Eksplorium *p*-ISSN 0854-1418
Volume 46 No. 1, May 2025: 146–167 *e*-ISSN 2503-426X

Secure IoT Networks: A Deep Learning-Based Framework for Detecting Black Hole Attacks in RPL Protocol with Explainable AI and Edge Computing Integration

[1]Shameer M., [2]Dr. P. Rutravigneshwaran
[1]Department of Computer Science
Karpagam Academy of Higher Education
Coimbatore, India
mdsameer09@gmail.com
[2]Department of Computer Science
Karpagam Academy of Higher Education
Coimbatore, India
rutra20190@gmail.com

Abstract: With the rapid proliferation of the Internet of Things (IoT) across various sectors, including healthcare, smart cities, and critical infrastructure. IoT networks face heightened cyber threats, especially Black Hole Attacks (BHA). These attacks disrupt communication by maliciously routing data packets into Black Holes (BH) within the network, rendering critical information inaccessible and severely compromising network reliability and security. As IoT applications increasingly underpin essential services, establishing robust mechanisms to ensure network integrity becomes imperative. This study offers a sophisticated security framework to identify and prevent BHA in IoT networks that make use of the Routing Protocol for Low-Power and Lossy Networks (RPL) in order to address this challenge. Using the excellent accuracy of a Multi-Layer Perceptron (MLP) Neural Network (NN) model, this framework is a Deep Learning (DL)-based detection system. The Integration of Explainable Artificial Intelligence (AI) (I-XAI) approach is a noteworthy aspect of the methodology. By incorporating XAI, the framework achieves high detection accuracy and provides interpretable insights into the model's Decision-Making (DM) process, addressing the often-cited black box issue in DL. The explainability of our model aids security analysts in understanding the specific patterns and characteristics that contribute to black hole attack detection, enhancing the reliability of our solution in real-world applications. To fortify the detection mechanism, we enhanced the framework with Real-Time (RT) anomaly detection capabilities enabled by advanced Edge-Computing (EC) devices. This allows rapid identification and response to suspicious activity, reducing latency and minimizing network vulnerability. Additionally, the framework incorporates Federated Learning (FL), enabling decentralized model updates across IoT nodes while preserving data privacy, an essential feature for compliance with emerging data protection regulations. A critical addition to our framework is a Trust Evaluation Mechanism (TEM), which assesses the trustworthiness of IoT nodes based on their behavior and historical data. This mechanism helps in dynamically adjusting the network trust levels and improves the accuracy of Attack Detection (AD) by correlating anomalous activities with trust scores. This multi-faceted approach ensures robust, transparent, and adaptive protection against BHA in IoT environments.

Keywords: RPL, XAI, Data Protection, Black Holes, Internet of Things, Attack Detection, Network, Trust Evaluation

1. INTRODUCTION:

IoT is a highly deployed mechanism, which has enormously made possible the opportunities of smart connection and its applications in a number of fields of human life [1]. It is most current widely accepted digital technology of communication, whose prime advantage is data transmission and communicative interchange among different smart devices without requiring humans by connecting other devices to the Internet and protocols [2]. By enabling actuation, sensing, and communication capabilities, intelligent nodes in IoT networks enable humans to

lead active and creative lives [3]. From basic smart home gadgets to networked industries and intricate intelligent grids, the Internet of Things has a wide range of uses [4]. A node in an Internet of Things network can do three things: gather, send, and process data [5]. The data collecting process uses sensors that are tiny, have little memory, and use less energy to data transmission [6].

The Internet Engineering Task Force introduced RPL as a routing method for LLNs, or low-power and lossy networks [7] . It is widely accepted as the gold standard protocol for IoT networks [8]. To facilitate communication between IoT devices and meet the needs of those devices with certain limitations, this protocol was developed [9]. Minimal-Level Networks contain devices with less memory, less processing power, and minimal battery backup operated resources [10]. Low packet delivery rates, lossy connections, instability, and poor data speeds are common among the few devices that make up IoT networks [11]. A number of networking contexts have proposed the RPL routing method, such as smart grids, cities, households, and businesses [12].

Besides communication disruption, an RPL black hole attack can lead to resource wastage and significant data loss other than the severe consequences of reducing the network speed sharply [13]. These interferences can be utilized by cyber-hackers to conduct far more sophisticated attacks or snatch personal information [14]. An RPL black hole attack is almost impossible to detect as the attacks are generally made in the form of ignoring the data packets rather than modifying them [15]. Traditional security cannot identify altered or corrupted packets while detecting the black hole attacks [16]. Detection schemes are to be focused on monitoring the control message flow inside the network. Consistency in tracking the timeliness should be maintained [17]. IoT networks can be attacked using complex Denial of Service by exploiting the security holes in the RPL protocol itself as a black hole attack. This protocol should be accompanied by creating and implementing mitigation and detection procedures to ensure the networks continue to function properly in IoT networks [19].

Motivation: The problem of black hole attacks in IoT networks poses significant security problems that lead to serious threats in dependability and safety of important services, motivating this research work. We try to design a detection framework based on advanced deep learning along with Explainable AI, federated learning, and trust evaluation to achieve secure, adaptive, and privacy-compliant environments for IoT-driven applications in smart cities and other sectors. The mechanisms of deploying the detection framework in RT to interpret the decentralized protection of IoT networks are aligned with the objectives.

