depend on predetermined parameters or signatures. These data-driven strategies improve the precision, flexibility, and efficacy of IoT security while decreasing the amount of time needed to respond to ever-changing cyber dangers.

AI encompasses a broad range of techniques, including ML, Federated Learning, and DL, designed to enable systems to simulate human-like cognitive functions.

A. Federated Learning

Dealing with privacy, suggested a federated learning framework was suggested that can catch anomalies in IoT networks. Training was possible on many separate edge devices together, and data never had to be moved to a central server[28]. As a result, users privacy remained protected while security threats could be found on several devices.

Nonetheless, using federated learning meant extra computational and data transfer, which made it difficult to apply in scenarios where these resources were low.

B. Machine Learning

This study's proposed model is a typical large enterprise or smart city facing a growing number of cyber risks related to the Internet of Things (IoT). For example, these organizations are being targeted by massive botnets like Mirai, which take advantage of weak or default passwords [29].

There are six main approaches in ML:

- **Supervised learning:** This is where the data has to be tagged, much like when gives a model a bunch of sample files to see if they include malware. The tagging of the data might help the model decide on more data [30]. Also known as the task-driven approach.
- **Ensemble learning:** It combines many models to solve a problem by adding label data, similar to supervised learning.
- **Unsupervised learning:** This kind of learning makes use of unlabeled data and has the model automatically classify it according to the qualities of the data. It typically detects outliers in the dataset and is hence thought of as the more powerful of the two [31]. A similar term for this strategy is the data-driven method.
- **Semi-supervised learning:** It makes an effort to merge supervised and unsupervised methods in data sets that contain labeled data [32].
- **Reinforcement learning:** This method is best used to dynamic settings. It is also known as a strategy that is driven by the environment [33].
- **Active learning:** In terms of how it adapts to new circumstances, it's very much like having a teacher at side. It belongs to the RLS family of algorithms [34].

C. Attack Detection Using ML Methods

Cybersecurity's spam filter distinguishes spam from various communication services. It would appear that spam is the most popular ML strategy used for information security. Classification is a common use of the supervised learning labeled data approach. Results were compared between Gradient Boosted DT, SVM, and RF classifications in the investigation.

1) Support Vector Machine (SVM):

There is no more well-known or well-liked method than this one. Although it has some regression capabilities, its primary application is in classification techniques. Points in an n-dimensional region, where n is the number of features being examined, are used to draw data items in support vector machines (SVMs) [35]. It makes a hyper plane and sorts the information into categories.

2) Gradient Boosted Decision Tree (GBDT):

GBDT consists of a group of DTs. The boosting approach is used by GBDT, an ML algorithm, to create susceptible DTs. It is necessary to train the algorithms on several samples in order to construct the tree ensemble. It is not possible to teach them with only one set, unfortunately.

3) Random Forest (RF):

The random subspace and bagging algorithms used by RF are based on CART DTs. It works on both regression and classification[36]. The education is achieved in parallel. It

injects randomness within the learning (testing and training), a process in which each tree isn't the same with the others.

D. Deep Learning

Automatically learning complicated patterns and representations from massive amounts of data is the goal of DL, a subfield of ML that employs multi-layered artificial neural networks. Anomaly detection, intelligent threat identification, intrusion detection, malware classification [37], and other IoT security tasks frequently employ DL models, which frequently outperform more conventional ML approaches.

1) Convolutional Neural Network (CNN)

It is an ANN deep feed forward collection used for analyzing visual imaging (not recurrent). These networks consist of neurons with weights and perceptions that can be learned. Each neuron has those inputs, and then they carry out a dot product. A CNN embraces the two-dimensional entrance as a picture or a voice sign and creates features via a secret layer chain.

2) Recurrent Neural Networks (RNN)

A neuron like node network is made up of subsequent layers[38]. In the following sequential sheet of each node, the soil cover designation, the estimate of crop production, the climate forecast, the calculation of soil humidity, animal science, in addition to others, are all linked with a single side-linking node in several agricultural regions.

3) Long Short-Term Memory (LSTM)

This is the most effective method of various algorithms. This can handle individual data sources as well as entire data sequences. This can be classified and predicted based on time series results. It is utilized for product classification, crop yield prediction, and weather forecast in agricultural applications.

Table I summarizes major AI-based threat detection techniques in IoT security, comparing ML and DL approaches by learning type, algorithms, targeted threats, advantages, and limitations. It highlights that advanced AI methods improve detection accuracy and efficiency for known and unknown attacks.

