International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

CYCYBER SECURITY FRAMEWORK FOR CLOUD DATA MANAGEMENT BASED ON THE INTERNET OF THINGS

***Vijayalaxmi Kadrolli[1] , Nethravathi. B [2], Rashmi Amardeep [3], Chitra. AD [4], Narendra Kumar. A [5], Sivaganesan. D [6], Muthulakshmi. V [7], Savitha. P. B [8]**

[1]Associate Professor, Department of Information Technology, Terna Engineering College, Nerul, Navi Mumbai, Maharashtra, India, udachanv@gmail.com

[2] Associate Professor, Department of Information Science and Engineering, JSS Academy of Technical Education, Bengaluru, Karnataka, India, nethravathi.sai@gmail.com

[3]Associate Professor, Department of Information Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bengaluru, Karnataka, India, rashmiamardeep@gmail.com

[4]Assistant Professor, Department of Computing – Software Systems, Coimbatore Institute of Technology, Coimbatore, Tamilnadu, India, dchitra@cit.edu.in

[5]Associate Professor, Department of Biomedical Engineering, Sethu Institute of Technology, Virudhunagar, Tamilnadu, India, nandhume@gmail.com

[6]Professor, Department of Computer Science and Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi, Tamilnadu, India, sivaganesand@gmail.com

[7]Professor, Department of Computer Science and Engineering, St. Joseph's College of Engineering, OMR Chennai, Tamilnadu, India, muthulakshmiv@stjosephs.ac.in

[8]Associate Professor, Department of Electrical and Electronics Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India, pbscvc@gmail.com

Abstract

The Internet of Things represents a model of networking where physical device, digital, and virtual objects possess thecapabilities for identifying, detecting, networking, gathering, and processing to communicate with one other and exchange data over the internet, thereby allowing them to execute tasks as dictated by users. Numerous IoT applications aim to increase convenience and enhance the quality of human life. Nevertheless, IoT services frequently manage sensitive user information, which may be targeted by malicious or unauthorized service providers. Conventional security protocols are insufficient to shield these data-intensive devices from diverse forms of attacks. Alongside refining current techniques, an additional security layer, like an Intrusion Detection System , has been shown to be beneficial in numerous cases. Nonetheless, standard Intrusion Detection System methodologies are not adequately prepared to

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

confront the rising danger of zero-day attacks. To address this issue, we present IoTPredictor, a sophisticated security strategy focused on effectively forecasting and identifying malicious behavior in IoT devices. To evaluate the success of IoTPredictor, we carry out a range of experiments and present a detailed analysis. The findings underscore the robustness and effectiveness of the security framework we have proposed in identifying and mitigating malicious threats.

Keyword: IoT, Intrusion Detection System, IoTPredictor, Security.

Introduction

A recently introduced concept called the Internet of Things (IoT) has emerged and is considered a major development of the next phase of internet technology.The Internet of Things is changing the real world. Billions of intelligent objects around the world leadsensed data about the environmental changes and report them. IoT distortions include everyday objects similar to boxes, buses and shoes that were not traditionally considered computer distortions. By 2030, 2022, the globally associated IoT would increase from 14.6 billion to 30.2 billion. This IoT network has expanded the need for cybersecurity beyond the field of information security to the field of physical security. This is due to the fact that IoT tension includes land that interacts with physical aspects and affects the impediments of IoT bias that can affect physical security and security.

Over time, advancements in RFID technology, sensors, actuators, wireless mobile communication, embedded systems, and cloud computing have allowed IoT technologies to offer numerous possibilities and lead to the creation of applications centered around the Internet network. This article presents IoTPredictor. This is a security framework that predicts the behavior of IoT devices in a FOG computing environment. The system uses predictive analytics to actively recognize anomalous activity. Its three-layer architecture and the overall distribution of components are shown in Fig. 1. IoTPredictors placed in the fog layer promote early detection of attacks and hope for IoT devices to work.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