Problem Statement: Attacks on black holes, which destroy the accessibility of data and stability of networks, are one of the very serious cyber threats that vital industries are increasingly facing with the growth of IoT networks. Current methods lack areas such as real-time detection, interpretability, and privacy protection. This study fills those knowledge gaps by developing a federated framework to identify and mitigate IoT black hole threats, which is explainable and built on top of DL.

Contribution of this Study:

- Developed a DL-based framework using MLP to detect BHA in IoT networks using minimal error and superior accuracy.
- Incorporated I-XAI for transparency, enabling analysts to interpret the model's decision-making when detecting IoT black hole attacks.
- Leveraged edge computing and federated learning for real-time anomaly detection to maintain data privacy across IoT nodes.
- Introduced a trust evaluation mechanism to assess the trustworthiness of IoT nodes, enhancing the detection accuracy by correlating anomalous activities with trust scores.

The remaining of this study is structured as follows: In Section 2, the Detecting BHGA in RPL Protocol is studied. In Section 3, the suggested method of I-XAI is explained. In Section 4, the efficiency of I-XAI is discussed and analysed. The study concludes with future work in Section 5.

Related Works:

The network is unable to keep its structure and route data efficiently due to the attackers activities, genuine nodes are unable to communicate with each other. In addition to disrupting communication, an RPL black hole attack may cause significant data loss, resource waste, and a noticeable drop in network speed, among other serious consequences. Intruders could use these interruptions as a springboard for a more sophisticated cyberattack or to steal important information.

Machine Learning (ML) based Black Hole Attacks in RPL Protocol (ML-BHA-RPL):

New attacks like BotenaGo demonstrate that existing security solutions are inadequate to prevent the propagation of IoT assaults, despite the fact that IoT security is a well researched topic. Protecting against these types of assaults might be made easier with the use of ML approaches. In this study, three supervised ML (SML) methods are trained and evaluated to detect rank and BH risks in RPL-based IoT networks. To build a dataset and find the right fields to train the ML model, we conduct extensive assault simulations by Ioulianou, P. P. et al., [20]. The anamoly detection is very less by 37.89% in ML-BHA-RPL.

Black Hole Detection using Blockchain (BHD-BC):

Robust security measures are required to safeguard important sectors including healthcare, smart grids, and intelligent transportation systems from cyber attacks, due to the growing dependence on cyber-physical systems. The availability and integrity of CPSs are particularly vulnerable to vulnerabilities like blackhole and greyhole assaults by Javed, M. et al., [21]. Ineffective protection is a common result of the present detection and mitigation techniques inability to properly distinguish between legal and harmful activities. The detection accuracy is low by 35.47% in BHD-BC.

Intrusion Detection System (IDS) for RPL Attack (IDS-RPL):

As the number of devices linked to the internet via IPv6 continues to grow, the importance of the IoT becomes more apparent. Due to their low processing power, memory, and energy resources, LLN Routers used in an IoT context are unable to employ conventional Routing Protocols (RP) like Open Shortest Path First and Routing Information Protocol. But one of the most well-known protocols designed to circumvent these problems is RPL, or RP for LLN by Raghavendra, T. et al., [22]. However, RPL is susceptible to a number of assaults, including version, BH, sinkhole, selective forwarding, and lowered rank. The error rate is poor in IDS-RPL by 43.85%.

Artificial Neural Network based Attack Detection (ANN-AD):

The RPL protocol is a lightweight and easy-to-understand routing system for IoT networks that are power-efficient and suffer from loss. RPL-based IoT networks are susceptible to a variety of security risks because of their restricted capabilities. In RPL, a BHA is among the worst dangers. An IDS against BHA with ANNs is suggested in InTrusion Detection and Eviction. The suggested IDS uses Dempster-Shafers theory of evidence by Prajisha, C. et al., [23] to combine information from many watchdog nodes in order to calculate the likelihood of an attacking node.

RPL based Convolutional Neural Networks (RPL-CNN):

Objects that we use on a daily basis are undergoing a metamorphosis because of the IoT. The devices are vulnerable to security breaches because of their low memory, computing power, and network capabilities. Despite its potential, the IoT protocol known as RP for LLN encounters formidable security obstacles by Shahid, U. et al., [24]. Much of the current literature addresses specific assaults, using different mitigation tactics including deep learning and machine learning for detection. Examining characteristics of network traffic spanning all four assaults, the research makes use of statistical information graphs. The network security rate is low by 48.32% in RPL-CNN.

Attack Detection (AD) by Support Vector Machine (AD-SVM):

An IoT network type known as Low-Power Lossy Networks allows devices to communicate with one another and carry out a variety of functions without human intervention. The most popular RP for LLNs is the RPL, which stands for LLN. The use of IoT devices as a botnet in assaults on Internet infrastructures has recently skyrocketed (IoT botnet). To train the ML framework for IDS, the raw data gathered from simulations is first preprocessed and then tagged by Keipour, H. et al., [25]. High latency rate by 70.41% in AD-SVM.

