Vol. 08, No. 3 (2026) 1611-1622, doi: 10.24874/PES08.03.016

Proceedings on Engineering Sciences

www.pesjournal.net

GA-ZAD: A GRAPH-BASED ADAPTIVE REASONING APPROACH FOR DETECTING ZERO-DAY ATTACK IN IOT

Neetu[1]
Deepak Kumar Sharma
Koyel Datta Gupta

Received 09.06.2026
Revised 21.07.2026
Accepted 29.08.2026

Keywords:

Zero-day Attack, IoT, Deep Learning, AI, Detection Model, graph neural network, intrusion detection.

A B S T R A C T

The growth of Internet of Things (i.e. IoT) devices has markedly increased the attack surface for cyber threats, notably zero-day attacks (ZdA), which are especially difficult due to their unknown characteristics. This study introduces an innovative Deep Neural Network (DNN) methodology for identifying zero-day threats in IoT networks utilising the Edge-IIoT dataset. The proposed model GA-ZAD utilises an encode-process-decode architecture, employing graph-based logic for relational pattern identification and meta-learning strategies for optimal performance. The methodology encompasses comprehensive data preliminary processing, feature selection, & architectural design, focusing on differentiating known attacks from undiscovered ones. The evaluation results indicate that PCA (Principal Component Analysis) based models surpass the performance of LDA (Linear Discriminant Analysis). The proposed GA-ZAD model combined with XGBoost and PCA attains the best performance with accuracy, precision, recall and F1-Score of 97.6%. While in combination with Random Forest achieves 97.5%. Visual analysis, encompassing attack type distribution, temporal trends, and IP source input, further corroborates the methodology with proficient, clear separation of attacks using latent space representations. This research is useful in many areas applicable to the industries, management, operations and especially for information & communication. It provides a framework which can be reliable and trustworthy from several intrusion attacks. This paper provides a fundamental framework for enhancing zero-day detection of attacks in IoT systems with further more research, in tackling significant difficulties in cybersecurity.

© 2026 Published by Faculty of Engineering

1. INTRODUCTION

The rapid enactment of IoT devices in various industries, homes, and public infrastructure has resulted in exceptional ease and efficiency. This spread has also increased susceptibility to advanced cyber threats, including zero-day attacks (ZdA). Zero-day attacks leverage unknown vulnerabilities, for which conventional signature-based detection techniques are ineffective. The substantial volume of IoT data, the diversity of devices, and the availability of IoT environments heighten the difficulties of ZdA detection.

[1] Corresponding author: Neetu
Email: neetu052phd22@igdtuw.ac.in

The ongoing attack detection methods depend on extensive datasets, which struggle to generalise between known and unknown attacks, or experience a rise in false-negative rates (Khraisat et al., 2019). These constraints highlights the need for innovative strategies that can aptly distinguish between recognised and unrecognised attacks.

The model's GA-ZAD (Graph-Based Adaptive Zero-Day Attack Detection Model) meta-learning ability guarantees strong performance in low-data environments, which is a vital need in IoT environment. The primary contributions of this paper are as follows:

1. This model provides the ZdA attack detection in the IoT networks using a graph reasoning and meta learning approach, which includes data pre-processing, model designing, and selecting features.
2. The efficiency of the model and its effectiveness are assessed using the precision, F1 score, recall and accuracy to represent the capacity to detect known and unknown attack types.
3. The latent space representations for clear separation of attacks provide deep insights into the patterns of threats by clearly separating.

This proposed methodology provides the fundamental methodology to enhance the ZdA detection in the IoT networks, that include the help of an overarching approach by aiming to provide a secure IoT ecosystem from the emerging several cyber threats. For several evaluations of these methods, findings and a comprehensive evaluation based on this research. The novelty of this model, GA-ZAD, is that it introduces a novel encode-process-decode architecture that integrates graph reasoning and meta-learning to enhance IoT security. In comparison to conventional IDS models, which rely on predefined or already existing attack signatures, GA-ZAD employs an Encoder Network to extract compact feature representations, and a Processor Network uses graph neural network-based reasoning to identify hidden relationships between the data. It works on the principle of message passing between neighbouring nodes. Information is gathered from immediate neighboring nodes and is subsequently aggregated to learn new hidden information. The incorporation of meta-learning ensures adaptability in low-data environments, making the model highly effective. This meta-learning uses metric-based learning, which works by calculating Euclidean distance scores between nodes for clear separation of data. To reduce feature dimensionality and eliminate redundancy elimination we applied PCA and LDA with RF, XGBoost, and optimised XGBoost to show the performance comparison of all the classifiers with both PCA and LDA. Compared to existing models, GA-ZAD offers superior scalability, accuracy and generalisation in detecting unknown threats, making it a groundbreaking advancement in IoT cybersecurity.

This research paper has been divided into the following sections, In section 2, the literature review is discussed, followed by section 3, where motivation is discussed. Section 4 shows the methodology behind the model. In section 5, the result will be demonstrated by comparing with existing models, followed by section 6, in which application-based case studies will be discussed. Section 7 is the conclusion of the entire research work.

2. LITERATURE REVIEW

Numerous previous models have tackled IoT anomaly detection & intrusion detection with diverse architectures. DeepAuto is a model that uses a deep autoencoder to identify abnormalities by learning & reconstructing standard traffic patterns (Atlas et al., 2024). Anomalies are identified as deviations from these patterns. This unsupervised method facilitates the identification of unknown threats but fails to adequately differentiate between benign anomalies & zero-day attack patterns. The suggested approach distinctly differentiates between recognised and unidentified attack patterns by employing graph-based reasoning, hence enhancing interpretability and accuracy in zero-day attack detection (Cevallos-Moreno et al., 2024). Another significant model is GCN-AE, which utilises Graph Convolutional Networks (GCNs) in conjunction with autoencoders to identify anomalies by capturing structural trends in network traffic (Seo et al., 2024), (Mohideen et al., 2024).

IoT-IntrusionNet model utilises a hybrid CNN-LSTM architecture to integrate convolutional feature extraction with sequential learning for intrusion detection (Tareq et al., 2022), (Selem & Jmili, 2024). Although proficient at identifying temporal trends in IoT traffic, it is significantly dependent on extensive datasets for training & has difficulties in addressing zero-day attack scenarios. The proposed model mitigates this issue with a meta-learning method, facilitating fast training in low-data contexts. Moreover, IoT-IntrusionNet does not provide distinct techniques for differentiating between known and unknown attacks, a critical attribute of the proposed system.