TABLE I. INTELLIGENT THREAT DETECTION TECHNIQUES IN IOT SECURITY

Technique	Learning Type	Common Algorithms/Models	IoT Threats Detected	Advantages	Limitations
Supervised Learning; Unsupervised Learning; Semi-Supervised Learning	Labeled data; Unlabeled data; Small labeled + large unlabeled datasets	Decision Tree, Random Forest, SVM, KNN, Naïve Bayes; K-Means, DBSCAN, Isolation Forest, One-Class SVM; Semi-Supervised SVM, Label Propagation, Self-Training	DDoS attacks, malware, intrusion, botnets; unknown attacks, anomalies, insider threats; intrusion detection, anomaly detection	High detection accuracy with quality datasets; detects zero-day and unknown attacks without labeled data; reduces labeling cost and improves learning from limited data	Requires large labeled datasets and performs poorly on unseen attacks; higher false-positive rate and difficult cluster interpretation; sensitive to incorrect pseudo-labels and moderate complexity
Reinforcement Learning (RL)	Reward-based learning	Q-Learning, Deep Q-Network (DQN), SARSA	Dynamic attack mitigation, adaptive security	Learns optimal defense strategies; adapts to changing environments	Long training time; computationally expensive
Convolutional Neural Network (CNN); Recurrent Neural Network (RNN); Long Short-Term Memory (LSTM)	Deep Learning	CNN, 1D-CNN, CNN-LSTM; RNN, GRU; LSTM, Bi-LSTM	Malware detection, traffic classification, intrusion detection; sequential attack detection, network traffic analysis; DDoS detection, anomaly detection, botnet detection	Automatically extracts spatial features and provides high accuracy; captures temporal dependencies; effective for long-term sequential patterns and high detection performance	Requires large datasets and high computational resources; suffers from vanishing gradient problems; high memory and training requirements
Autoencoder	Deep Learning	Sparse Autoencoder, Variational Autoencoder	Anomaly detection, unknown attack detection	Learns normal behavior without labels; effective for anomaly detection	Reconstruction errors may increase false alarms
Graph Neural Network (GNN)	Deep Learning	GCN, GraphSAGE, GAT	Botnet detection, network intrusion, attack propagation	Captures relationships among IoT devices; suitable for network graphs	Complex graph construction; computational overhead
Transformer Models	Deep Learning	Transformer, BERT, Vision Transformer (ViT)	Advanced malware detection, intrusion detection, traffic analysis	Learns long-range dependencies; scalable for large datasets	High computational and memory requirements
Hybrid AI Models	Combined Learning	CNN-LSTM, CNN-GRU, RF-XGBoost, Ensemble Learning	Multiple cyber threats	Improved accuracy and robustness; combines strengths of multiple models	Increased model complexity and training time
Explainable AI (XAI)	Model Interpretation	SHAP, LIME, Grad-CAM	Supports all AI-based detection systems	Improves transparency, trust, and regulatory compliance	Additional computational overhead; explanations may vary

V. LITERATURE REVIEW

This section highlights related studies on Current Perspectives on Internet of Things Security and Intelligent Threat Detection, showcasing their roles in Internet of Things Security, enhancing threat detection in IoT.

X. Cheng and Y. Fan (2026) FL has promise for IoT problems since it allows collaborative model training without direct data exchange. However, heterogeneous IoT devices cause feature shifts across clients, degrading FL performance. To tackle this, FedTAN employs an agile normalization scheme for the Transformer, along with a dynamic Tanh

(DyT) activation function, to minimize feature shifts, communication overhead, and maintain model efficacy [39].

K. N., S. E., M. Agoramoorthy, *et al.* (2026) introduce the concept of a security model for IoT using federated learning and real-time anomaly detection. Preserving data confidentiality, the IoT devices locally update the anomaly detection models, sending only updates to the central server. Experimental results show accurate detection of atypical behavior, fewer false positive detections and lower communication requirements compared to centralized learning. The approach offers a comprehensive, privacy-oriented, and flexible solution for securing medical, industrial, and smart city IoT environments [40].

A. Nejari *et al.* (2025) conduct an in-depth study and review of recent research in IoT security using artificial intelligence, with an emphasis on using IDS and AI techniques to detect and counter cyberattacks. It uses accuracy, precision, recall and F1-score to assess its strengths and weaknesses. Results indicate that hybrid learning strategies and autoencoders can be used together to enhance IoT security. Adaptive and lightweight AI models for IoT security are worthy of future research [41].