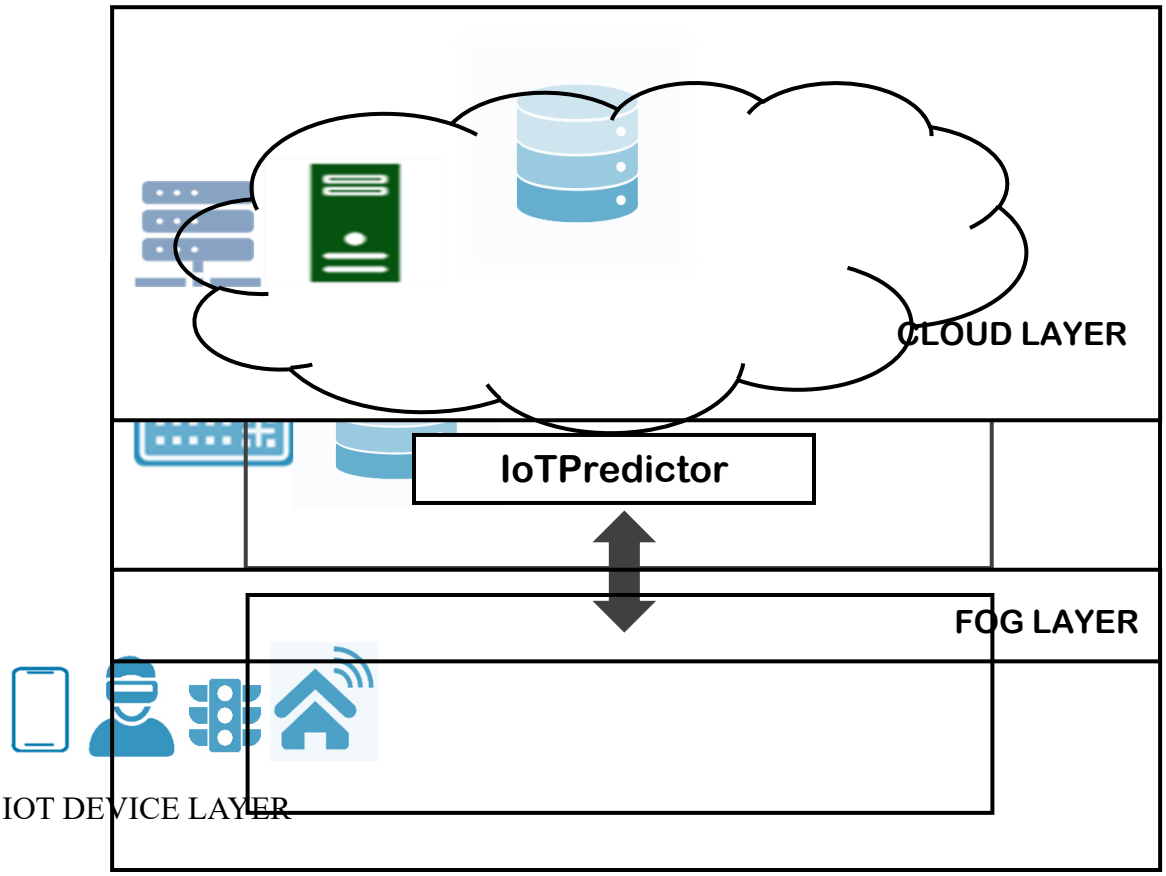


Fig. 1 Three layer of IoTPredictor framework

Related Work

There are variety of techniques proposed to tackle these challenges, each having advantages and disadvantages.

Makhdoom et al. (2023) provide a thorough evaluationof present techniques for identifying breachesIoT devices. The work interviews both active (behavioral integrity verification) and passive authentication ways, highlighting existing barriersand suggesting how to create Formulate standardized, secure, affordable, and trustworthy strategies for IoT device protocols. IoT devices are also increasingly susceptible to numerous attacksacross multiple applications.

Pajouh et al. represent anintrusion detection model employing a two-layer feature reduction and dual-classification mechanism. This model is also designed to flag harmful threatsmovements as an exampleusers, corney (U2R) and local (R2L) attacks. In order to reduce the measurement, analysis of linear identification and component have been implemented. I have done the entire

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

experiment using NSL-KDD data. In order to identify suspicious behavior in two levels of the classification module, the reliability of naive bays and K-Nearest-Schedul was applied.

Diro et al. reviewed the detection of attack using fog-to-things architecture. The authors of this paper described a comparative study of deep, flat neuronal networks using open source data records. The central focus of this study was to recognize four distinct attacks and anomaly classes. In four classes, the system received 98.27% accuracy in theadvanced deep neural network model and 96.75% accuracy in the model of flat neural network.According to Rachna et al. (2015), the migration of data to the cloud has made cloud

computing the main engine of many enterprises. The information that needs transmission cannot be outsourced without first being decrypted which is a fundamental drawback of the first security layer under which cloud computing might benefit from cryptography, i.e. secure storage. Implementation of unique architecture for safe data access in a cloud context. At this point, safety is taken into consideration for that only data owners must be able to encrypt and decrypt transaction. Additionally, users should be given access to their access rights.Utilizing the multi-cloud idea improves security.

Tian et al., 2024, Tian et al., 2022, Tian et al., 2021 delve into the challenges posed by adversarial and false data injection attacks on deep learning models. These studies underline the importance of developing resistance models that can withstand such attacks. Furthermore, Grammatics et al. We introduced extenensive security frameworkssuch as Speer and SDN Microsense. It integrates different elements to safeguard the smart grid against possible dangers and increase overall security measures. Both systems emphasize how advanced technologies are key to addressing the complex safety concerns in modern smart grids.