This section mostly addresses related efforts focused on the generation and categorisation of data about zero-day attacks in light of the two principal pillars of the current study outlined above. Kim et al. (2018) propose an architecture for a malware detection system that utilises both authentic and counterfeit malware data, featuring modifications relative to the genuine data. This data is generated by a deep-convolutional generative adversarial network (i.e. DCGAN) founded deep autoencoder (DAE) technique, which demonstrates superior accuracy as well as stability to learn as compared with analogous models. In the context of ZdA data production, Won et al. (2022) propose a framework, PlausMal-GAN, introduced GAN models designed and trained to generate high-quality and diverse zero-day malware images. There is another

NetML technique based on feedforward neural networks (FNN) that identifies IoT abnormalities via supervised training on pre-engineered features (Messaoud, 2025).

The increasing expansion of IoT networks has introduced particular security challenges, particularly the identification and forestalling of cyber threats, including zero-day attacks (Crandall et al., 2005). Conventional IDS relies on signature-based or anomaly-based methods for identifying known threats, which can make the system vulnerable; it often struggles with unknown or unidentified attacks. Several studies have delved into ML and DL approaches for enhancing the effectiveness of IDS (Guo, 2022), (Nandiraju et al., 2025), (Mahboubi et al., 2024), (Dwibedi et al., 2020). Meidan et al. (2018) introduce a framework based on anomaly detection that uses autoencoders for differentiating between normal and malicious traffic in IoT-identified unknown attacks. While approaching the enhanced detection rates, the lack of adapting evolving patterns to attack by attackers makes them less effective against zero-day threats. These approaches get improved based on the increasing pattern of attacks (Krishnan et al., 2025). This is an assembly-based technique to detect anomalies from this method that shows incremental learning. However, it suffers from the high computational costs of deploying the large-scale methods (Ali et al., 2025).

DL and graph-based techniques both has begun to advance ZdA detection in IoT networks in recent years. There is enough research for this; Redino et al. (2022) a remarkable study, proposed the DL approach that combines the network flow telemetry with the asset-level-based features in the graph. This kind of dual-auto encoder provides a structured and effective way to identify zero-day threats in real-time, which demonstrates the high accuracy and recall across the datasets at a large scale that represents real-world organisational networks. The model can generalise and scale the promising solution that can be a contemporary challenge to the cybersecurity of the IoT environment.

Lo et al. (2022) introduced E-GraphSAGE, a GNN-based IDS method that can be implemented in IoT environments. To capture both the edge features along with the topological information of the network traffic, the E-GraphSAGE surpasses the traditional techniques in terms of key classification metrics that can be observed across the multiple benchmark datasets, for this model, Edge-IIoT dataset will be the best dataset to examine and analysis the model (Ferrag et al., 2022). This shows the potential of GNNs to enhance the IDS capability within the IoT networks.

Current studies have integrated DL and graph-based methods to improve IoT security (Cevallos-Moreno et al., 2024). Esmaeili et al. (2023) provides the GNN (Graph Neural Networks) based model to make it efficient enough to provide higher accuracy that identifies the known attacks and also detects coordinated attacks. There was a limit to detecting novel attacks because of the scarcity of adaptive learning mechanisms that play an important role in IoT security. Alhwaiti et al. (2024) demonstrated an LSTM-based model for capturing temporal-based attack patterns to improve the performance of detection. However, LSTM models need an extensive environment to train the data, to make them less practical ZdA detection. The research has limitations which highlight the requirement of an adaptive, highly scalable as well as higher accuracy detection model which is capable enough to handle evolving attack patterns.

Another critical challenge while implementing a real-time IoT environment related to security is the detection or identification of malicious IP sources that can exploit the system and trace out important data or documents. The existing traditional methods are based on blacklist-based detection. However, it has become obsolete against dynamic and polymorphic attacks. Al-Aql (2024) introduced a hybrid DL model, which is a combination of the techniques of RNN and LSTM-based architectural environment for IP-based IDS. The model enhanced the identification of the attack sources that failed to use the inter-device relationships, which are important for detection on IoT devices by the attacker. To address these abovementioned issues, our proposed model, GA-ZAD, introduces the Graph Convolutional Networks (i.e., GCN) with an adaptive learning framework that not only classifies attacks but also helps to identify the anomalous patterns that indicate zero-day exploitation.

By leveraging graph-based reasoning, deep encoding of the feature, as well as adaptation for real-time mode, GA-ZAD outperforms recent existing models in terms of detecting scalability and accuracy. Not like existing methods, it helps to update knowledge-based information by identifying emerging attack patterns, to make more suitable real-world IoT-based security applications. The proposed model for novel architecture enables early zero-day attack detection by having minimal false positives for significant upgradation of cybersecurity for resilience in the IoT ecosystems.

Additionally, the research by Friji et al. (2023) explored a multi-stage attack exposure and prediction framework that uses GNNs. By inspiring the version of Lockheed Martin for Cyber Kill chain introduced a system was introduced that accomplishes an average F1-score of 94% throughout the different stages, also to evaluate the Ton IoT dataset. This performance surpasses the standard approaches of Random Forest Techniques that show the efficiency of the GNNs model to detect advanced multi-step attacks in IoT settings (Alshehri et al., 2025), (Wang et al., 2025).

The proposed model distinguishes innovative encode-process-decode architecture that integrates a network of encoders to extract features and a processor network to provide graph-based reasoning. This combination

ensures the accurate identification of known attacks while concurrently recognising the relational patterns that suggest zero-day exploitation (Alam et al., 2025), (Su & Wang, 2024). Moreover, the application of meta-learning marked by reducing reliance on extensive datasets, to render the model for appropriate IoT contexts that constrain the labelled data. The practical model for usefulness further ensures that real-world datasets to tackle the scalability that typically encounters prior approaches.

Collectively, the research shows various kind of effectiveness that combines DL with Graph-based methods to detect ZdA within the IoT Networks. The proposed GA-ZAD model builds upon the advanced integration within IoT networks. The proposed GA-ZAD model has been designed on the enhanced integrated graph-based reasoning and meta-learning environment within the encode-process-decode architecture. This architecture enhances detection accuracy and adaptability to address the evolving cyber threats in the IoT environment. Table 1 shows the comparison with the other datasets; it explains that Edge-IIoT is better to use for this model. The proposed methodology outperforms the equivalent that effectively handles the unique issues of zero-day attack detection in IoT networks which offers data-efficient, interpretable, and scalable solution that fulfils real-world application-based requirements (Abdi et al., 2024), (Soliman et al., 2023), (Fu et al., 2025).