S. S. Ajmire, *et al.* (2025) proposes a hybrid approach that combines ML and DL models to identify and categorize cyber threats in an IoT context. The framework integrates anomaly detection and classification sub systems to obtain a better identification of known and unknown attacks. The hybrid model outperforms traditional models in terms of accuracy, precision, and recall, as shown in experiments with

benchmark datasets like UNSW-NB15 and BoT-IoT. The proposed framework provide a base to develop adaptive, real-time, and scalable IoT security mechanisms [42].

A. Upadhyay *et al.* (2024) Protecting the safety and reliability of IoT networks requires the ability to identify and counteract potential dangers. The sheer number and complexity of contemporary assaults frequently overwhelms conventional approaches to identifying and countering IoT security risks. Using four different ML algorithms—DT, RF, MLP, and NB—this study presents a detection method for IoT networks. Overfitting, increased computing time, and reduced ML model quality are some of the issues that arise when using ML approaches to data with high dimensions. As a result, PCA has been employed to lower the dataset's dimensionality in this case. The NSL-KDD datasets are used for training and evaluation of the proposed ML algorithms [43].

M. R. Joel, G. Manikandan, and G. Bhuvaneswari, *et al.* (2023) The IoT introduces security risks due to the fact that every item in the system has its own unique identity and sends data automatically via the network. Using AUC, F1-score, recall, precision, and accuracy as evaluation metrics, this article provides an overview of approaches to IoT data security. The accuracy of ML algorithms like DT, RF and ANN were measured as 99.4%, where RF yielded higher accuracy [44].

Table II shows an overview of the existing IoT security research, the identified key findings, the limitations found, and future directions in intelligent threat detection for federated learning, AI, ML, and hybrid approaches.

TABLE II. CURRENT PERSPECTIVES ON INTERNET OF THINGS SECURITY AND INTELLIGENT THREAT DETECTION

Reference	Study Focus	Approach / Methodology	Key Findings	Challenges / Limitations	Future Directions
X. Cheng and Y. Fan,(2026)	Federated learning for IoT security	Proposed FedTAN, a transformer-based federated learning framework with Dynamic Tanh (DyT) activation to mitigate feature shift in non-IID IoT data	Improves federated learning performance, reduces communication overhead, and effectively handles heterogeneous IoT data	Feature shift across clients; normalization complexity; performance under highly heterogeneous environments	Develop adaptive normalization strategies and scalable federated transformer models for large-scale IoT networks
K. N, S. E, M. Agoramoorthy, et al. (2026)	Federated learning-based IoT security	Distributed federated learning with real-time anomaly detection using locally trained models	Preserves data privacy, reduces false positives, minimizes communication cost, and improves anomaly detection accuracy	Depends on communication efficiency and synchronization among distributed devices	Enhance privacy-preserving federated learning and adaptive threat detection for large-scale IoT applications
A. Nejari et al. (2025)	AI-driven IoT security review	Comprehensive review of Intrusion Detection Systems (IDS) and AI-based security techniques using performance metrics	Autoencoders and hybrid learning approaches improve IoT security and attack detection performance	Lightweight deployment, computational complexity, and adaptability remain challenging	Design lightweight, adaptive, and explainable AI models for IoT security
S. S. Ajmire et al. (2025)	Hybrid ML–DL framework for IoT security	Hybrid framework integrating ML and DL with anomaly detection and classification using UNSW-NB15 and BoT-IoT datasets	Achieved higher accuracy, precision, and recall than conventional models; effectively detected known and unknown attacks	Increased model complexity and computational requirements	Develop adaptive, scalable, and real-time hybrid security frameworks for IoT
A. Upadhyay, et al. (2024)	IoT threat detection using Machine Learning	PCA-based feature reduction with Decision Tree (DT), Random Forest (RF), Multilayer Perceptron (MLP), and Naïve Bayes (NB) on the NSL-KDD dataset	PCA improves detection accuracy; Naïve Bayes and MLP achieved superior performance for IoT threat detection	High-dimensional datasets may cause overfitting and increase computational cost	Develop more efficient feature selection and lightweight ML models for real-time IoT security
M. R. Joel, G. Manikandan, and G. Bhuvaneswari, (2023)	Survey of IoT security techniques	Comparative survey of IoT security methods using ML algorithms (DT, RF, ANN) and evaluation metrics (Accuracy, Precision, Recall, F1-score, AUC)	Random Forest achieved the best detection performance with approximately 99.4% accuracy	Existing methods require improved scalability and robustness against evolving cyber threats	Develop intelligent, scalable, and real-time IoT security frameworks with enhanced threat detection capabilities

