Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3951–3961
DOI : 10.47974/JDMSC-3022

AI-driven early warning systems for IoT cyber threats

Abhiraj Bhaskar Ubale [§]
Department of Computer Science and Engineering
COEP Technological University
Pune 411005
Maharashtra
India

Vijay Kotkar [†]
Department of Computer Engineering
Pimpri Chinchwad Education Trust's
Pimpri Chinchwad College of Engineering and Research
Ravet
Pune 412101
Maharashtra
India

Sayali D. Joshi *
Department of Information Technology
Mararhwada Mitra Mandal's College of Engineering
Pune 411052
Maharashtra
India

Milind S. Patil [‡]
Department of Electronics & Telecommunication Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

[§] *E-mail:* abu.comp@coeptech.ac.in
[†] *E-mail:* vijay.kotkar@pccoer.in
* *E-mail:* sayalidjoshi@gmail.com (Corresponding Author)
[‡] *E-mail:* milind.patil@vit.edu

© Taru Publications

Puneet Kumar Yadav [@]
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

V. S. N. Kumar [#]
Department of Computer Science
Aditya Degree & PG Colleges (Autonomous)
Kakinada 533003
Andhra Pradesh
India

Abstract

Internet of Things (IoT) ecosystems has been associated with serious cybersecurity threats due to the heterogeneous nature, dynamism in connectivity, and poor computing abilities. The present paper presents an AI-based early warning system, which is strong in detecting and predicting cyber threats in an IoT environment, with a high accuracy and low latency. The framework is a combination of sequential learning algorithms, i.e., BiLSTM and GRU, to learn temporal anomalies of network traffic, and Graph Neural Networks (GNN) to learn complex interactions among devices. A hybrid ensemble of Autoencoder based anomaly detectors and XGBoost based classification can achieve an improved predictive performance and a reduced false positives. It has a distributed monitoring and edge intelligence layer to mitigate threats in real time by processing real time data. The experimental results indicate that the proposed system is more accurate in detecting and has a shorter response time and higher system robustness and hence can be applied to scalable and security-critical internet of things applications in other domains.

Subject Classification: *68M25, 68T05, 68M12, 94A60.*

Keywords: *IoT security, Early warning system, Deep learning, Graph neural networks, Anomaly detection.*

I. Introduction

The rapid advancement of Internet of Things (IoT) technologies have revolutionised the digital ecosystem providing seamless integration with smart homes, medical devices, automation and critical systems [1, 2]. But the massive use of resource-constrained and heterogenous IoT devices has made them more vulnerable to cyber-threats [3, 4]. Established security measures that are based on rigid policies and signature matching may not be enough to deal with more advanced and dynamic threats like distributed

[@] *E-mail:* **puneet.yadav1@niu.edu.in**
[#] *E-mail:* **vsnkumar@gmail.com**

denial-of-service (DDoS), botnets and advanced persistent threats [5, 6]. This kind of constraint requires to develop intelligent and adaptive security solutions that can automatically detect and notify security attacks. The recent developments in machine learning (ML) and artificial intelligence (AI) technologies have shown an enormous potential to improve the cybersecurity of the IoT by using predictive analytics and anomaly detection in an automatic way [7, 8, 9]. Specifically, the complex and highly dependent temporal and network relations are easily captured by recurrent neural networks (RNN) and graph-based deep learning algorithms [10, 11].

II. AI Models for Threat Prediction and Early Warning

AI models can help actively identify IoT cyber threats via temporal patterns, structural relationships, and anomaly behavior, enhancing the accuracy of predictions and reducing false alarms by a significant margin [12, 13]. Figure 1 demonstrates AI models that make it possible to predict threats in IoT.

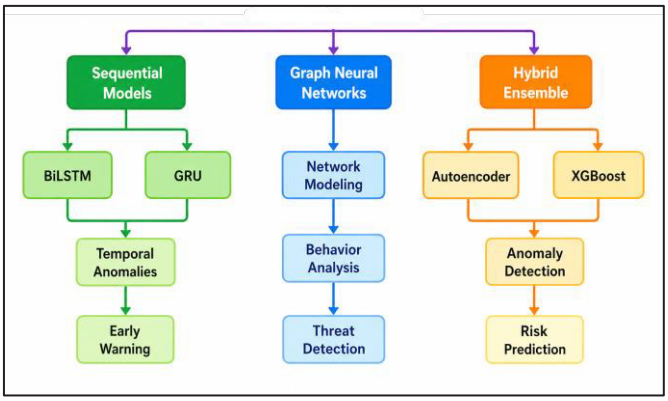


Figure 1
AI Models for IoT Threat Prediction and Early Warning

A. *Sequential learning models (BiLSTM, GRU) for temporal anomalies*

BiLSTM and GRU sample networks capture the time-dependent characteristics of network traffic, which allows them to detect sequential abnormalities and novel types of cyber-attacks by learning long-term behavior patterns [14].