Table 1. Dataset Comparison

Dataset	Size & Diversity	Attack Types	Realism	Feature Set	ZdA inclusion	Strength	Limitation
Edge-IIoT Dataset (Ferrag et al., 2022)	Large, diverse IIoT data	Known and Zero-Day attacks	High (Collected from real IoT devices)	Network traffic, timestamps, protocol, IP features	Yes	Covers a wide range of real-world IoT attacks	High complexity may require feature selection
NSL-KDD (Khraisat et al., 2019)	Medium, outdated	DoS, R2L, U2R, Probe	Moderate	Basic network traffic features	No	Widely used for IDS research well-structured	Lacks IoT-specific attacks, no real zero-day threats
UNSW-NB15 (Tareq et al., 2022)	Large	9 attack types including generic, exploits, and worms	High	Rich feature set, packet-based analysis	No	More realistic than NSL-KDD, captures modern attack behaviours	Not IoT-specific, lacks zero-day attack coverage
CICIDS 2018 (Khraisat et al., 2019)	Large	DDoS, Botnet, Web attacks	High	Full packet capture, flow-based features	No	Simulates real-world attack traffic well	Not IoT-specific limited zero-day representation
TON_IoT (Tareq et al., 2022)	Large	IoT and non-IoT cyber threats	High	Logs, network, and telemetry data	Partial	IoT-specific dataset, includes devices behaviours	Not explicitly designed for zero-day detection
BoT-IoT (Lo et al., 2022)	Large	DDoS, Data Exfiltration, Keylogging	High	Flow-based network features	No	Designed specifically for IoT security	Focused mainly on botnet-related attacks, lacks zero-day cases

3. MOTIVATION

Increasing expansion of the IoT has revolutionised industries by enabling industrialisation to enable seamless connectivity that provides connectivity & automation across diverse domains, for instance, smart cities, manufacturing, transportation, and healthcare. However, this surge in connected IoT devices has concurrently introduced significant vulnerabilities in cybersecurity. Among these criteria, ZdA has exploited the unknown as well as unpatched vulnerabilities by posing a specific severe threat because of the unpredictable and stealthy behaviour.

Traditional IDS and ML-based solutions often rely on large labelled datasets, also predefined known signatures. Such approaches scuffle for generalizing the encounter of novel threats which leads for high false negative rates, also delayed detection. Additionally, the most traditional models lack the adaptability for evolving attack patterns in resource-constrained of IoT environments.

This research is driven by the requirement for an intelligent, lightweight framework and an adaptable framework which is capable of distinguishing known attacks and detecting unseen or unknown zero-day threats to exploit the solutions with high accuracy and efficiency. To integrate the DNN with graph-based reasoning, along with the meta-learning strategies, the proposed model GA-ZAD targets to increase the generalisation capacity & resilience of IoT security systems.

The motivation stems from both practical requirements and academic gaps for building a scalable as well as robust solution that performs well along with the benchmark datasets of Edge IoT, also applicable to real-

world IoT scenarios where attack patterns are dynamic, and limitations of the system resources are there.

4. PROPOSED METHODOLOGY

The proposed GA-ZAD architecture is designed to identify both known and previously unseen attacks in the IoT framework through an intelligent combination of graph-based learning and adaptive classification, making the system intelligent by integrating these techniques**.** The dataset is subjected to pre-processing data to encompass missing value treatment that normalized, and category encoding. Feature engineering-based techniques help to identify the important characteristics, for instance, temporal trends and IP source activities. The Encoder network compresses the input data to show the reduced dimensional representation, whereas the Processor network demonstrates the graph-based reasoning for identifying the network traffic patterns. The Decoder Network categorises network traffic as regular, recognised attacks, or zero-day attacks. And then to reduce feature dimensionality and redundancy elimination we applied PCA and LDA along with RF, XGBoost, optimized XGBoost to show the performance comparison with both. The model undergoes training using Edge-IIoT dataset utilising meta-learning approaches, hence improving its adaptability in low-data contexts. Performance evaluation is done using accuracy, precision, recall, and F1-score.

This study presents a basic architecture for detecting zero-day attacks utilising a Deep Neural Network (i.e. DNN) method. Figure 1, shows the encode-process-decode approach, wherein the encoder derives significant feature representations, and the processor applies graph-based reasoning to unknown relationship patterns. Figure 2, which shows the methodology flow. The methodology encompasses several essential steps: data preparation, feature selection, model design, & evaluation. This research examines implemented on the Edge-IIoT dataset for the identification of zero-day attacks (ZdA) in IoT settings utilising a DNN-based framework.

a) Data Preprocessing

The analysis Edge-IIoT dataset was done for its structure and quality. The following steps were performed to design this architecture:

- Data cleaning: The timestamping column was converted into a standard date-time format for the time-series analysis.
- Timestamping Parsing: The timestamping column was converted into the standard date-time format for time-series analysis.