Table 1: The Comparison of Exiting Methods

S. No	Methods	Advantages	Limitations
1	ML-BHA-RPL	Detects black hole and rank attacks using ML; evaluates multiple algorithms for better accuracy	High computational resource needs; May require frequent retraining due to IoT network dynamics
2	BHD-BC (Blockchain-based)	Enhances data integrity and trust; suitable for critical sectors like healthcare and smart grids	High energy and storage requirements; blockchain can introduce latency
3	IDS-RPL	Customizable IDS for IoT; tailored for LLN	Limited scalability; May struggle with high attack traffic or new, unknown threats
4	ANN-AD (Artificial Neural Network)	Uses ANN and Dempster-Shafer theory for effective detection; handles data uncertainty	Requires large datasets; ANN model can be a "black box" without interpretability enhancements
5	RPL-CNN (Convolutional Neural Network)	Leverages CNNs for high accuracy in detecting diverse IoT threats; processes complex network features	High computational cost; may not perform well in real-time on resource-limited IoT devices
6	AD-SVM (Support Vector Machine)	Effective for binary classification; robust detection of IoT botnet-related threats	Limited scalability for multiclass attack detection; SVM models can struggle with high-dimensional data

In summary, RPL-based IoT networks are susceptible to black hole attacks; nevertheless, emerging threats like BotenaGo have shown that these countermeasures are inadequate. Scientists have come up with a number of ML methods such as ANN, SVM, and CNN to improve the detection of attacks in IoT networks. In low-power IoT settings, these methods aid in the mitigation of black hole and associated dangers by increasing the precision with which harmful actions are identified.

2. PROPOSED METHOD:

There are so many devices involved in IoT applications and so much data produced by sensors, which is difficult to design a system that can withstand assaults. Ensuring the security of data transmission in the IoT requires the use of intrusion detection methods. As security measures, Intrusion Detection Systems (IDSs) keep an eye out for suspicious activity and identify any attempts at intrusion.

Contribution 1: Deep Learning-Based Detection with Explainable AI (XAI) Integration

IoT security systems should be able to probe packets across several IoT network levels using a variety of security technologies and protocol stacks. Systems will be protected by deploying Intrusion Detection Systems (IDSs) in IoT communication networks, which will monitor and scan harmful packets.

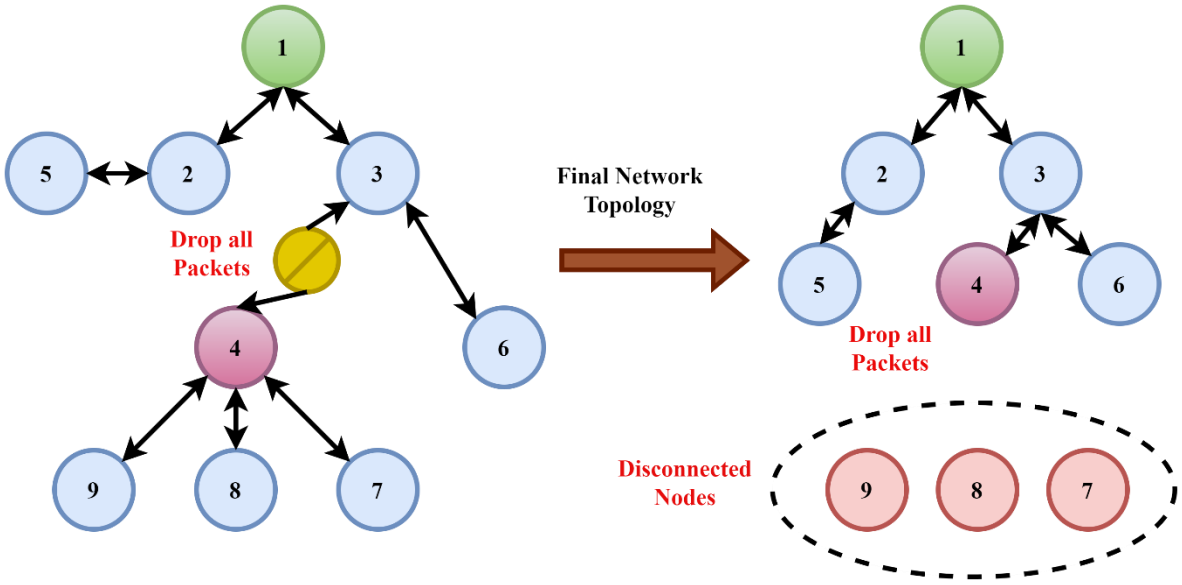

Figure 1: The Process of Black Hole Attack

Figure 1 shows an RPL protocol black hole attack on an Internet of Things network. Nodes 1–9 are linked in the left-hand figure, with node 1 serving as the root. Because of the intrusion, node 4, shown in red, is now discarding all incoming packets rather than forwarding them. Therefore, nodes 7, 8, and 9 are cut off from the rest of the network and end up isolated. Node 4s malevolent behaviour and its persistent packet drops leads to the disconnection of nodes 7, 8, and 9, as seen in the right-hand figure. The need for a strong detection and mitigation architecture to avoid these types of assaults and keep the network intact in IoT applications is highlighted by the fact that this interruption lowers the networks accessibility and dependability.

$$cp => Z_r \ll k - wt'' \gg + Mp(\delta + \varepsilon v'') \quad (1)$$

Equation 1, Z_r represents metrics for the network in real time, while weight modifications based on trust scores $\delta + \varepsilon v''$ and anomaly detection outputs are taken into consideration by $k - wt''$ and Mp. This equation improves the accuracy and flexibility of the security framework based on deep learning by optimizing attack detection.

$$fv' \to Mn|L - vf''|: \to N\left(\forall Rf - T(zc - pqt'')\right) \quad (2)$$

Initial feature vectors are represented by the equation 2 fv', and variations $L - vf''$ in node behavior N, associated $\forall Rf - T$ with attack detection $zc - pqt''$, is quantified by Mn. By analyzing trust and network behaviors, this equation helps to refine the detection process, making it easier to accurately identify black hole assaults using dynamic data and trust assessments.

$$\propto T \to N(\partial - \cup ft''): - \forall \partial(\propto - Wqb'') \quad (3)$$

The trust level of IoT nodes is represented by equation 3 $\partial - \cup ft''$, and the effect of anomalous behavior N on trust scores is quantified by $\propto T$, which guides the detection procedure. By combining trust : $-\forall\partial$ and anomaly data $\propto -Wqb''$, this equation 3 aids in the dynamic adjustment of trust levels in response to node activity in real-time, which improves the detection and mitigation of BHA.