$$X = \{x1, x2, \dots, xT\}, xt \in R^n \quad (1)$$

The input sequence representation can be defined by Equation (1), in which the time-series information of the IoT traffic is organized into vectors where temporal dependencies can be learned by the sequential models.

$$\vec{h_t} = LSTM\left(xt, \vec{h_{\{t-1\}}}\right) \quad (2)$$

The forward LSTM equation (2) explains how the hidden states are changed by the present input and the past context to capture historical trends in network behavior.

$$h_t^{\leftarrow} = LSTM\left(xt, h_{\{t+1\}}^{\leftarrow}\right) \tag{3}$$

The backward LSTM process is represented in equation (3), and it is learnt using the reverse sequence of data, which helps to enhance the detection of anomalies using the latest data due to the processing of both forward and backward directions.

$$h_t = sqrt((h_t^{\rightarrow})^2 + (h_t^{\leftarrow})^2) \tag{4}$$

The BiLSTM fusion of equation (4) will integrate forward and backward hidden states, where root-based aggregation will be used to better portray the features and more completely represent the temporal dependencies.

$$L = \int^{0\,\mathrm{T}} \left|\left|y_t - \hat{y}_t\right|\right|^2 dt \tag{5}$$

The temporal loss function (Equation (5)) is the sum of squared prediction error over time, and it makes the model minimize the difference between real and predicted output over sequences.

$$z_t = \sigma\left(Wz\, xt + Uz\, h_{\{t-1\}}\right) \tag{6}$$

$$S_t = sqrt\left(\Sigma\left(h_t - \bar{h}\right)^2\right) \tag{7}$$

GRU update mechanism is described as follows in equation (6): the information flow is regulated by gating functions which enable the achievement of efficient learning of any temporal dependences without any significant increase in computational complexity over standard LSTM. The calculation of the anomaly score is done according to equation (7) which calculates the abnormality of the mean hidden representation and the higher the values, the stronger the abnormality and the successful detection of potential cyber threats.

B. *Graph Neural Networks (GNN) for network behavior modeling*

GNNs represent IoT networks as graphs, including device interactions and structural dependencies, allowing coordinated attacks and abnormal patterns of communication across distributed systems to be accurately detected.

$$G = (V, E), A \in R^{N \times N} \tag{8}$$

The graph representation of IoT networks as illustrated in equation (8) is used to model the relationship between devices and interactions to represent the graph and hence model communication relationships effectively.

$$L = I - D^{-\frac{1}{2}} A\, D^{-\frac{1}{2}} \tag{9}$$

Equation (9) defines the normalized Laplacian matrix, which reflects structural connectivity and stabilizes propagation of features, and thus nodes with high degree will not dominate compared to the low degree nodes found in the network.

$$H(l+1) = \sigma\left(D^{-\frac{1}{2}}A\,D^{-\frac{1}{2}}H(l)W(l)\right) \tag{10}$$

The node feature propagation in GNN is described by equation (10), in which features are updated sequentially with neighboring information and learnable weights, and complex dependencies and patterns of behavior on a network-wide scale are learned.

$$h_G = \int_V H(L)\,(v)dv \tag{11}$$

Equation (11) is the graph-level embedding aggregation, which is an aggregation of node features over the whole graph domain that results in a global representation that can be used to perform system-wide anomaly detecting and analyzing activities.

$$S_G = sqrt(\Sigma\,(\lambda i)^2) \tag{12}$$

Spectral anomaly score is calculated by equation (12) based on eigenvalues with greater energy showing atypical structure and thus revealing patterns of abnormal connectivity and coordinated cyber threats in IoT networks.