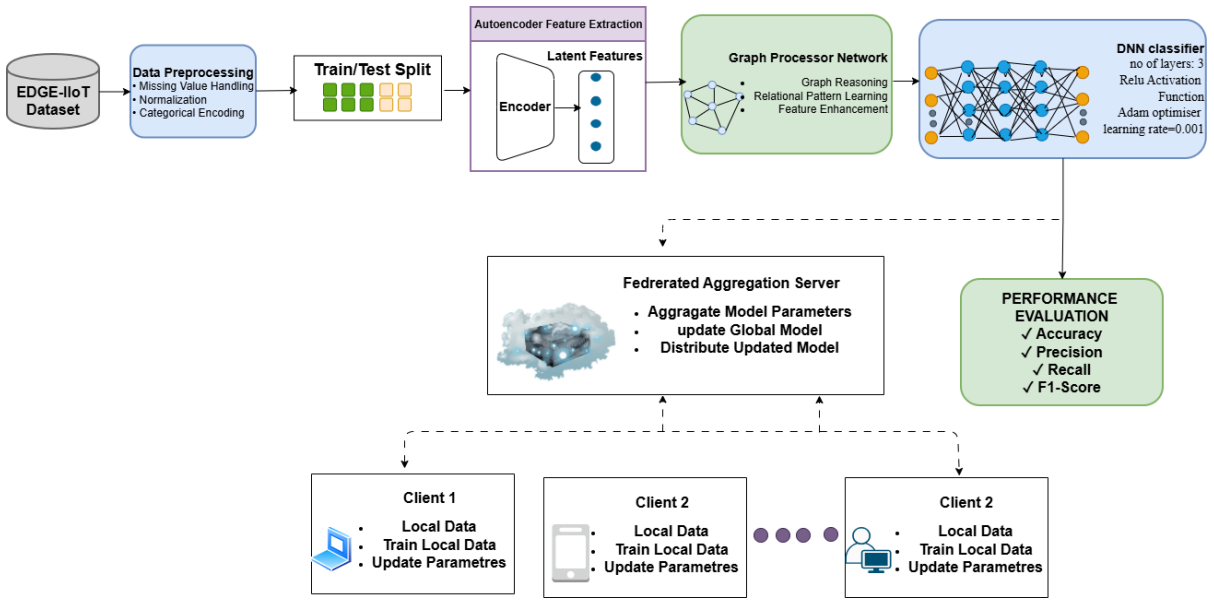


Figure 1. Proposed Architecture of the Model GA-ZAD

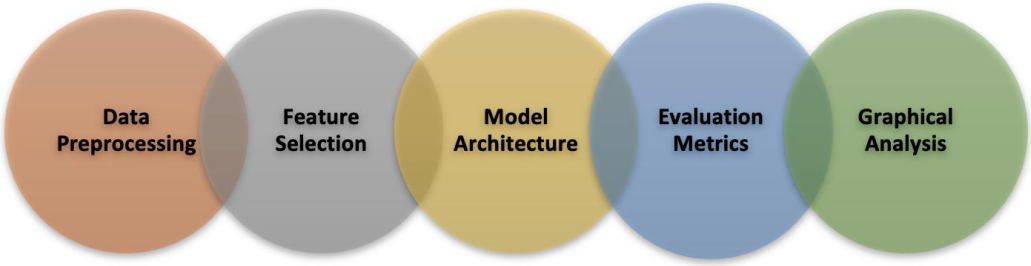


Figure 2. Methodology flowchart

- Categorical Encoding: The labels for attack types were encoded into the numerical values for model compatibility.
- Feature normalisation: All the numerical features were scaled to uniformity and improved model convergence.
- Data balancing: Data imbalancing is handled by using SMOTE (Synthetic Minority Over-sampling Technique) which creates new artificial points for minority class (Hussein et al., 2019).

b) Feature Selection

Key features were identified based on their relevance to the zero-day attack detection:

- Network-specific features: IP_source, IP_destination, type of protocol and the port numbers.
- Traffic Behaviour: Packet size, flow duration and payload characteristics.
- Attack labels: The dataset includes known attack types and enables supervised learning.

c) Model Architecture

The proposed DNN architecture follows an encode-process-decode framework to make the proposed architecture trustworthy:

- Encoder layer: It converts the high-dimensional input data features into compact or low-dimensional features. It consists of Multi-layer Perceptron (MLP) which applies linear transformation and Relu activation function.

$$H_{latent} = \sigma(WencX + b_{enc}) \quad (1)$$

Where W_{enc} is encoder weight, σ is activation function, X is input feature vector, b_{enc} is bias vector and. These latent features then passed to the next processor stage.

- Processor layer: It utilises graph-based reasoning to capture the relational patterns. It works by collecting the information from immediate neighboring node and aggregate it and updates to learn new information.

$$H_{GNN} = \sigma(\hat{A}\sigma H_{latent})\, W_{gnn}) \quad (2)$$

Where H_{latent} is the embeddings generated by encoder, $\hat{A}$ is the matrix having graph connectivity information and W_{gnn} is the learning weight matrix.

- Output layer: It performs the multi-class classification for distinguishing between known and unknown attacks.

Hyperparameter tuning was conducted to optimise the architecture, including:

- Number of layers: 3 hidden layers are there.
- Activation functions: Rectified Linear Unit (ReLU) for non-linearity.
- Optimisation Algorithm: Adam optimiser for adaptive learning rates.

To reduce feature dimensionality and eliminate redundancy, we then used PCA and LDA. Reduced features are used to train RF, XGBoost and Optimised XGBoost and comparison is discussed in result section.

d) Federated Learning

Hence designing a framework which can acclimate to new attack patterns is a vital requirement for the IDs. The client-server block represents how the distributed learning, as well as the centralised decision-making mechanism can be applied.

- Each distributed client will train local model independently process their own network segment data, and learned parameters are transmitted the to the Central server.
- The server consistently updates the model parameters by aggregating knowledge obtained from the multiple clients and then redistributes it back for further training, enabling adaptive learning against evolving cyber threats.

This client-server architecture in the DNN-hybrid mechanisms helps to achieve real-time monitoring, adaptive threat intelligence, scalable IDS, and distributed data collection to make it highly suitable for large-scale IoT, as well as the IIoT deployment model. This architecture will enhance the performance of the IDs and also preserve data privacy while reducing need for collecting data at a central server point.

e) Evaluation Metrics

Standard metrics were employed to assess the model performance:

- Precision, Recall, F1-Score: Measures classification performance for individual attack types.
- Visualisation: Latent space projections using t-SNE to understand the separation of attack classes.

f) Graphical Analysis

Additionally, the visualisation was created to analyse the data using Latent space representation along with the bar graphs which shows the performance metric comparison of the different techniques applied.

This given below pseudocode sketches a precise method for revealing both known and unknown attacks in IoT networks by utilizing graph-based reasoning in combination with deep learning and adaptive meta learning approach. This model is intended to serve in real

time IoT setting providing scalable and accurate cybersecurity solutions.

Pseudocode of GA-ZAD

1. Data Preprocessing
   - Clean D, normalise F, and encode categorical labels.
   - Split D into training (Dtrain) and testing (Dtest) sets.
2. Feature Engineering
   - Extract relevant features from F (for instance, time trends, and IP statistics)
3. Model Design
   - Encoder: Compress input features into the latent space
   - Processor: Use graph-based reasoning for relational patterns
   - Decoder: Classify traffic as normal, known attack, or unknown.
4. Training
   - Train the model on Dtrain with a suitable optimiser and loss function.
5. Evaluation
   - Predict attack types in Dtest
   - Compute Evaluation metrics.
6. Visualization Analysis
   - Plot graphs for evaluation metric
   - plot Latent Space diagram for clearly analyzing separation of known vs unknown attacks.

5. DATASET

In this experimental evaluation We have used Edge-IIoTset Dataset (Ferrag et al., 2022) which is a pragmatic dataset containing both normal and attack network traffic from various industrial protocols and devices. This dataset contains nearly 14 types of attacks clubbed in 5 major categories. In Figure 3, the bar graph portrays the distribution of several attack types samples within the dataset. Also in Figure 4, the bar graph shows the count of the normal and attack type distribution in the dataset.