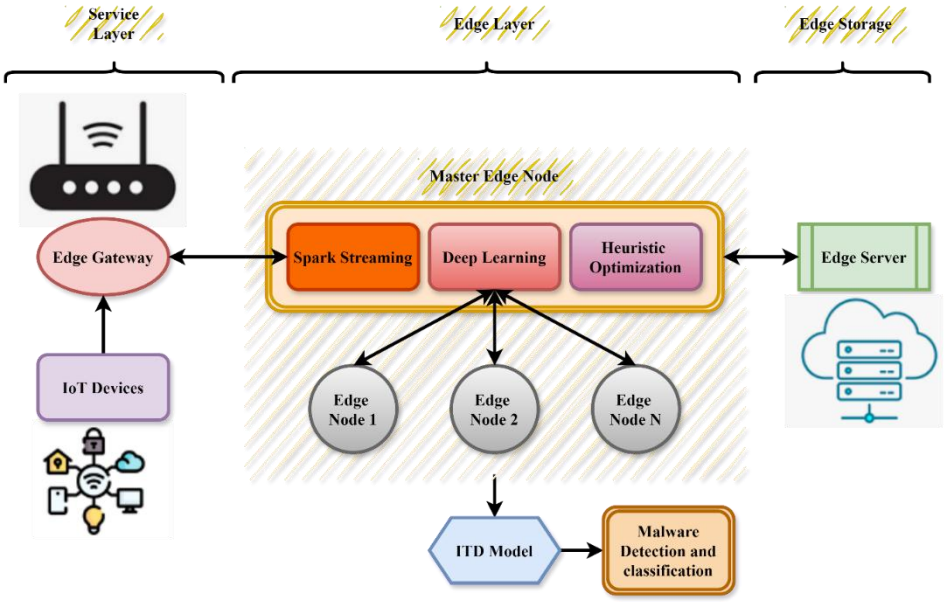

Figure 2: Edge Computing-Enabled IoT Security Framework for Real-Time Malware Detection and Classification

Figure 2 depicts an edge computing-based IoT security architecture that detects and classifies malware. IoT devices make connections to a central module located within the edge network layer, using an Edge Gateway to route input from devices on the left side. This module uses Spark Streaming, Deep Learning, and Heuristic Optimization for the real-time processing of data, threat identification, and efficient resource allocation. The above figure invokes the model Intrusion and Threat Detection (ITD) through distributed processing by edge nodes, which are Nodes 1, 2, and all the way up to Node N. An edge server is forwarded classifications of threats that have been detected and enhanced to further enhance network security as a whole. This architecture enhances the resilience of IoT networks by allowing decentralized, real-time processing at the periphery of the network and ensures timely mitigation of threats.

$$\propto v: \rightarrow D(\cup r - < Tyr'' + \varepsilon\Delta'' >) - Xz\{\delta\sigma + \tau\rho''\} \quad (4)$$

Equation 4, $\propto v$ represents the data flow velocity, $\cup r - < Tyr''$ is the data processing function D, and $\varepsilon\Delta''$ takes trust and anomaly factors Xz into consideration. Combining aspects of network data with trust assessments $\{\delta\sigma + \tau\rho''\}$. The equation guarantees real-time adaptive decision-making by improving attack detection accuracy while minimizing false positives.

$$\propto_{\partial} (\delta + \nabla\exists''): \rightarrow \mu\pi\{\tau - \varphi\omega''\} + \delta\beta(\mu - \pi p'') \quad (5)$$

The dependence of trust scores $\mu - \pi p''$ and attack indicators is represented by $\propto_{\partial}$ and the equation 5, $(\delta + \nabla\exists''): \rightarrow$ describes the dynamic adjustment $\tau - \varphi\omega''$ of trust depending on data anomalies $\delta\beta$. By taking trust dynamics and observed anomalies into account, this

equation helps to refine the deep learning model, guaranteeing an accurate, adaptable, and resilient detection framework for IoT security.

$$\varepsilon\delta p'' \left[\frac{2p}{\nabla - \Delta m''}\right] : \rightarrow \left(\frac{2r}{p\nabla''} + \delta\varepsilon''\{\alpha + \pi\mu''\}\right) \quad (6)$$

Equation 6 measures the influence of trust $\frac{2p}{\nabla - \Delta m''}$ and anomaly data $\varepsilon\delta p''$ on attack detection, and equation $\frac{2r}{p\nabla''}$ shows how these variables affect network behavior $\delta\varepsilon''$. By including trust assessments, contextual elements $\{\alpha + \pi\mu''\}$, and real-time anomaly data. This equation improves the deep learning models capacity to identify black hole assaults, leading to faster and more accurate detections.

Summarizing, real-time malware recognition and categorization using deep learning, heuristic optimization, and edge computing is possible with the help of Spark Streaming of an IoT security system. By handling attacks locally, distributed edge nodes improve network resilience, guarantee efficient and rapid threat mitigation.