C. *Hybrid ensemble model (Autoencoder + XGBoost)*

The hybrid model is a combination of Autoencoder-based anomaly detection and XGBoost classification that will enhance detection accuracy, minimize false positives, and be resistant to sophisticated and unknown cyber threats.

$$z = f(x) = \sigma(We\,x + be) \tag{13}$$

The encoder transformation, defined in equation (13), is the transformation of the input features to a lower-dimensional latent space via weights and activation, which contains important patterns needed in the task of detecting anomalies.

$$\hat{x} = g(z) = \sigma(Wd\,z + bd) \tag{14}$$

The process of decoder reconstruction is shown by equation (14) and in this equation the latent representation is converted to the approximate original input and thus the deviation of reconstruction is identified and this deviation shows the patterns of abnormal behavior.

$$L_{rec} = \int_0^n \left|\left|x - \hat{x}\right|\right|^2 dx \tag{15}$$

The reconstruction loss is given by equation (15), which is a compilation of squared differences between original and reconstructed data, and requires minimal error, and proper learning of normal data distributions across features by the model.

$$x' = \sqrt{(x^2 + \hat{x}^2)} \tag{16}$$

In equation (16), feature enhancement is done by root normalization where the original and reconstructed values are combined to enhance the representation which enhances the robustness and brings out the deviations that will help in identifying the small anomalies.

$$\hat{y} = \sum_{k=1}^{K} fk(x'), fk \in F \tag{17}$$

The equations (17) represent the XGBoost prediction, which involves several decision trees, which jointly predict output summing up their contribution, which allows the correct classification of normal and abnormal patterns of IoT network behavior.

III. Proposed AI-Driven Early Warning Architecture

The suggested architecture combines distributed monitoring, edge intelligence, and AI analytics to provide the ability to detect threats in real-time, respond swiftly, and protect dynamically scalable across IoT ecosystems.

A. *Distributed IoT monitoring layer (devices, sensors, gateways)*

This layer receives real-time data on IoT devices, sensors and gateways and offers continuous monitoring and full data on its input to be utilized in the threat analysis and anomaly detection process.

$$X(t) = \sum_{i=1}^{N} x_{i(t)} \tag{18}$$

Aggregated network data (equation (18)) is a network data, in which the signals of multiple IoT devices are summed during the time period, which will provide one view of the trends in the system-wide activity.

$$G(t) = \int_0^T X(t)dt \tag{19}$$

The data fusion of equation (19) entails the integration of signals, which are time-dependent to observe cumulative behavior so as to get a better view of the long-term trends and possible anomalies.

$$X_f = \sqrt{\left(\left(\frac{1}{N}\right) \Sigma \left(x_{i(t)}\right)^2 \right)} \tag{20}$$

Noise filtering in equation (20) is based on root mean and it minimizes the changes in signal by averaging the squared signals, which enhances the signal stability and increases the reliability of the monitored IoT data streams.

$$X_n = \frac{X_f}{\max(X_f)} \tag{21}$$

Normalized data distribution (Equation 21) scales the filtered values to the largest value, and provides consistency across devices, and avoids high amplitude signals dominating analysis.

$$S_m = \sqrt{(\Sigma (X_n - \mu)^2)} \tag{22}$$

The score of monitoring anomaly calculated as a distance between mean behavior is computed in equation (22) with larger variance of behavior indicating abnormal activity, thus helping to identify possible cyber threat in networks in time.

B. *Edge intelligence layer for real-time preprocessing*

Edge layer data is filtered, feature extracted and preprocessed on the edge, minimizing latency, bandwidth consumption and providing a faster response to anomalies and possible cyber threats detected.

$$x_{p(t)} = x(t) - \int^{0\,\mathrm{T}} noise(t)dt \tag{23}$$

The process of data preprocessing is defined in equation (23) as noise elements are combined and removed in the raw signals resulting into better quality data and cleaner inputs to be used in the edge analytics downstream tasks.

$$f(t) = W\, x_{p(t)} + b \tag{24}$$

Equation (24) is an operation of feature extraction, which converts preprocessed data with the help of weights and bias, creating meaningful feature vectors, which reflect significant patterns to perform anomaly detection and classification tasks.

$$f_n = \frac{f(t)}{sqrt(\Sigma\, f(t)^2)} \tag{25}$$

Equation (25) explains feature normalization, scaling features with root-based magnitude normalization, which guarantees equal representation, less bias and greater stability of the model during the training and inference step.

$$S_e = \sqrt{\left(\Sigma\left(f_n - \bar{f}\right)^2\right)} \tag{26}$$

The score of equation (26) to compute edge anomaly detection is a measure of deviation of normalized features, concerning mean behavior, and the high scores of this measure represent abnormal patterns and possible cyber threats in the IoT systems.