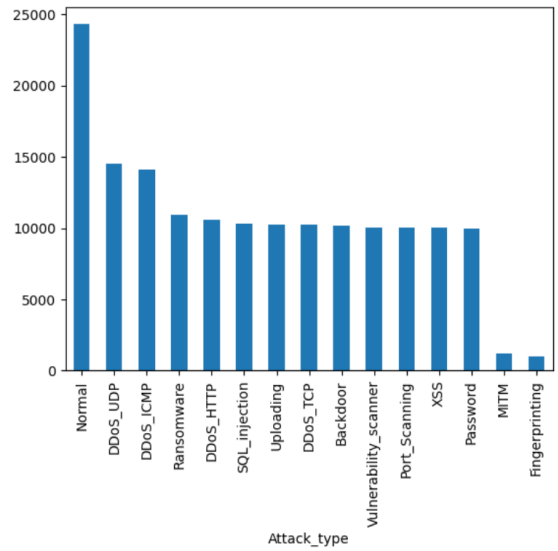


Figure 3. Distribution of Attack Types

Attack_type	
Normal	24301
DDoS_UDP	14498
DDoS_ICMP	14090
Ransomware	10925
DDoS_HTTP	10561
SQL_injection	10311
Uploading	10269
DDoS_TCP	10247
Backdoor	10195
Vulnerability_scanner	10076
Port_Scanning	10071
XSS	10052
Password	9989
MITM	1214
Fingerprinting	1001

Name: count, dtype: int64

Figure 4. Distribution of normal and Attack traffic

6. RESULT

In this experiment, the performance of the GA-ZAD model is appraised against Random Forest (RF), XGBoost, and Optimised XGBoost after applying Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA). The statistical measure that we have used for evaluation are accuracy, precision, recall and F1-score as given below. From the results it can be inferred that the model trained using PCA is outperformed than those trained using LDA. Among all, GA-ZAD model in combination with XGBoost and Optimised XGBoost with PCA achieves high accuracy, Precision, Recall and F1-Score approximately 97.6%. And also, Random Forest with PCA demonstrate nearly same score of 97.5% in all metrics. In contrast the use of LDA, results in declination of classification performance, particularly for XGBoost it declines to 90.7% and 90.4% after optimisation. RF performance declines to 96.2% after LDA across all metrics which is slightly better than XGBoost. Findings also suggest that PCA is better than LDA which provides most robust and accurate classification when combined with XGBoost. The similarity among all metrics suggests balanced performance with minimal bias towards false positives or false negatives. This affirms of its dependability to reduce the false positives and negatives. Altogether performance metric with these 3 classifiers of the model is shown in Table 2. The proposed methodology shows the enhance generalization for unfamiliar attacks, due to its graph-based reasoning, also for its meta-learning capabilities which is discussed in further section. It shows clear separation of attacks, to render the scalability and pragmatic options which might be able to seen in real-world applications of IoT security.

a. Model Performance Metric

The proposed DNN Model, by using the XGBoost and Optimised XGBoost with PCA method, demonstrated strong detection capabilities achieving 97.6% across all metrics:

Precision: The ability to correctly identify positive instances.

$$Precision = \frac{true\ positives}{true\ positives + false\ positives} \quad (3)$$

Recall: It assesses the detection of actual positive instance

$$Recall = \frac{true\ positives}{true\ positives + false\ negatives} \quad (4)$$

The F1 score is a balance assessment of precision and recall via harmonic mean

$$F1\ Score = \frac{true\ positives}{true\ positives + \frac{1}{2}(false\ positives + false\ negatives)} \quad (5)$$

Accuracy = It measures overall correctness of model.

$$Acc = \frac{true\ positives}{true\ positives + false\ positives + flase\ positives false\ negatives)} \quad (6)$$

Table 2. Performance Metric

Model	Performance			
	Accuracy	Precision	Recall	F1-Score
Random Forest with PCA	0.975	0.975	0.975	0.975
Random Forest with LDA	0.962	0.963	0.962	0.962
XGBoost with PCA	0.976	0.976	0.976	0.976
XGBoost with LDA	0.907	0.911	0.907	0.907
Optimised XGBoost with PCA	0.976	0.976	0.976	0.976
Optimised XGBoost with LDA	0.904	0.907	0.907	0.907

With this we can say, that this model outperforms with PCA rather than LDA. The proposed model, GA-ZAD in combination with XGBoost and PCA attains best performance and effectively tackle zero-day threat detection in IoT contexts. In Figure 5, the correlation heatmap of numerical features is presented which shows how strongly features are connected.

b. Latent Space Visualisation

By using the t-SNE projections, the model's latent space effectively separated known attack classes from unknown attacks to form distinct clusters as shown in Figure 6. This shows the ability to generalise unseen attack patterns. Same type of behavior or pattern are being clustered using meta learning approach which works on distance-based score i.e. Euclidean distance from neighboring nodes. Information from neighboring node is exchange through message passing and then aggregate the information to learn new pattern or behaviors which in turn help in predicting attack type.

In Figure 7, the classification of the model accuracy of different algorithms has been visually analysed using bar graph which is discussed in result section.

The DNN model, including graphical and statistical studies, exhibited its capacity to recognise known attacks and unknown patterns suggestive of zero-day exploits. Future endeavours will concentrate on augmenting the model's capacity to address certain zero-day attack variants and strengthening scalability for extensive IoT networks. It shows an effective range of detection and is capable enough to secure many applications, which can be applied to futuristic smart AI-based applications such as smart cities, healthcare, banking, cloud data and so on.

Utilising a novel encode-process-decode architecture, the model proficiently distinguished between known and unknown attack patterns, demonstrating its resilience in managing varied IoT traffic. The integration of graphical reasoning into the deep learning framework boost resilience against the dynamically evolving attacks by extracting relational patterns in the data, which markedly improves the detection skills of the model.

The proposed model combines deep learning with graph reasoning for capturing the Zero-Day attacks with a minimal dependency on already existing datasets. The Meta learning approach ease the effective operation of the model in low data environment which is difficult in IoT environment. However, the validation of proposed model on Edge-IIoT dataset highlights its applicability for IoT security.