VI. CONCLUSION AND FUTURE WORK

The IoT is increasingly a key component of contemporary digital infrastructure, linking various devices and allowing intelligent services to be provided in a number of application areas. Enabling connectivity, however, also poses a major security threat and demands sophisticated and adaptive threat detection mechanisms. This review covered the underlying principles of IoT security, architectures, security challenges, threat detection frameworks, datasets, and AI-driven techniques for threat detection. The results show that ML, DL, hybrid AI, and federated learning can offer more accurate, adaptive and intelligent security to help detect known and unknown cyber threats. Moreover, Random Forest, SVM, CNN, LSTM and hybrid models have shown promising results for the IoT threat detection, and federated learning also enables privacy-preserving threat detection. However, there are still issues of data quality, device diversity, compute limitations, communication overheads, scalability, and false-positive alerts. In conclusion, the use of AI-based solutions in an intelligent way offers a solid basis for the creation of secure, reliable, scalable, and adaptive IoT environments.

Lightweight, adaptive, and explainable AI models for resource constrained IoT devices is an important area of further research. Further research is needed to assess the scalability, data privacy, computational efficiency, and detection of evolving and unknown attacks in federated learning, real-time detection, standardized datasets, hybrid approaches, and efficient feature selection.

- **Funding:** This research received no external funding.
- **Institutional Review Board Statement:** Not applicable.
- **Informed Consent Statement:** Not applicable.
- **Data Availability Statement:** The data supporting the findings of this study are available from the corresponding author upon reasonable request.
- **Conflicts of Interest:** The author declares no conflict of interest.

How to cite this article:

P. S. Rathore, "Current Perspectives on Internet of Things Security and Intelligent Threat Detection," *Journal of Global Research in Electronics and Communication*, vol. 2, no. 8, pp. 08–15, Aug. 2026, Doi: xxxxxx