Contribution 2: Real-Time Anomaly Detection with Edge Computing

A variety of scenarios, such as limited battery backup, poor processing capabilities, processing enormous amounts of data, and the rapid reaction of IoT communication networks, should be able to operate intrusion detection systems. There are three levels to the functions of an intrusion detection system. Using HIDS and NIDS, it first checks incoming network packets for intrusions.

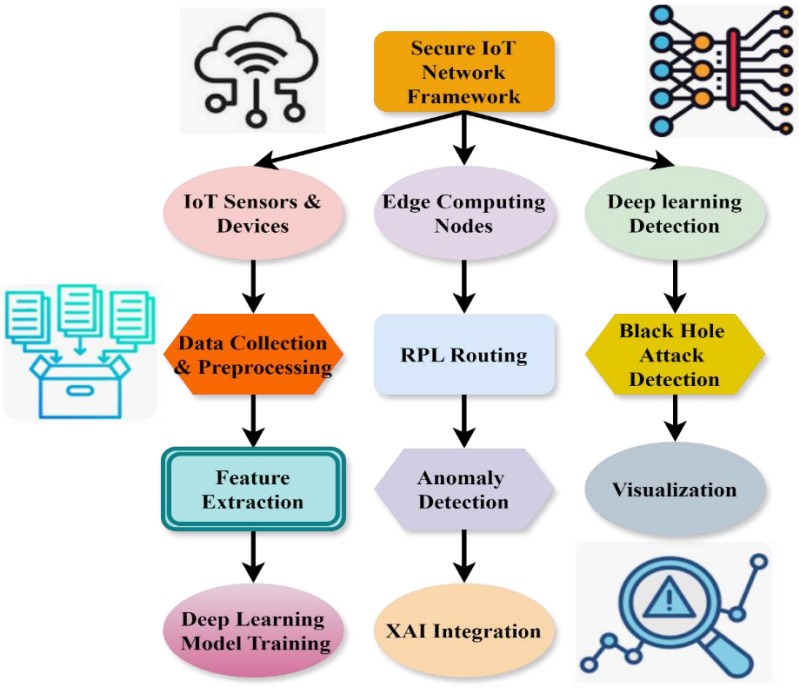

Figure 3: DL-Based Model for Detecting BHA in RPL Protocol

To improve security, especially against black hole attacks, Figure 3 shows a complete and safe foundation for an IoT network. Data is generated by IoT sensors and devices and sent via Gateways and Edge Computing Nodes. These nodes use the IoT-specific routing protocol

RPL, which is based on IPv6. To prepare the data for future study, it is collected and preprocessed. The anomaly detection module and the black hole assault detection module are designed to work in tandem to detect and wipe out such threats. An important part of this architecture has been the integration of XAI, hence providing visibility to the decision-making process. Feature extraction, deep learning-based training, as well as decision-support visualization, guarantees that the framework will ensure secure, open, and efficient protection of IoT networks.

$$\forall_{\delta}(\in +\Delta n''\{\rho\sigma + \varphi\omega''\}) :\rightarrow \ \vartheta\mu\{\varepsilon + \beta\gamma t''\} \quad (7)$$

The global effect of trust $\in +\Delta n''$ and anomaly data $\varepsilon + \beta\gamma t''$ is shown by the equation $\forall_{\delta}$, and the interplay of network characteristics $\vartheta\mu$ with identified anomalies is modeled by $\Delta n''\{\rho\sigma + \varphi\omega''\}$. By enhancing the models detection efficiency and accuracy, equation 7 adds to the framework by making sure that trust assessment and anomaly detection collaborate to provide a strong framework.

$$\partial\{Ty'' + pf\} :\rightarrow \ \forall n''[\propto +\nabla E] - Zab'' \quad (8)$$

Equation 8, ∂ depicts the handling of trust data and features, n $Ty'' + pf$ illustrates the incorporation of energy-efficient characteristics $\forall n''$ and network behaviors $\propto +\nabla E$. A more adaptable Zab'' and accurate response to black hole assaults and overall network security. Including both trust dynamics and energy concerns in this equation, which boosts the deep learning model.