IV. Result and Discussion

A. *Dataset Description and Preprocessing*

To test the proposed AI-based early warning system, an open-source dataset, CICIoT2023, created by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick, can be used. This dataset consists of around 46.7 million network traffic records collected from an IoT setup with 105 IoT devices and 33 attack types categorized into 7 attack categories. These types are DDoS attacks, DoS attacks, reconnaissance, web-based attacks, brute force, spoofing, and Mirai attacks. The data-set

contains 46 input features related to traffic and supports two types of intrusion detection: binary and multiclass.

The original data split into training, validation and test data with a ratio of 70:15:15 for reproducible evaluation, keeping the class distribution as much as possible. Duplicate records should be explored, missing/incorrect values should be dealt with, and the numerical features should be normalized based on the statistics computed from the training data. Temporal sequences must not be allowed to cross the partitions of the datasets for processing by BiLSTM and GRU. Only generate graph representations for GNN component when device identities or communication relationships are reliably reconstructable.

B. *Experimentation result*

The experimental findings have shown a higher level of accuracy, shorter latency, and high detection efficiency in contrast to the baseline approaches, which prove the effectiveness and scalability of the proposed AI-driven early warning system.

Table 1

Performance Evaluation of AI-Driven Early Warning System for IoT Cyber Threats

Metric	Conventional Methods	Proposed AI-Driven System
Detection Accuracy (%)	91.8	97.4
Precision (%)	90.6	96.2
Recall (%)	89.9	95.7
F1-Score (%)	90.2	95.9
False Positive Rate (%)	8.7	3.1

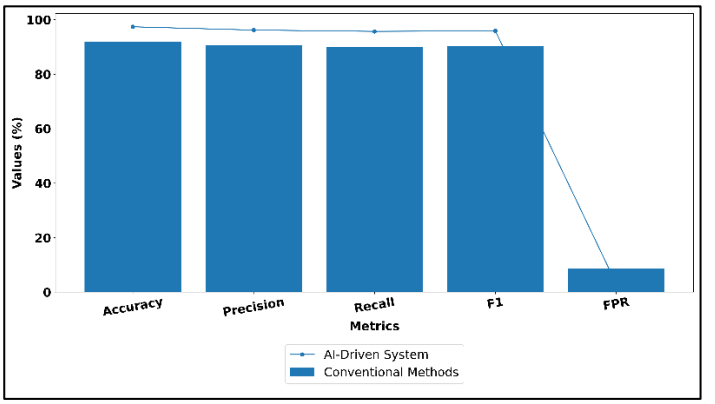


Figure 2

Analysis of Conventional vs AI-Driven Detection Performance

Table 1 will provide a comparison of the performance of traditional and the suggested AI-based system. Figure 2 is the comparison of traditional and AI-based approaches with a better detection.

The accuracy of detection, precision, recall, and F1-score of the proposed approach are great, and this means that there is a high degree of trust in the threat detection. Figure 3 provides a comparison of metrics, with AI system better detection performance.

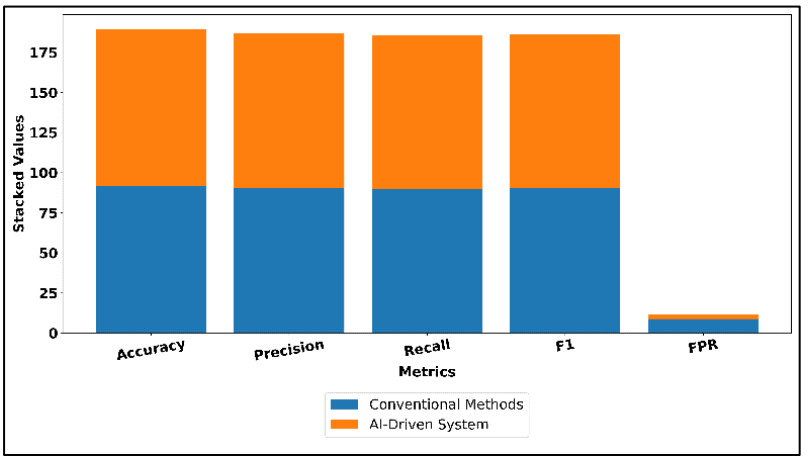


Figure 3

Comparison of Detection Metrics for Conventional and AI Systems

Interestingly, false positive rate is lowered significantly, increasing the system credibility. Such enhancements reveal the usefulness of combining the state-of-the-art AI frameworks to detect and predict IoT cyber threats in real-time in an accurate and efficient way.