REFERENCES

- [1] V. Chaturvedi, R. Narra, and S. K. Chintagunta, *Applied AI Engineering for Developers: Building Intelligent Applications at Scale*. WISSIRA RESEARCH LAB, 2026.
- [2] H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, "A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories," *Computers*, vol. 14, no. 2, 2025, doi: 10.3390/computers14020061.
- [3] S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York City, NY, USA: IEEE, 2025, pp. 1–6, November, December. doi: 10.1109/CSCloud66326.2025.00055.
- [4] M. Moucharraf, M. Ridouani, F. Salahdine, and N. Kaabouch, "IoT Security: A Comprehensive Review of Architectures, Threat Models, Detection Methods, and Countermeasures," *Futur. Internet*, vol. 18, no. 5, pp. 1–31, 2026, doi: 10.3390/fi18050266.
- [5] N. Karra and N. Karra, "Priority-Aware Heuristic Load Balancing Framework for IoT Applications in Fog-Cloud Environments," in *2025 International Conference on Intelligent & Innovative Practices in Engineering & Management (IIPeM)*, Singapore, Singapore: IEEE, 2025, pp. 1–6, November. doi: 10.1109/IIPeM65914.2025.11548242.
- [6] M. A. Gilbert, "AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities International Journal of Research Publication and Reviews AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and V," vol. 5, no. November, pp. 219–236, 2024.
- [7] V. K. Sharma, "AI-Driven Spectrum Management for 6G Radio: Cognitive and Self-Optimizing Wireless Networks," in *2026 4th International Conference on Inventive Computing and Informatics (ICICI)*, Bangalore, India: IEEE, 2026, pp. 611–617, June. doi: 10.1109/ICICI68773.2026.11580613.
- [8] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, "Things Network Anomaly Detection — Current Research Trends," 2024.
- [9] S. Remella, J. Ligam, U. K. R. Gangula, V. Sannamuri, R. Ganta, and Q. T. Sadat, "End-to-End Cloud Procurement Lifecycle Automation," in *2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT)*, Belagavi, India: IEEE, 2025, pp. 1–8. doi: 10.1109/ICAFT66710.2025.11452870.
- [10] A. Nimodiya and S. Ajankar, "A Review on Internet of Things," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 135–144, 2022, doi: 10.48175/IJARSC-2251.
- [11] R. Palwe, "Three Layers of Trust in AI Interfaces: Interface, Behavior, and Organization," *Int. J. Sci. Res.*, vol. 15, no. 1, pp. 1152–1160, Jan, 2026.
- [12] A. Dauda, O. Flauzac, and F. Nolot, "A Survey on IoT Application Architectures," *Sensors*, vol. 24, no. 16, 2024, doi: 10.3390/s24165320.
- [13] R. K. Thakur and R. K. Tiwari, "Security on Iot: a Review," *Int. J. Electron. Eng. Appl.*, vol. VIII, no. II, p. 40, 2020, doi: 10.30696/ijeea.viii.ii.2020.40-48.
- [14] M. Beyene and K. R. Shekar, "Performance Analysis of Homomorphic Cryptosystem on Data Security in Cloud Computing," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India: IEEE, 2019, pp. 1–7, July. doi: 10.1109/ICCCNT45670.2019.8944837.
- [15] K. Shaikat, T. Mahboob Alam, I. Hameed, W. Khan, N. Abbas, and S. Luo, "A Review on Security Challenges in Internet of Things (IoT)," 2021. doi: 10.23919/ICAC50006.2021.9594183.
- [16] M. Kumar and R. K. Saini, "Internet of Things (IoT) Applications and Security Challenges: A Review," *SSRN Electron. J.*, vol. 7, no. 12, pp. 1–7, 2024, doi: 10.2139/ssrn.4903947.
- [17] R. Palwe, "The Role of User Experience Design in Advancing Digital Sustainability," *Int. J. Sci. Res.*, vol. 14, no. 10, October, pp. 1168–1176, 2025, doi: 10.21275/SR251021070714.
- [18] W. Olabiya, A. Chole, and Y. Themmah, "Signature-Based vs. Anomaly-Based Detection," 2023.
- [19] I. A. Shaik, "Hybrid Threat Detection Systems: A Synergistic Approach to Modern Cybersecurity," *Eur. J. Comput. Sci. Inf. Technol.*, vol. 13, no. 43, pp. 62–69, 2025, doi: 10.37745/ejcsit.2013/vol13n436269.
- [20] M. Abosaeeda and M. Mansour, "A Malware Detection and Classification using Neural Networks: A Review," vol. 2, pp. 64–90, 2025.
- [21] M. A. A. Faiz, M. Phil, and R. S. Julia, "Intelligent Threat Detection," *IRJEdT Int. Res. J. Educ. Technol. Peer Rev. J.*, vol. 09, no. 03, pp. 2581–7795, 2026.
- [22] A. A. Abba Ari et al., "Data collection in IoT networks: Architecture, solutions, protocols and challenges," *IET Wirel. Sens. Syst.*, vol. 14, no. 4, pp. 85–110, 2024, doi: 10.1049/wss2.12080.
- [23] R. Krishnamurthi, A. Kumar, D. Gopinathan, A. Nayyar, and B. Qureshi, "An overview of iot sensor data processing, fusion, and analysis techniques," *Sensors (Switzerland)*, vol. 20, no. 21, pp. 1–23, 2020, doi: 10.3390/s20216076.
- [24] B. Brown, D. Clever, and S. Gabriel, "Feature Engineering Techniques for Enhancing AI Accuracy," 2024.
- [25] S. Choudhary and N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," *Procedia Comput. Sci.*, vol. 167, pp. 1561–1573, 2020, doi: 10.1016/j.procs.2020.03.367.