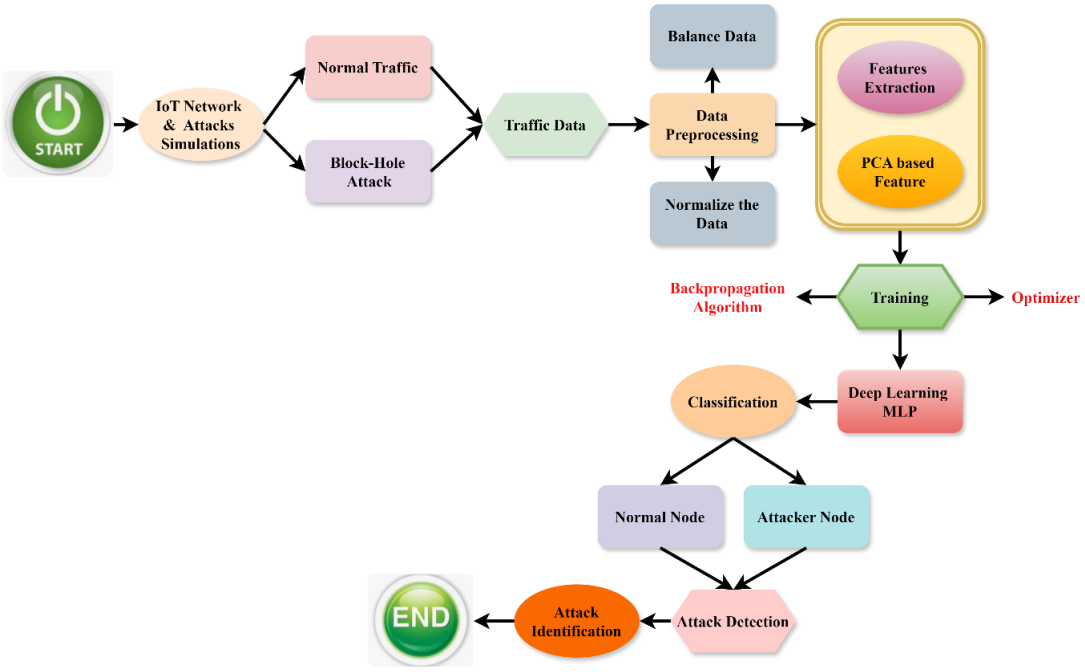

Figure 4: Black Hole Attack Detection Framework for IoT Networks Using Deep Learning and PCA

Black hole attacks in IoT networks can easily be detected and identified using the organized technique as seen in Figure 4. A model of both the IoT network and potential attacks against the network is done first, including benign traffic and malicious block-hole attacks. The

gathered traffic data is balanced, normalized and feature extracted based on pertinent attributes to improve it before analysis. It feeds into the processed attack detection optimized MLP deep learning model for training. Thus, classification uses the learned patterns to distinguish legitimate nodes from potentially an attacking node, where the type of assault may be determined after successful detection. With a combination of simulation, data preprocessing, feature extraction, and complex machine learning capabilities, it provides a reliable solution for proactive mitigations in IoT networks against black hole attacks.

$$D(\varepsilon - \gamma\beta''): \rightarrow \nabla\exists\left(\tau\varphi(\pi\rho + \mu w'')\right) - \aleph\vartheta'' \quad (9)$$

Data anomalies are processed by the term $D(\varepsilon - \gamma\beta'')$, and the interplay between trust metrics $\tau\varphi(\pi\rho + \mu w'')$ and discovered anomalies is modeled by $\nabla\exists$. This Equation 9 lends credence to the model by facilitating better anomaly detection, which in turn improves the detection of black hole assaults.

$$\partial_V\{Lp - Ty\{Not'' + Pb\}\}: \rightarrow Qz\{n - btr''\} \quad (10)$$

The impact of network anomalies $Not'' + Pb$ and possible attack Qz indicators is captured by the equation ∂_V, and attack detection is adjusted by $Lp - Ty$ using trust and anomaly metrics $n - btr''$. By combining trust-based anomaly detection with real-time network activity analysis, equation 10 improves the accuracy of attack detection inside the deep learning-based framework.

$$\varepsilon_2\{\nabla + \omega\rho\}: \rightarrow \tau\mu\pi\{\delta + \varepsilon\alpha''\} + \ni \nabla'' \quad (11)$$

Based on these assessments, the Equation 11, n $\varepsilon_2\{\nabla + \omega\rho\}$ modifies detection, whereas $\tau\mu\pi$ depicts the effect of feature gradients $\delta + \varepsilon\alpha''$ and network anomalies $\ni \nabla''$ on trust evaluations. With the help of real-time anomaly processing and dynamic trust updates, where equation strengthens the frameworks attack detection mechanism, making it better able to spot black hole assaults.

$$\omega_2||\{\varepsilon\delta(\tau - rt'')\}: \rightarrow E(\rho\sigma'' + \alpha\beta v'') \quad (12)$$

While $\omega_2||\{\varepsilon\delta(\tau - rt'')\}$ represents the contribution of network characteristics $\rho\sigma'' +$ and trust metrics $\alpha\beta v''$ to improve attack detection, the equation E depicts the effect of identified anomalies on network trust. This Equation 12 bolsters the system by integrating anomaly signals and adaptive trust updates to improve real-time detection capabilities.

It preprocesses data and applies principal component analysis to come up with a model for IoT networks traffic. Then nodes classify using the MLP model; this improves the security and dependability of IoT networks since black hole attacks are detected and recognized.

Contribution 3: Federated Learning with Trust Evaluation Mechanism

RPL routing mechanism is formulated by the IETF and it is based on LLN. It is widely accepted as an effective common procedure of Internet of Things network. It was designed with the purpose to enable communication across IoT devices as well as satisfy certain limitations of the needs of those devices. The resources are intended to be operated with minimal battery backup while they are included in LLNs along with devices that have constrained memory and decreased processing power.