Contribution of this work

This paper provides an introduction toa strongarchitecture security for IoT device, called IoTPredictor. The greatestinvolvement of this work are as follows:

1. **IDS classification at the Fog Layer**: We introduce an innovative classified IDS framework at the fog layer, which facilitates the early exploration and avoid the attacks, reducing their potential to spread across the larger network. This method differs from conventional centralized IDS systems, improving **performance and adaptability.**
2. **Predicting the Behavior of IoT device using HMM**: We present various types of Internet of Things device and also predicting their statesutilizinga Hidden Markov Model (HMM). Our method features an algorithm that estimates probabilities for predicting future states, which is essential for implementing forward-thinkingsecurity strategies.
3. **Extensive Framework of IoTPredictor** This is applicable with IoTPredictor framework, a total system to predict the optimal solution of IoT device. By utilizing IoT

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

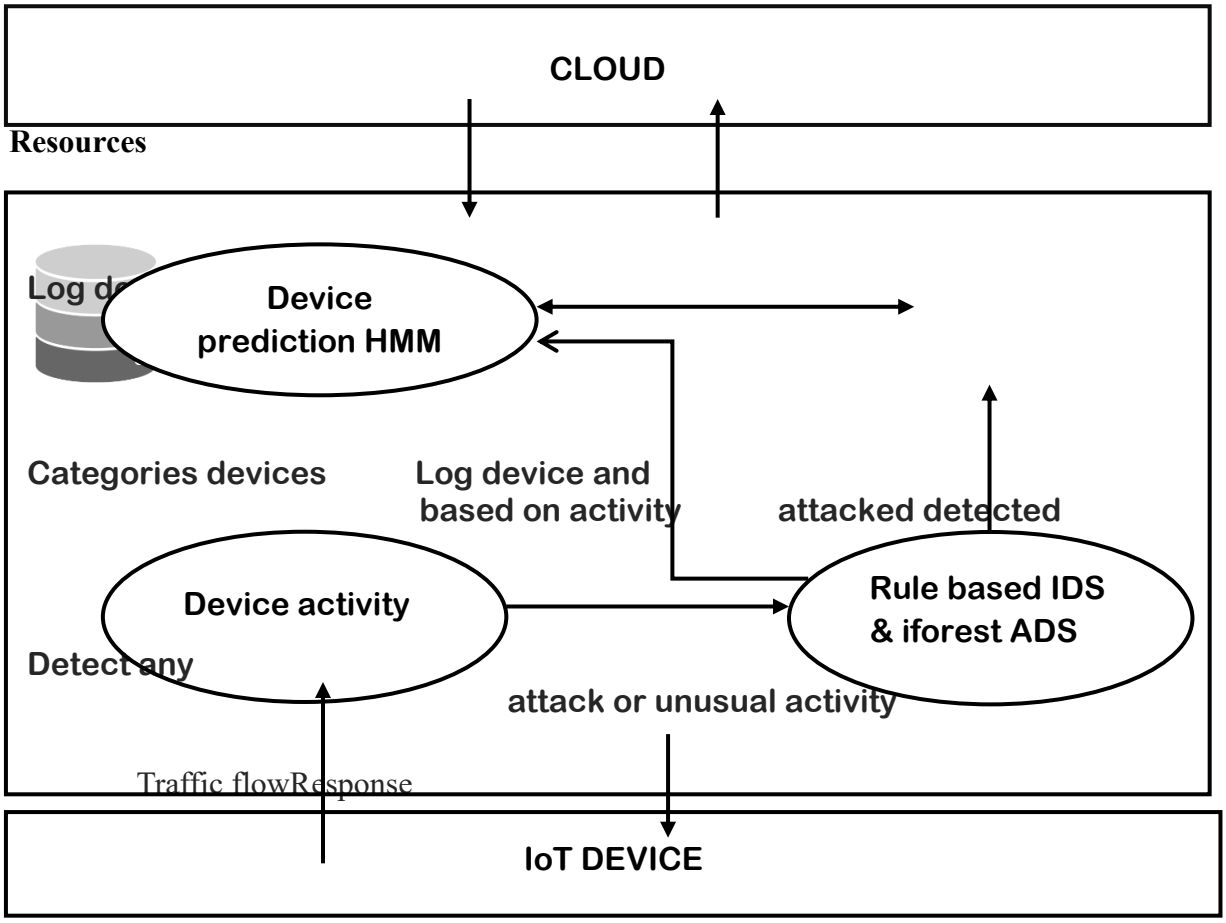
data to provide actionable insights and predictions, this framework facilitates industries in improving operational efficacy, minimizing costs, and enhancing system performance.

4. **Network Security Assessmentand Packet Modification**: Here we utilizeScapy, a popular Python library tool for security analysis, to create authenticsecurity breach scenariosand modify packets. This hands-on approach assures that our IDS and HMM Forecasting model are thoroughly validated andapprovedacross various stage.
5. **Effective illustration of fog-layerpositioning**: We showcase the efficacyof placing framework components at the fog level as opposed to atotallycentralized Strategy in the cloud layer. We present evidence showing that our system improves the speed of Identification, system scalability, and security in general.

The following is a summary of the remaining portion of this paper: The introduction and related works were found in Sections 1 and 2, the suggested approach is explained in more detail in Section 3, the simulation results are shown in Section 4, and conclusion and future research possibilities are discussed in Section 5.