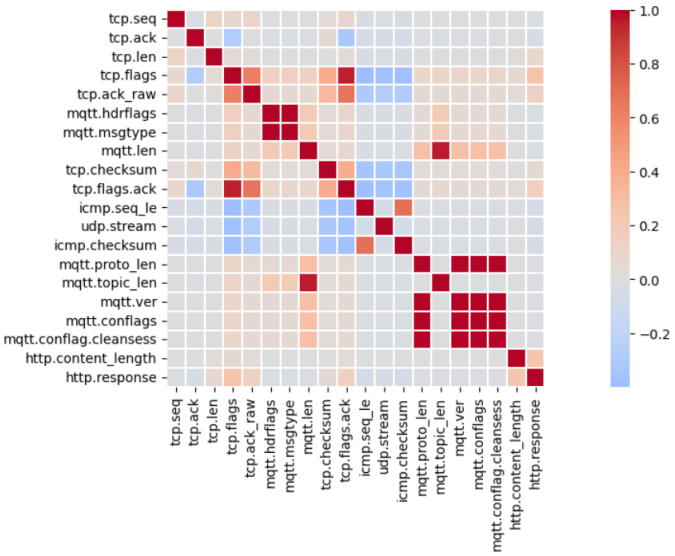


Figure 5. Correlation Heatmap of Numerical Feature

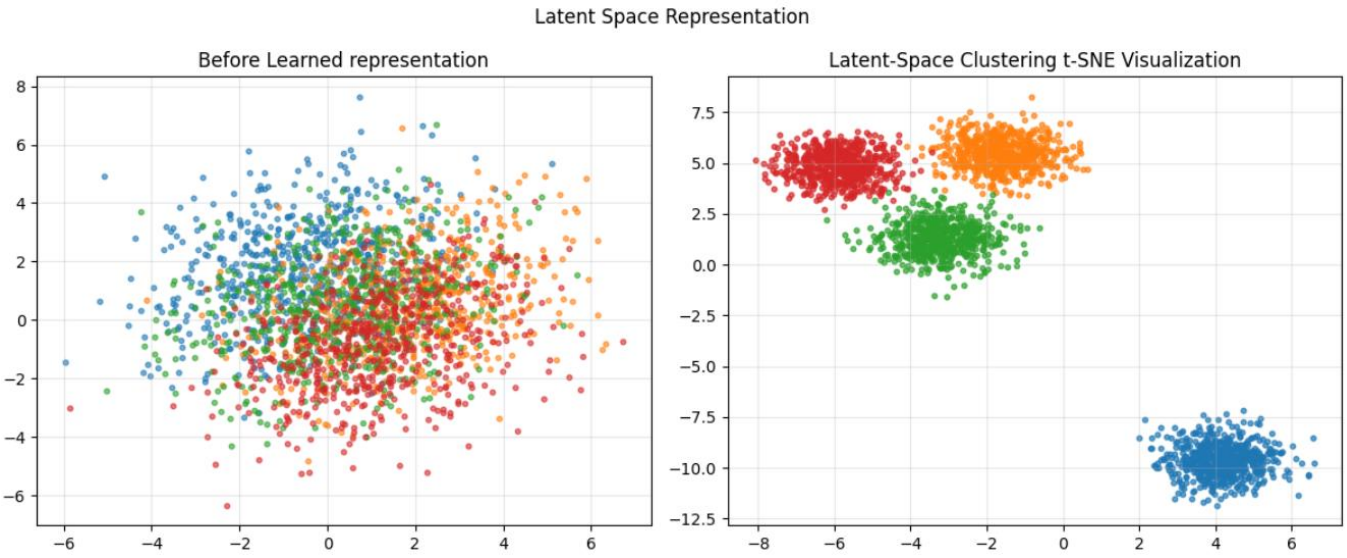


Figure 6. Latent Space Clustering using t-SNE visualization

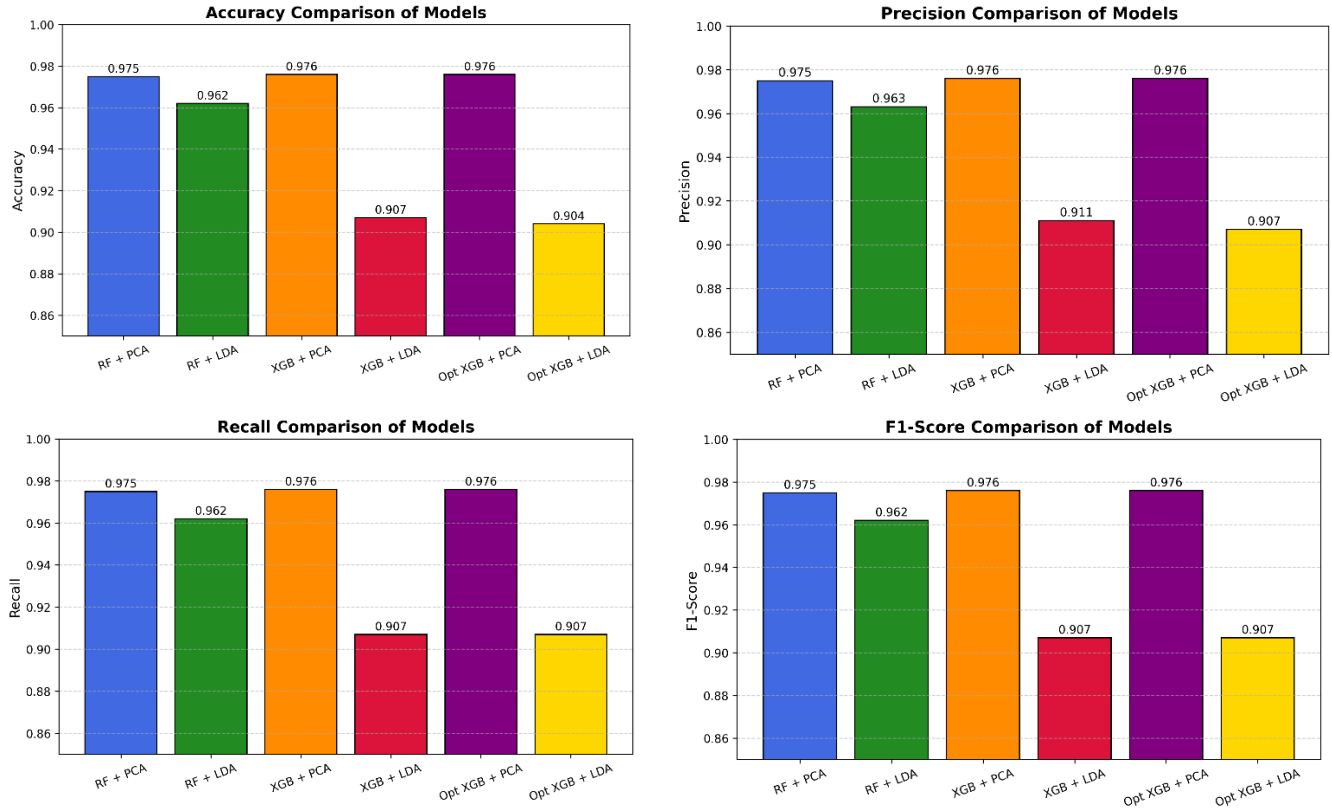


Figure 7. Classification Model Accuracy

7. GA-ZAD IS BETTER FOR REAL-WORLD APPLICATIONS (CASE STUDIES AND

After experimental evaluation and results, we can say that the GA-ZAD model is convenient solution for IoT environment. The following are case studies and real settings illustrating its efficacy:

Case Study 1: Smart Cities and Critical Infrastructure Protection

In smart cities, IoT devices such as smart traffic systems, energy grids, and surveillance cameras are interconnected, making them highly vulnerable to cyberattacks. The traditional IDS models have a dependency on signature-based detection that fails to recognise emerging zero-day attacks. On the other hand, the GA-ZAD detects unknown attacks by using graph-based techniques in which the device-to-device interactions help to identify anomalous traffic patterns that indicate the ongoing intrusion. The meta-learning is capable of ensuring the model adapts to evolving attack strategies that allow the city admin to prevent catastrophic failures in the smart infrastructure of the city.