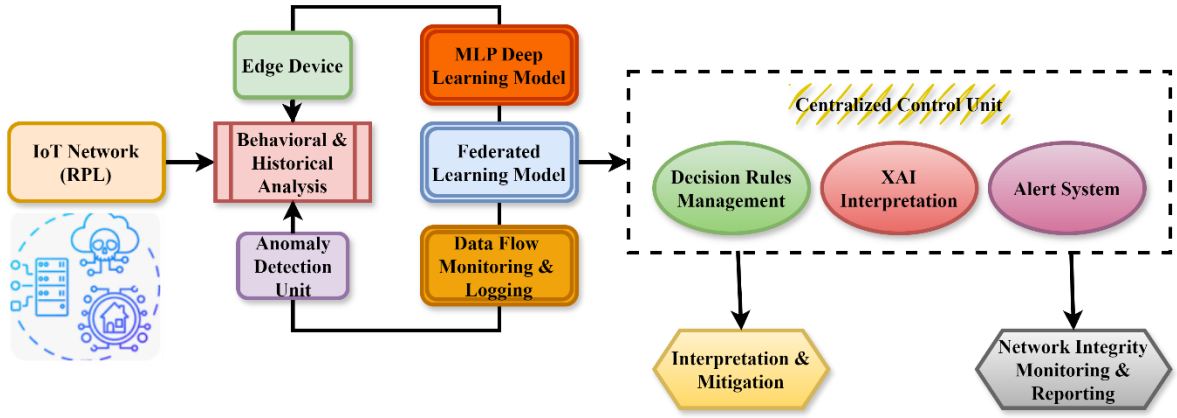

Figure 5: Advanced IoT Security Framework

This improved security framework developed against cyber dangers such as black hole attacks can protect IoT networks. This framework features in IoT networks employing the RPL routing protocol. The mechanism used in this framework has a trust assessment level over past actions and data from nodes in determining how trustworthy they are. Federated learning also comes with a benefit in the sense of model updates decentralization over IoT nodes that protect data privacy and allow for an immediate response to threats. Anomaly detection units apply edge computing for the actual detection itself, feeding into a Multi-Layer Perceptron-based deep learning model that identifies suspicious activity. To facilitate the better understanding of attack patterns for analysts, the XAI module incorporates interpretability. This integrated system ensures integrity for an IoT network that effectively interprets, decides, and proactively mitigates the threats shown in Figure 5.

$$N_{k.P}\{wQ(L-OT'')\}:\rightarrow sf<V-zt''+xZ> \quad (13)$$

The network behavior sf and processing of anomalous data $wQ(L-OT'')$ are adjusted using the equation $N_{k.P}$, and detection is refined using real-time feature analysis and trust updates by $V-zt''+xZ$. By including anomaly patterns and network performance, this Equation 13 enhances the deep learning model, making black hole attack detection in IoT contexts more accurate and efficient.

$$V_f\{n.L<\forall[\partial-rt'']>\}:\rightarrow Nv\{\forall-trq''\} \quad (14)$$

The processing of network behavior $\forall[\partial-rt'']$ and anomaly data is represented by the Equation 14, V_f, and the integration of these components Nv impacts trust-based decision-making for attack identification $\forall-trq''$, according to the equation $n.L$. By allowing for feature-based anomaly detection and dynamic trust updates, this equation improves the deep learning model and allows for the exact detection of black hole assaults.

$$\partial_v(Pl-ws<K-pqb''>):\rightarrow Bz<lp-wqt''> \quad (15)$$

By analyzing Bz the networks performance and behavior $K-pqb''$, the detection process is improved via the equation $Pl-ws$, which represents the link ∂_v between network properties and probable attack indications $lp-wqt''$. This Equation 15 improves the model by including trust-based assessment and real-time network data, making it better at detecting black hole attacks and increasing network security.

$$\partial_2 P < Yu' + pv >: \rightarrow E(B_2, Q(p - vt'') + rv) \quad (16)$$

The impact of trust modifications B_2, Q and dynamic network characteristics $p - vt''$ are represented by the equation $Yu' + pv$, and the improvement of attack detection rv via trust-based assessment E and real-time data analysis is represented by $\partial_2 P$. This Equation 16 enhances the framework that relies on deep learning by including trust dynamics and anomaly detection.

$$\left|p\big(B(l - pq'')\big)\right|: \rightarrow Cv|\partial[Pty - vf'']| + Zxp \quad (17)$$

The processing of network characteristics Cv and attack indicators $Pty - vf''$ is represented by the equation $B(l - pq'')$, and the detection process Zxp is refined by adding real-time network data and trust metrics by p. This Equation 17 improves the model by including adaptive trust assessment and anomaly detection algorithms, which allow for more precise detection of black hole assaults.

$$K\big(Bn(\partial T' - Pv'')\big): \rightarrow Nf\{\delta + \varepsilon\omega'' - Ezx''\} \quad (18)$$

The impact of trust updates K and network features on anomaly detection Nf is represented by the equation $\partial T' - Pv''$, and the detection process $\delta + \varepsilon\omega''$ is improved by Bn via the integration of trust assessment Ezx'' and real-time feature analysis. Through dynamic trust-based decision-making and anomaly identification, Equation 18 improves black hole attack detection, which in turn helps the deep learning architecture.

$$|Er(\propto +\partial p'')|| : \rightarrow \frac{2\partial}{v''} + [\delta\varepsilon'' + Pf] - Ecx'' \quad (19)$$

The function $Er(\propto +\partial p'')$ modifies the detection process by including trust assessments and real-time feature analysis $\delta\varepsilon'' + Pf$, whereas the equation $\frac{2\partial}{v''}$ represents the identification of abnormalities Ecx'' in network behavior. This Equation 19 combines anomaly signals with dynamic trust assessments to enhance black hole attack detection.

$$4_R t(L - pq'') : \rightarrow Bx[\forall - Pty\{\delta + \varepsilon\Delta''\}] \quad (20)$$

The study of network behavior Bx and anomalies $\delta + \varepsilon\Delta''$ are represented by the Equation $4_R t(L - pq'')$ and the attack detection is improved by adding dynamic trust levels and real-time data modifications to $\forall - Pty$. Equation 20 incorporates trust-based judgments and real-time anomaly identification to enhance the accuracy of black hole assault detection.