- [26] Z. I. Khan, M. M. Afzal, and K. N. Shamsi, "A Comprehensive Study on CIC-IDS2017 Dataset for Intrusion Detection Systems," *Int. Res. J. Adv. Eng. Hub*, vol. 2, no. 02, pp. 254–260, Feb. 2024, doi: 10.47392/IRJAEH.2024.0041.
- [27] I. Tareq, B. M. Elbagoury, S. El-Regaily, and E.-S. M. El-Horbaty, "Analysis of ToN-IoT, UNW-NB15, and Edge-IIoT Datasets Using DL in Cybersecurity for IoT," *Appl. Sci.*, vol. 12, no. 19, p. 9572, Sep. 2022, doi: 10.3390/app12199572.
- [28] M. R. Mohammed, "AI-Driven Threat Detection in IoT Environments Using Adaptive Cybersecurity Frameworks," *Int. J. Comput. Sci. Eng. Innov.*, vol. 1, pp. 1–8, 2025, doi: 10.64137/31079458/IJCSEI-V1I1P101.
- [29] M. Anwer, M. Umer, S. M. Khan, and Waseemullah, "Attack Detection in IoT using Machine Learning," *Eng. Technol. Appl. Sci. Res.*, vol. 11, no. 3, pp. 7273–7278, 2021, doi: 10.48084/etasr.4202.
- [30] M. Hasan, M. M. Islam, I. Islam, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," 2019. doi: 10.1016/j.iot.2019.100059.
- [31] A. Haldorai, A. Ramu, and M. Suriya, *Organization Internet of Things (IoTs): Supervised, Unsupervised, and Reinforcement Learning*. 2020. doi: 10.1007/978-3-030-44407-5_2.
- [32] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," 2018, doi: 10.1016/j.asoc.2018.05.049.
- [33] M. Lopez-Martin, B. Carro, and A. Sanchez-Esguevillas, "Application of deep reinforcement learning to intrusion detection for supervised problems," *Expert Syst. Appl.*, vol. 141, no. 6, pp. 112963, September, 2020, doi: 10.1016/j.eswa.2019.112963.
- [34] K. Yang, J. Ren, Y. Zhu, and W. Zhang, "Active Learning for Wireless IoT Intrusion Detection," *IEEE*, 2018, pp. 19–25, December. doi: 10.1109/MWC.2017.1800079.
- [35] B. S. Bhati and C. S. Rai, "Analysis of Support Vector Machine-based Intrusion Detection Techniques," 2020, doi: 10.1007/s13369-019-03970-z.
- [36] M. Bin Farukee, M. S. Z. Shabit, M. R. Haque, and A. H. M. S. Sattar, *DDoS Attack Detection in IoT Networks Using Deep Learning Models Combined with Random Forest as Feature Selector*. 2021. doi: 10.1007/978-981-33-6835-4_8.
- [37] S. Chatterjee, "Advanced Malware Detection in Operational Technology: Signature-Based Vs. Behaviour-Based Approaches," *ESP J. Eng. Technol. Adv.*, vol. 1, no. 1, pp. 272–279, 2021, doi: 10.56472/25832646/JETA-V1I2P128.
- [38] S. Askar, C. Mohammed, and S. Kareem, "Deep Learning in IoT systems: A Review," 2021, doi: 10.5281/zenodo.5221646.
- [39] X. Cheng and Y. Fan, "FedTAN: Federated Learning in Internet of Things Data via Transformer With Agile Normalization," *IEEE Internet Things J.*, vol. 13, no. 10, pp. 20021–20031, 2026, doi: 10.1109/JIOT.2026.3655168.
- [40] K. N. S. E. M. Agoramorthy, K. V. Kanimozhi, L. A. and K. V. Bhaskar, "Securing IoT Devices Using Federated Learning and Anomaly Detection for Cyber Threat Prevention," in *2026 8th International Conference on Intelligent Sustainable Systems (ICISS)*, 2026, pp. 265–271. doi: 10.1109/ICISS67859.2026.11453976.
- [41] A. Nejari, A. Badaoui, A. Elmounadi, and N. Berbiche, "AI-Driven IoT Security: A Comprehensive Review on Current Trends and Future Perspectives," in *2025 International Conference on Circuit, Systems and Communication (ICCS)*, 2025, pp. 1–6. doi: 10.1109/ICCS66714.2025.11135299.
- [42] S. S. Ajmire, A. Wankhade, K. V. Agarkar, S. Thakare, and K. K. Shahale, "Towards Robust IoT Security: An ML and DL-Based Threat Detection Framework," in *2025 2nd International Conference on Integration of Computational Intelligent System (ICICIS)*, 2025, pp. 1–4. doi: 10.1109/ICICIS65613.2025.11371028.
- [43] A. Upadhyay, P. Agarwal, S. Naaz, and V. Thakur, "Improving IoT Threat Detection through Machine Learning using PCA for Dimensionality Reduction," in *2024 International Conference on Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA)*, 2024, pp. 1–6. doi: 10.1109/ARIIA63345.2024.11051572.
- [44] M. R. Joel, G. Manikandan, and G. Bhuvaneswari, "An Analysis of Security Challenges in Internet of Things (IoT) based Smart Homes," in *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, 2023, pp. 490–497. doi: 10.1109/ICEARS56392.2023.10085106.