Proposed Work

This partProvides an in-depth overview of the architectureand Description of our proposedframework of IoTPredictor.



Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

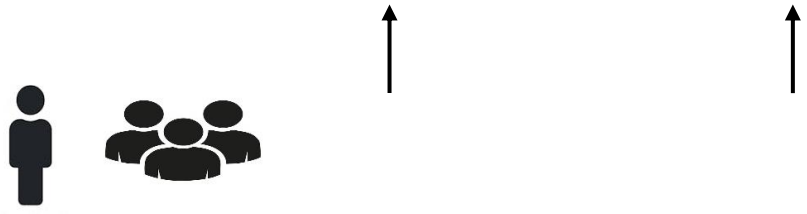


Fig.2 proposed IoTPredictor framework

Fig. 2 depicts the various components and communication flow of the proposed framework. At first, theobtained traffic is acquired by IoT devices, and their actions are observed. Thenthis IDS is a used for checking about the traffic either it would be for possible invasion or a unusual behavior. After the IDS checks device usage, the tool are categorized using an HMM based on the IDS findings. The results from both the IDS and HMM predictions are recorded in a storage system for subsequent steps at the fog stage, including future expectation.

This procedure is carried out again for recent requests or traffic generated by IoT device. The IDS is deployed to identify and stop attacks before anything happen at the fog level, preventing this distributionacross the network. This ensures the security of another element at both the fog and cloud levels. After the identification of a GID, this GID device will have access to resource required. From the legitimate requests and no attack detected, all other devices, CID or CFID must be recategorized for approaching the resources to a matching GID state. IoTPredictor adapts by taking this decision dependent onpast behaviors, attack types, and categorization information stored in the local fog-level database.

3.1 A Hybrid IDS in IoTPredictor

Adaptive IDS: Hybridness Combining the Strength of RIDS and ADS With this, we offer a novel hybrid IDS combining the precision and coverage of a rule-based IDS (RIDS) with the high robustness at the character level coming from an anomaly detection system (ADS), leading to an ideal threat detection solution. Such a hybrid IDS (Intrusion Detection System) aids to effectively detect and mitigate the IoT security threats. As a result, it provides a more robust and reliable system by integrating detection via both signature and anomaly techniques schemes. The hybrid method employs data processed from known attack modules and behavioral detection modules, providing wider coverage of attacks as well detecting unknown or unusual behaviors, giving the method the ability to adapt to new attacks.

When the traffic from new hardware gets captured we instantly check if the device is legitimate and protected against intrusions, on the basis of laid down conditions. Once the device is

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

determined to be authentic, it can access resources. If not, an alarm is raised, and traffic is sent to the IDS, meanwhile, the log is stored in a local fog-level database. In fact, the proposed IDS can detect and prevent the damage from attacks to the infected devices spreading in the network. Once this information is received, if the IDS recognizes the device as a legitimate user, the device will be tagged as genuine and continue sending the data, and if it cannot be generated, it will raise an alert, and the device will be blocked.

3.2. RIDS module

In our hybrid IDS, the RIDS module is typically requires less processing capability, as its rule-matching process demands minimal computating and storage, making it ideal for resource-limited devices. RIDS establishes and applies predefined protocols for identified threatsor specific behaviors. These rules are designed to target particular attacks or behaviors. When RIDS detects a predefined pattern associated with a known attack, it immediately triggers an alert. Examples of Protocols for the three categories of devices are outlined on the following page. The logical operators used in these rules include ∧ (AND), ∨ (OR), and ¬ (NOT).

1.GIDs: These devices typically generate steady as well as regular data traffic, with consistent and reliable connections.

Rule:

- If the typical data packet size, avg(P$size$), stays within ±10% of the typical traffic(T$usual$).
- If the count of active connections,num(C$open$), remains stable over time t.

$$[(0.9 \text{ x Tusual} <= avg(P\text{size}) <= 1.1\ x\ T\text{usual}) \wedge$$

$$(|\text{num(Copen(t)}) - \text{num(Copen(t}')\text{)}| \leq \epsilon)] \longrightarrow \text{“NoAlert”}$$

2. CIDs: These devices may be involved in attacks or show unusual data transfers.
Rules:

• If the device immediately starts an uncommonlylarge volume of outgoing connections, num(Cout).

• If the device shows an abnormal data transmission rate with respect to the expected transfer rate (dn).

$$[(\text{num(Cout)}] > threshold) \vee (\text{abs(Do} - \text{Dn}) > \epsilon)] \longrightarrow \text{“Alert”}$$

In the given equation, Do denotes the measured rate of data transferredin the device, while ϵdenotes a threshold value that defines the reasonable variation from thetransfer rate which is normal.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. CFIDs: These devices display abnormal protocol usage or unexpected traffic leaving the network.

Rules:

• If the device is being initiated applying an unconventional protocol (Pt($used$)) quickly.