Case Study 2: Healthcare IoT Security in Smart Hospitals

Smart hospitals are dependent on the IoT-enabled medical devices for monitoring patients, drug admin, and remote surgeries. The zero-day ransomware attack on such devices could compromise the safety of a patient. It leads to data breaches or operational failures. GA-ZAD provides a real-time monitoring system that can provide an adaptive learning approach to detect deviations in the network traffic originating from the medical devices and flag malicious activities before escalation. Unlike the other conventional models, GA-ZAD has a timestamp-based analysis that secures the environment when an attack attempt occurs, which allows the hospital cybersecurity team to take any kind of proactive defensive measures as per their standard, rulebook or strategy.

Case Study 3: Industrial IoT (IIoT) and Smart Manufacturing

In industrial environments, all the automated machinery and IoT sensors are connected to the IIoT networks to optimise production. Cyberattacks targeting Programmable Logic Controllers (PLCs) or robotic systems could lead to delays in production as well as safety hazards. All the current IDS models often generate false positives, which disrupt operations. GA-ZAD mitigates this by applying graph-based reasoning for network traffic; it differentiates between normal system fluctuations & real-time cyber threats. Moreover, the model's scalability allows deployment across large-scale IIoT environments without consuming excessive resources.

There are several reasons behind the GA-ZAD model that excels over existing models applicable in the real world are as follows:

a) Superior Zero Day Detection: Unlike the signature-based IDS models that fail to recognise new threats, GA-ZAD is based on a meta-learning approach that identifies unknown attack patterns to make it more resilient against zero-day exploits.
b) Graph-based Relational Intelligence: It is a conventional model that analyses IoT traffic as isolated records; while doing so, GA-ZAD can capture interactions between the IoT devices, to enhance the model's detection skills to identify hidden anomalies in the network behaviour.
c) Real-Time Detection & Response Time: The timestamping based on the attack trend analysis allows the cybersecurity team to track, predict, as well as mitigate attacks before they can cause ample amounts of damage all over the place.
d) Scalability & Low Resource Overhead: GA-ZAD is designed for large-scale IoT deployments such as healthcare, IIoT, smart cities and so on. It offers high detection accuracy to maintain a low computational overhead.

By addressing these limitations of the traditional models of IDS, GA-ZAD (the proposed model) provides a more proactive, scalable and reliable approach for securing IoT-based real-world applications.

8. CONCLUSION

The proposed model GA-ZAD presents a novel and effective solution to address the growing threats in cybersecurity, especially in IoT networks, specifically in ZdA. The existing Traditional IDS as well as anomaly detection methods that rely heavily on signature-based detection, also supervised learning that fails to recognise previously known and unknown attack patterns. On the other hand, GA-ZAD demonstrates the encode-process-decode architecture to integrate graph-based reasoning as well as meta-learning approaches to enable and detect the threats in IoT environments, i.e. known and unknown attacks. The GA-ZAD model has a rigorous evaluation by using the Edge-IIoT dataset that includes diverse attack types and realistic IoT traffic scenarios. The outcomes of the experiment show a high precision of 97.6% and an F1-score of 97.6% with XGBoost and optimized XGBoost to show the superior ability for benign traffic based on known attacks and ZdA threats.
The GA-ZAD dynamically adapts the evolving attack patterns without significant overheads of computational overhead. It allows the model to identify the complexity of attack behaviours that would be overlooked by DL models for treating the network traffic independently at their data points. It captures the relational dependencies between the network entities, and GA-ZAD significantly enhances their detection accuracy and reliability.

9. FUTURE SCOPE

Scorn its strengths, the proposed model GA-ZAD shows the opportunities for enhancing the model further, future research could focus on real-time deployment optimisations by integrating it with security information and SIEM systems for managing events. Also, it enhances the explainability of the techniques for making GA-ZAD more accessible to the analyst of cybersecurity. Moreover, the expansion of the dataset with ZdA variations and testing for the model on different IoT architectures could further lead to the validation of the model's robustness.

Acknowledgement: I would like to express my sincere gratitude to my supervisors for their valuable guidance and support throughout this research. Their valuable insights and encouragement greatly contributed to the successful completion of this work.

References:

Abdi, N., Albaseer, A., & Abdallah, M. (2024). The role of deep learning in advancing proactive cybersecurity measures for smart grid networks: a survey. *IEEE Internet of Things Journal, 11*(9), 16398–16421. https://doi.org/10.1109/jiot.2024.3354045

Alam, K., Monir, M. F., Hossain, M. J., Uddin, M. S., & Habib, M. T. (2025). Adaptive Defense: Zero-Day attack detection in NIDS with deep reinforcement learning. IEEE Access, 13, 116345–116361. https://doi.org/10.1109/access.2025.3585445

Al-Aql, N. (2024). Hybrid RNN-LSTM networks for enhanced Intrusion detection in vehicle CAN systems. *Journal of Electrical Systems, 20*(6s), 3019–3031. https://doi.org/10.52783/jes.3318

Alhwaiti, Y., Alrashdi, I., Ahmad, I., & Khan, A. (2024). A computational deep learning approach for establishing long-term declarative episodic memory through one-shot learning. *Computers in Human Behavior, 156*, 108213. https://doi.org/10.1016/j.chb.2024.108213

Ali, G., Robert, W., Mijwil, M. M., Sallam, M., Ayad, J., & Adamopoulos, I. (2025). Securing the Internet of Wetland Things (IOWT) using machine and deep learning methods: a survey. *Mesopotamian Journal of Computer Science*, *2025*, 17–63. https://doi.org/10.58496/mjcsc/2025/002

Alshehri, S. M., Sharaf, S. A., & Molla, R. A. (2025). Systematic Review of Graph Neural Network for Malicious attack Detection. *Information, 16*(6), 470. https://doi.org/10.3390/info16060470

Atlas, L. G., Shiny, K., KP, A., NM, S., & Nithiya, J. L. (2024). Detection of intrusions in internet of things based deep auto encoder using deepnets. International Journal of Sensors Wireless Communications and Control, 16(1), 42–52. https://doi.org/10.2174/0122103279327268240911034337

Cevallos-Moreno, J. F., Rizzardi, A., Sicari, S., & Porisini, A. C. (2024). NERO: NEural algorithmic reasoning for zeRO-day attack detection in the IoT: A hybrid approach. *Computers & Security, 142*, 103898. https://doi.org/10.1016/j.cose.2024.103898