V. Conclusion

The current paper introduced an AI-based early warning system to detect and predict cyber threats in IoTs. The proposed framework combines sequential learning models, graph neural networks, and a hybrid Autoencoder-XGBoost ensemble, thus successfully capturing the temporal anomalies, structural dependencies, and intricate attack patterns. The addition of distributed monitoring and edge intelligence layers allows processing real-time data, low latency, and scalable deployment of heterogeneous IoT networks. Experimental analysis has shown the system to have greater rates of detection, lesser rates of false positive and shorter reaction times to traditional methods. These enhancements outline the strength and flexibility of the suggested approach under the conditions of dynamism and security-related issues.

References

[1] W. Zhao and P. Wang, "AI-Driven Cybersecurity in IoT-Based Systems," *Sensors*, vol. 25, no. 23, Art. no. 7254 (2025), doi: 10.3390/s25237254.

[2] I. Mutambik, "AI-Driven Cybersecurity in IoT: Adaptive Malware Detection and Lightweight Encryption via TRIM-SEC Framework," *Sensors*, vol. 25, no. 22, Art. no. 7072 (2025), doi: 10.3390/s25227072.

[3] M. J. C. S. Reis, "AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities," *Electronics*, vol. 14, no. 12, Art. no. 2492 (2025), doi: 10.3390/electronics14122492.

[4] M. H. Alsulami, "An AI-Driven Model to Enhance Sustainability for the Detection of Cyber Threats in IoT Environments," *Sensors*, vol. 24, no. 22, Art. no. 7179 (2024), doi: 10.3390/s24227179.

[5] M. A. Siam, K. Y. Lucky, S. N. Hasan, J. Kaur, H. Kaur, M. S. Uddin, and M. M. T. G. Manik, "Cybersecure Intelligent Sensor Framework for Smart Buildings: AI-Based Intrusion Detection and Resilience Against IoT Attacks," *Sensors*, vol. 25, no. 24, Art. no. 7680 (2025), doi: 10.3390/s25247680.

[6] R. Abreu, E. Simão, C. Serôdio, F. Branco, and A. Valente, "Enhancing IoT Security in Vehicles: A Comprehensive Review of AI-Driven Solutions for Cyber-Threat Detection," *AI*, vol. 5, no. 4, pp. 2279–2299 (2024), doi: 10.3390/ai5040112.

[7] E. Skoubris and G. Hloupis, "An AI-Powered, Low-Cost IoT Node Oriented to Flood Early Warning Systems," *Engineering Proceedings*, vol. 58, no. 1, Art. no. 44 (2023), doi: 10.3390/ecsa-10-16023.

[8] Warin Sripanya, Wannarut Rungrottheera, and Pacharapol Hyunsin, "Fourier series analysis and computation based on function characteristics," *Journal of Interdisciplinary Mathematics*, vol. 28, no. 6, pp. 2109–2120 (2025), doi: 10.47974/JIM-2352.

[9] A. Oacheşu, K. S. Adewole, A. Jacobsson, and P. Davidsson, "Enhancing IoT Security with Generative AI: Threat Detection and Countermeasure Design," *Electronics*, vol. 15, no. 1, Art. no. 92 (2026), doi: 10.3390/electronics15010092.

[10] M. Esposito, L. Palma, A. Belli, L. Sabbatini, and P. Pierleoni, "Recent Advances in Internet of Things Solutions for Early Warning Systems: A Review," *Sensors*, vol. 22, no. 6, Art. no. 2124 (2022), doi: 10.3390/s22062124.

[11] S. Fernandes-Pereira, "Deep Learning and Optimization Approaches in Deep Convolutional U-Shape Network with Jump Attention-Based Vision Transformer for Integrated Sequence Scheduling and Trajectory Planning with Obstacle Avoidance in Wireless Rechargeable Sensor Networks: A Rev," *IJEECS,* vol. 14, no. 1, pp. 353–359 (Apr. 2025).

[12] M. Chaturvedi, S. Sharma, G. Ahmed, and V. Bhatnagar, "Implementation of localized frequency transform-based encryption for enhanced cybersecurity in communication networks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 1, pp. 169–178 (2026), doi: 10.47974/JDMSC-2533.

[13] S. Quaye, A. H. Khan, K. Tapre, and M. Dawson, "AI-Powered Cybersecurity Models for Training and Testing IoT Devices," *Applied Sciences*, vol. 15, no. 24, Art. no. 13073 (2025), doi: 10.3390/app152413073.

[14] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

Received April, 2026