• If the proportion of outgoing packets(Pout) to inbound packets (Pin)Exceeds two times the amount.

$$[(\text{Pt(used)} \notin \text{Pt(common)}) \vee (\text{Pout Pin} > 2)] \longrightarrow \text{“}Alert\text{”}$$

In addition to the general rules specified above, all the traffic patterns of network are tracked and assessed. This allows thresholds and parameters to be adapted according to the expected behavior in the network of the different categories of devices.

3.3 Component of ADS and its algorithm

Automated Decision System (ADS) is a system that automatically collects, processes, analyses, and makes decisions about data. The system is composed of multiple modules such as: the Data Input Layer collects raw data from sensors, external APIs, etc. The Data Processing Layer pre-processes and integrates the data for further analysis and so on. Then comes the Analytics and Decision-making Layer that applies the models and algorithms on the data to find insights and create decisions based on the rules specified in advance or predictive models. When a decision is reached, the Action Layer automates tasks or sends commands to other systems to change settings or send alerts. It also consists of a User Interface to monitor the performance, visualise the real time outputs of the system and give notifications to the user to take an action when needed.Such an automated system ensures efficiency, accuracy, and consistency in decision-making for different operations.

Algorithm 1 describes the process of constructing an iForest whichis used for anomaly detection by constructing multiple decision trees.The building utilizes traffic information gathered from internet of things devices. A height constraint (l) is applied to regulate the thickness of each separate tree (iTree) in the forest. The purpose of setting the sub-sampling size (s) is to escape from overlearning and the building of excessively intricate trees. Building each tree within the specified height limit is the responsibility of the recursive BuildTree function.

Algorithm 1:

ADS Using iForest

1: **Input**: X - Input dataset (traffic data captured), t - Number of trees, s - Subsampling size
2: **Output:** A set of t iTrees representing the Isolation Forest

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3: **procedure** IsolationForest(X, t, s) State initialise an empty forest set State set height limit l= ceil (log2 (s))
4**: for** i=1 to t do: State randomly sample data points s from X
5: sampledX = subSample(X,s) State create an iTree using sampled data
6: iTree = recursiveBuildTree(sampledX,0,1) State add iTree to iForest
7: iForest = iForest ∪ iTree
8:**return** Forest
9: **procedure** subSample(X, size) State randomly shuffle X random.shuffle(X) State select 'size' samples from X
10: sampledX = X[:size]
11: sampledX=random(X,size)
12:**return** sampledX
13: **procedure** recursiveBuildTree(X,h,l)
14: **if** h>=l ∨ size(X)<=1
15: create a leaf node with a single data point or reach height limit
16: **return** leafNode
17: **else**
18: select a feature f and splitValue v
19: split X based on f and v
20:Xleft, Xright = split(X,f,v)
21: create an internal node(iNode) with f and v
22: iNode = ciNode (f, v)
23:build left and right subtrees recursively
24: iNode.LeftChild=recursiveBuildTree (Xleft,h+1,l)
25: iNode.RightChild=recursiveBuildTree(Xright,h+1,l)
26:**return** iNode

3.4 Evaluating IoTPredictor

VirtualBox (Oracle VM 7.0.6) is used to build virtual machines (VMs) that simulate different IoT devices to simulate IoT device. VirtualBox is compatible with Linux, macOS, Windows, and Solaris, and supports a variety of guest operating systems. This functionality allows users to take snapshots of the virtual machine's current state, which can later be restored. Two Virtual Raspberry Pi and Virtual Arduino VMs are used to emulate IoT devices. In addition, two other VMs generate threat-related packetsthat are constructedto be distinguishable from normal traffic. One VM operates as a fog network node. IoTPredictor, located at the fog level, includes our HMM and the hybrid ADS implemented in Python, and is connected to the IoT devices within the same network to process the data. Tcpdump [3] is employed to capture data traffic on the network from these IoT devices, with the captured features listed in Table 1.
Table 1

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Attributes of traffic are gathered from IoT device

Attributes	Descriptions
Packet Size& Payload	Size of packets and content of the payload
Protocols and Headers	Method recognition and header specifications
Request-Response Patterns	HTTP request operations and responses
Defects and Deviations	Spotting of corrupted packets or errors; invalid TCP packet, Packet loss identified.
Data Protection and Safety	Recognitionof security protocols or encryption; encrypted communication using TLSv1.2.
Identification of device	identification of traits or identifiers unique to a device; MAC address of the device

Malicious packets are introduced into a network to gain unauthorized access, disrupt services, or bypass security measures. Scapy [1], a versatile packet manipulation tool, is used to create threat-related data unitsthat mimic capacityvulnerabilities in the fog layer of IoT. Scapy is a powerful tool that can be utilized for both ethical and malicious purposes. It enables the creation, transmission, capture, and analysis of network packets, making it ideal for tasks such as intrusion detection, network scanning, and protocol testing. Different threat scenariosare emulatedby designing malicious packets that exploit various weaknesses. The types of attacks generated are listed in Table 2.