Crandall, J. R., Su, Z., Wu, S. F., & Chong, F. T. (2005). On deriving unknown vulnerabilities from zero-day polymorphic and metamorphic worm exploits (pp. 235–248). https://doi.org/10.1145/1102120.1102152

Dwibedi, S., Pujari, M., & Sun, W. (2020). A Comparative Study on Contemporary Intrusion Detection Datasets for Machine Learning Research (pp. 1–6). https://doi.org/10.1109/isi49825.2020.9280519

Esmaeili, B., Azmoodeh, A., Dehghantanha, A., Srivastava, G., Karimipour, H., & Lin, J. C. (2023). A GNN-Based Adversarial Internet of Things Malware Detection Framework for Critical Infrastructure: Studying GAFGYT, MIRAI, and Tsunami campaigns. *IEEE Internet of Things Journal, 11*(16), 26826–26836. https://doi.org/10.1109/jiot.2023.3298663

Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIOTSET: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. *IEEE Access, 10*, 40281–40306. https://doi.org/10.1109/access.2022.3165809

Friji, H., Mavromatis, I., Sanchez-Mompo, A., Carnelli, P., Olivereau, A., & Khan, A. (2023). Multi-stage Attack Detection and Prediction Using Graph Neural Networks: An IoT Feasibility Study (pp. 620–627). https://doi.org/10.1109/trustcom60117.2023.00095

Fu, M., Pasuksmit, J., & Tantithamthavorn, C. (2025). AI for DevSecOps: A Landscape and Future Opportunities. *ACM Transactions on Software Engineering and Methodology*, *34*(4), 1–61. https://doi.org/10.1145/3712190

Guo, Y. (2022). A review of Machine Learning-based zero-day attack detection: Challenges and future directions. *Computer Communications, 198*, 175–185. https://doi.org/10.1016/j.comcom.2022.11.001

Hussein, A. S., Li, T., Yohannese, C. W., & Bashir, K. (2019). A-SMOTE: a new preprocessing approach for highly imbalanced datasets by improving SMOTE. *International Journal of Computational Intelligence Systems, 12*(2), 1412. https://doi.org/10.2991/ijcis.d.191114.002

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity, 2*(1). https://doi.org/10.1186/s42400-019-0038-7

Kim, J., Bu, S., & Cho, S. (2018). Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. *Information Sciences, 460*, 83–102. https://doi.org/10.1016/j.ins.2018.04.092

Krishnan, D., Singh, S., & Sugumaran, V. (2025). Explainable AI for zero-day attack detection in IoT networks using attention fusion model. *Discover Internet of Things*, *5*(1). https://doi.org/10.1007/s43926-025-00184-8

Lo, W. W., Layeghy, S., Sarhan, M., Gallagher, M., & Portmann, M. (2022). E-GraphSAGE: A Graph Neural Network based Intrusion Detection System for IoT. NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, 1–9. https://doi.org/10.1109/noms54207.2022.9789878

Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., . . . Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications, 232*, 104004. https://doi.org/10.1016/j.jnca.2024.104004

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BAIOT—Network-Based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing, 17*(3), 12–22. https://doi.org/10.1109/mprv.2018.03367731

Messaoud, M. (2025). CLASSIFICATION OF NETWORK TRAFFIC USING MACHINE LEARNING MODELS ON THE NETML DATASET. *International Journal of Computer Networks & Communications, 17*(3), 111–125. https://doi.org/10.5121/ijcnc.2025.17307

Mohideen, M. a. M., Nadeem, M. S., Hardy, J., Ali, H., Tariq, U. U., Sabrina, F., . . . Ahmed, S. (2024). Behind the code: identifying Zero-Day exploits in WordPress. *Future Internet, 16*(7), 256. https://doi.org/10.3390/fi16070256

Nandiraju, S. K. K., Chundru, S. K., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., & Kakani, A. B. (2025). Enhancing Cybersecurity: Zero-Day Attack Detection in Network Traffic with Deep Learning Model. *Asian Journal of Research in Computer Science, 18*(7), 262–273. https://doi.org/10.9734/ajrcos/2025/v18i7734

Redino, C., Nandakumar, D., Schiller, R., Choi, K., Rahman, A., Bowen, E., . . . Weeks, M. (2022). Zero day threat detection using graph and flow based security telemetry. 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 655–662. https://doi.org/10.1109/icccis56430.2022.10037596

Selem, M., & Jmili, F. (2024). A comparative study of CNNs and DNNs deep learning algorithms for enhancing IoT attack detection. In *Lecture notes in networks and systems* (pp. 439–453). https://doi.org/10.1007/978-3-031-64836-6_43

Seo, J., Noh, Y., Kang, Y., Lim, J., Ahn, S., Song, I., & Kim, K. C. (2024). Graph neural networks for anomaly detection and diagnosis in hydrogen extraction systems. *Engineering Applications of Artificial Intelligence, 135*, 108846. https://doi.org/10.1016/j.engappai.2024.108846

Soliman, H. M., Sovilj, D., Salmon, G., Rao, M., & Mayya, N. (2023). RANK: AI-Assisted End-to-End architecture for detecting persistent attacks in enterprise networks. *IEEE Transactions on Dependable and Secure Computing, 21*(4), 3834–3850. https://doi.org/10.1109/tdsc.2023.3338136

Su, Y., & Wang, X. (2024). An Deep Learning-Based Malicious Code Detection System Combining Graph Convolutional Networks and Bidirectional LSTM (pp. 771–774). https://doi.org/10.1109/itnec60942.2024.10732927

Tareq, I., Elbagoury, B. M., El-Regaily, S., & El-Horbaty, E. M. (2022). Analysis of TON-IoT, UNW-NB15, and Edge-IIoT datasets using DL in Cybersecurity for IoT. *Applied Sciences, 12*(19), 9572. https://doi.org/10.3390/app12199572

Wang, Y., Han, Z., Du, Y., Li, J., & He, X. (2025). BS-GAT: a network intrusion detection system based on graph neural network for edge computing. *Cybersecurity, 8*(1). https://doi.org/10.1186/s42400-024-00296-8

Won, D., Jang, Y., & Lee, S. (2022). PLAUsMaL-GAN: Plausible malware training based on generative adversarial networks for analogous Zero-Day malware detection. *IEEE Transactions on Emerging Topics in Computing, 11*(1), 82–94. https://doi.org/10.1109/tetc.2022.3170544

Neetu
Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India.
neetu052phd22@igdtuw.ac.in
ORCID 0009-0009-2075-9771

Deepak Kumar Sharma
Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India.
dk.sharma1982@yahoo.com
ORCID 0000-0001-6117-3464

Koyel Datta Gupta
Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, Delhi, India
koyel.dg@msit.in
ORCID 0000-0001-5887-2475