Table 2 Forms of attacks generating harmful traffic

Attacks	Descriptions
TCP/IP Hijacking	controls the specified session between two hosts by forging the TCP package.
SYN Floods	producing & delivering a deluge of TCP SYN packets in an attempt to deplete a target server's resources and render it inoperable.
ICMP Attacks	creating ICMP packets to be used in ICMP redirect or ping flood attacks.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Wireless Network Attacks	creating malicious Wi-Fi packets or wireless frames for threats like deauthentication.
DDoS Simulation	creating a lotof activity to overpower a target server or organizein order to mimic DDoS attacks.
Network Scanning	carrying out reconnaissance, port scanning, and network discovery.

Result

To evaluate the performance of our hybrid IDS and its capability to correctly Determine and categorize behaviors that are usual and unusual, we calculate precision, recall, and F1 scores. These standardsprovides a thorough assessment of the configuration's effectiveness in identifying possible security risks and attacks risks. The accuracy of the IoTPredictordesign is shown in Table 3.

Precision, which is the Percentage of equipment and intrusions accurately identified within all predictions made by IoTpredictor, provides information about how accurate the optimistic predictions made by the system are. The model has a recall of 0.95 and a precision of 0.93.

Table 3

IoTPredictor - Model accuracy

Metric	**Value**
Precision	0.9309
Recall	0.9496
F1 Score	0.939
Accuracy	0.8869

We examined how well different machine learning models work in detecting attacks on IoT systems. The specific models we looked at are DNN, CNN, LSTM, and a new model we came up with. In Figure 6, you can see a straightforward graph that shows how these models compare in four key areas: Accuracy, Precision, Recall, and F1 Score. From reviewing past studies and our own experiments, we noticed that the LSTM model did better than the DNN and CNN

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

models. This is mainly because LSTM is good at recognizing patterns that change overtime.

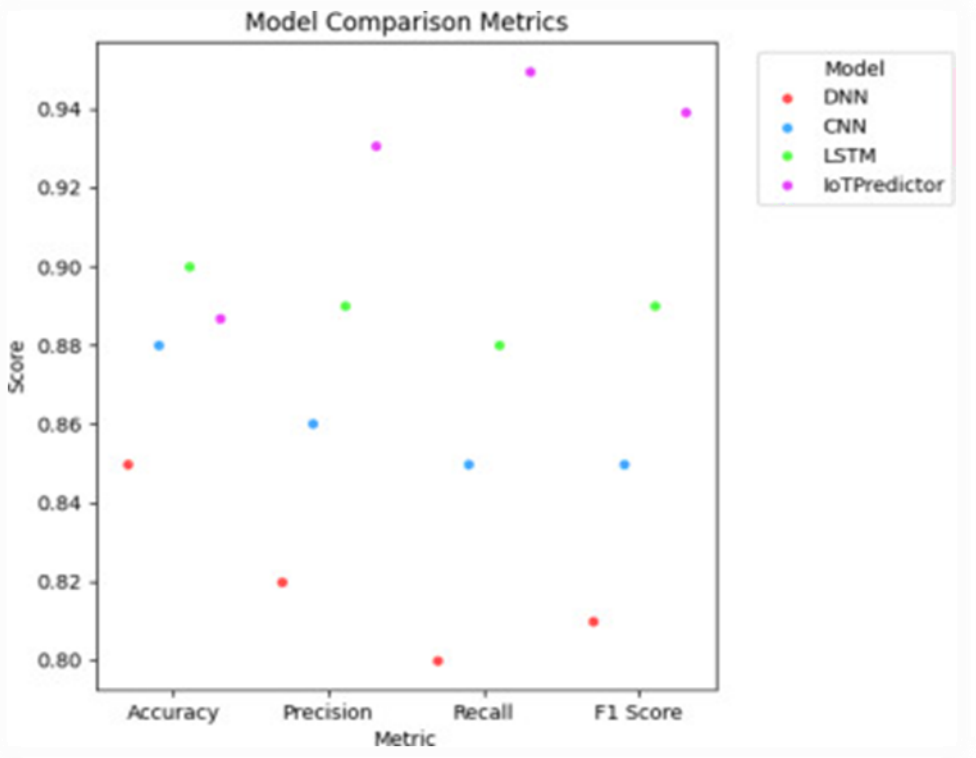


fig. 3Model comparison metrics

When evaluating security in **IoT** and **FogComputing** environments, it is important to consider the various attack types that can target both the edge devices (IoT) and the fog layer. These attacks can jeopardize not just individual devices but also the entire network infrastructure, impacting data integrity, confidentiality, and availability. The evaluation results for each attack type are shown in Table 4, which includes metrics like F1 score, recall, accuracy, and precision. A thorough examination of several attack types pertinent to IoT and fog computing can be found below:

Table 4 Attack type metrics of IoTPredictor

Attack type	**Accuracy**	**Precision**	**Recall**	**F1 Score**
Denial of service	**0.9**	**0.89**	**0.92**	**0.91**
Spoofing	**0.88**	**0.85**	**0.92**	**0.88**
Port Scanning	**0.92**	**0.94**	**0.90**	**0.92**

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Man-in-the -Middle	**0.87**	**0.84**	**0.88**	**0.86**
Packet Sniffing	**0.91**	**0.92**	**0.91**	**0.91**
Injection Attacks	**0.89**	**0.88**	**0.90**	**0.89**
Malware Communication	**0.86**	**0.83**	**0.87**	**0.85**

These outcomes demonstrate how well the IoTPredictor can identify different kinds of attacks. A screenshot of the results of capturing and processing packets using Scapy's sniff function is shown in Fig. 3. Based on predetermined criteria, it gathers features and tags traffic as either benign or malicious (malicious traffic denotes 1 and benign denotes 0). For the sake of illustration, the outputs are restricted to 10 samples out of 1000.

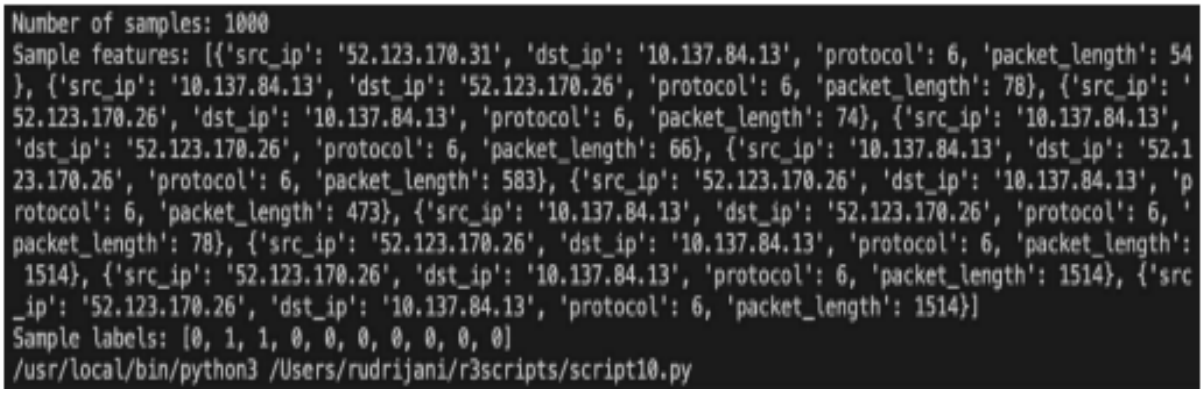


Fig. 3 Capturing packets and analyzing them with Scapy

Figure 4 shows the type of attack on the confusion matrix, broken down intoTrue Negatives (TN), True Positives (TP), False Negatives (FN) and False Positives (FP),.
The confusion matrix's values may be used to compute a number of performance indicators, including:

- Accuracy = (TP + TN) / (TN+ TP + FN + FP)
- Precision = TP / (FP + TP)
- Recall = TP / (FN + TP)
- F1Score = 2 * (Precision * Recall) / (Precision + Recall)

For example,Five occurrences were misclassified as invasion (FP), 4were inaccurately categorizedas non-invasion (FN), and 89 occurrenceswere correctly classified as non-invasion (TN) and 92 as assaults (TP), respectively, in the DoS scenario. These outcomes demonstrate how well the IoTPredictor can identify different kinds of attacks.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

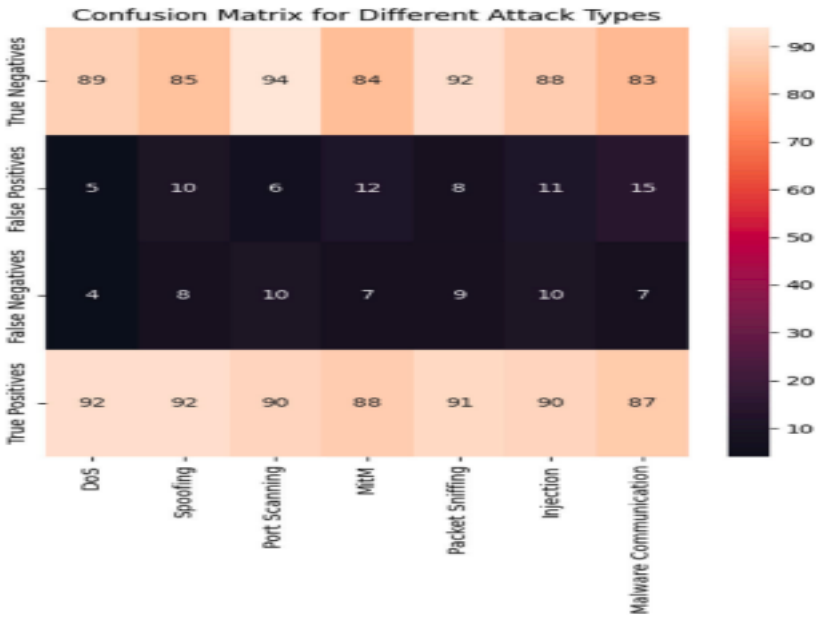


Fig. 4 Confusion matrix of IoTPredictor

Figure 5displays the completeIoT device deploymentwithin three classes which are of GID, CID, CFID, along with the HMM's anticipated distribution.The observations closely matched the actual count, with CID and CFID showing high accuracy and precisely matching the core values. HMM-based device categorization is particularly useful in environments like IoT-fog computing, where the number and diversity of devices are large and continuously changing. It enables effective monitoring and management by identifying device types based on their interaction patterns or other behavioral signals.

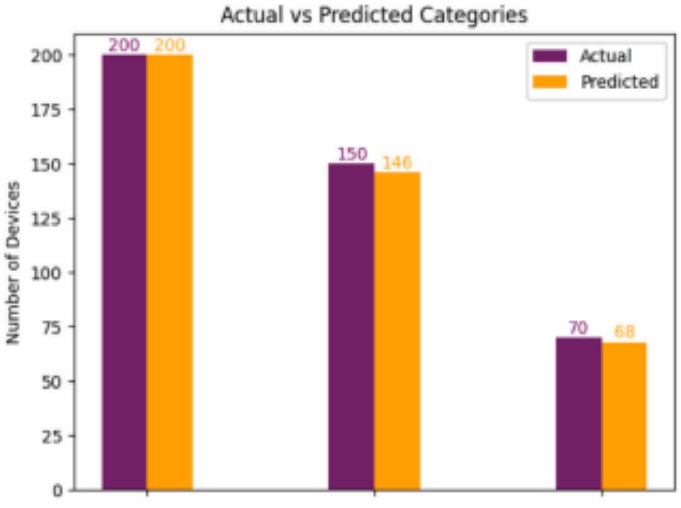


Fig. 5 Device categorisation using HMM

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Conclusion

In this paper, we introduced a security strategy called IoTPredictor, aimed at forecasting the behavior of IoT devices and identifying attacks within the evolving IoT-fog computing environment. As heterogeneous smart IoT devices continue to advance, security concerns have become more prominent. We have listed several kinds of IoT threats in this study along with defenses against them. Our strategy used a hybrid IDS that combined rule-based and iForest techniques with HMM to forecast the behavior of IoT devices. Through deployment and assessment, we proved that our method was successful in recognizing various device assaults, classifying devices according to their behaviors, and spotting irregularities. When it came to predicting the behaviors of IoT devices, the predictive model based on HMM showed encouraging results. But because the IoT-fog scenario is dynamic, it needs constant adaptation and development. Our proposed approach to security, IoTPredictorestablish a solid frameworkwhich helps toprotect thesmart technology and thefog layer in IoT completely. Since we keep tackling the changing risk scenario, acknowledging these restrictionsand exploring future directions will strengthen our method, ensuring a flexible as well as robust protection strategyfor the ever-evolving fog computing in IoT environment.

Reference

[1] Bansal, S., Bansal, N., 2015. Scapy-a python tool for security testing. J. Comput. Sci. Syst. Biol. 8 (3), 140.

[2] Bansal, S., Kumar, D., 2020. IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. Int. J. Wirel. Inf. Netw. 27, 340–364

[3] Joseph, D.A., Paxson, V., Kim, S., 2006. Tcpdump Tutorial. University of California, EE122 Fall.

[4] Park, C., Lee, J., Kim, Y., Park, J.-G., Kim, H., Hong, D., 2023. An enhanced AI based network intrusion detection system using generative adversarial networks. IEEE Internet Things J. 10 (3), 2330–2345.

[5] Patel, A., Qassim, Q., Wills, C., 2010. A survey of intrusion detection and prevention systems. Inf. Manage. Comput. Secur. 18 (4), 277–290.

[6]Tian, J., Wang, B., Guo, R., Wang, Z., Cao, K., Wang, X., 2022. Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles. IEEE Internet Things J. 9 (22), 22399–22409. http://dx.doi.org/10.1109/JIOT.2021.3111024.

Received: August 06, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[7]Tian, J., Wang, B., Wang, Z., Cao, K., Li, J., Ozay, M., 2021. Joint adversarial example and false data injection attacks for state estimation in power systems. IEEE Trans. Cybern. 52 (12), 13699–13713.

[8] Ullah, I., Mahmoud, Q.H., 2019. A two-level hybrid model for anomalous activity detection in IoT networks. In: 2019 16th IEEE Annual Consumer Communications & Networking Conference. CCNC, IEEE, pp. 1–6.

[9] Verma, A., Ranga, V., 2019. ELNIDS: Ensemble learning based network intrusion detection system for RPL based internet of things. In: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages. IoT-SIU, IEEE, pp. 1–6.

[10]Vermesan, O., Friess, P., 2013. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River publishers.

[11]Vijayanand, R., Devaraj, D., Kannapiran, B., 2017. Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid. In: 2017 4th International Conference on Advanced Computing and Communication Systems. ICACCS, IEEE, pp. 1–7.

[12] Yu, S.-Z., Kobayashi, H., 2003. An efficient forward-backward algorithm for an explicit-duration hidden Markov model. IEEE Signal Process. Lett. 10 (1), 11–14.

Received: August 06, 2025