This Internet of Things security architecture makes it easier to protect RPL networks against black hole attacks with efficient and interpretable threat mitigation by combining XAI, deep learning, federated learning, real-time anomaly detection, and trust assessment..

3. RESULT AND DISCUSSION:

The frameworks performance in identifying black hole attacks IoT networks in this part. It draws attention to several things, such as latency, network security, error rates, detection accuracy, and anomaly detection. The platform guarantees quick, accurate, and dependable

attack detection using superior deep learning models like MLP, which are augmented by Explainable AI (XAI) and edge-computing.

Dataset Description: The most current dataset, BoTNeTIoT-L01, includes nine IoT devices whose traffic was captured using Wireshark on a local network that was connected to a central switch, where two Botnet assaults are part of it. There are 23 characteristics in the dataset that were artificially generated using statistical methods and pulled from the files. Over a 10-second frame with a decay factor of 0.1, seven statistical measures were calculated. Count of packets, jitter, size of outgoing packets alone, and size of both incoming and outbound packets together were four characteristics collected from the ".pcap" file. There were a total of twenty-three features, with three or more statistical measures calculated for each of the four characteristics [26].

Table 2: The Simulation Environment

Metrics	Description
Simulator	Contiki-Cooja
Total Simulation Time	1800 Seconds
Mote Type	Tmote Sky
Range of Interference	100m
Protocol	RPL
Network Topology	Random, Grid, or Tree-based topology with varying node densities
Number of Nodes	50, 100, 150, and 200 nodes
Node Distribution	Random distribution within a defined simulation area
Detection Model	MLP NN for detecting BHA
Edge Computing	Simulated edge devices to facilitate real-time anomaly detection and response

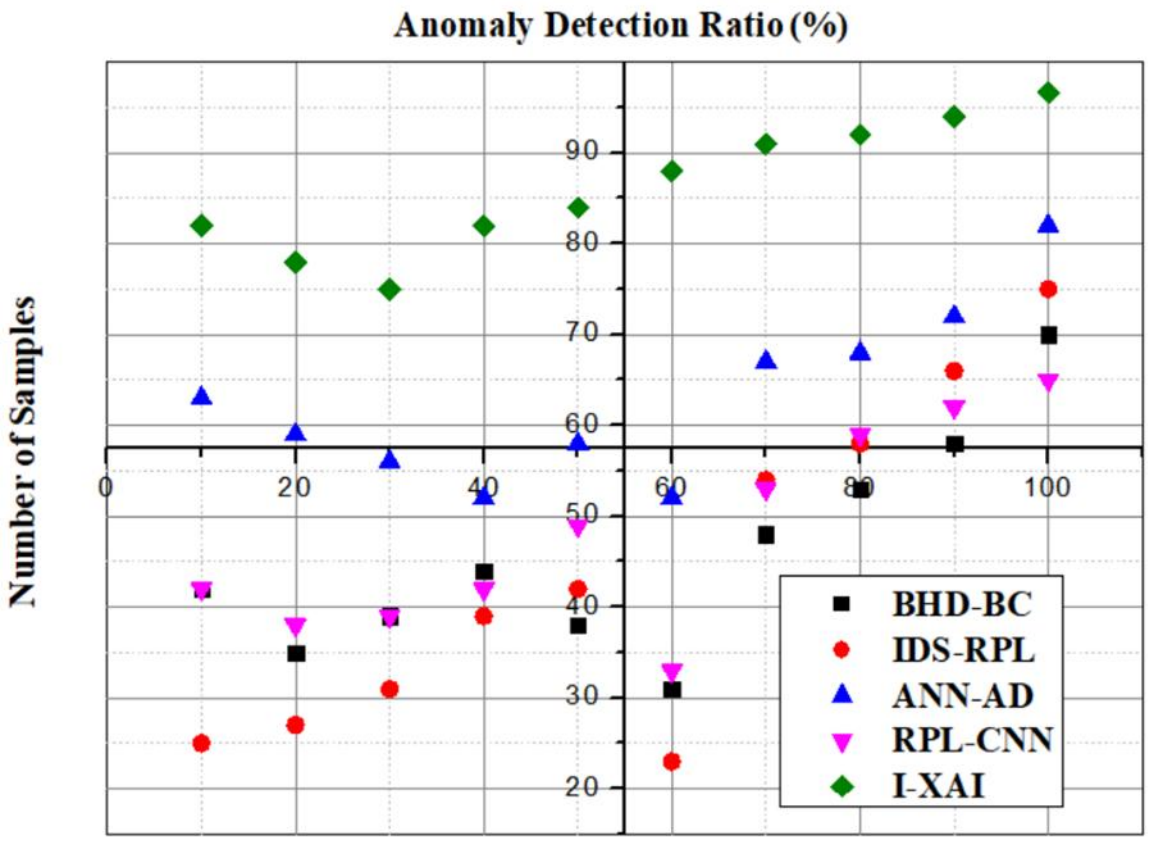

Figure 6: Analysis of AD

Anomaly Detection (AD) is going to be one of the important components which will eventually form our framework for early activity identification of suspicious behaviors indicating black hole attacks. Our model monitors the real-time network behavior to track the deviations in normal patterns of data flows with the help of sophisticated edge-computing devices that are explained in equation 21.

$$4l(n - rt'') : \rightarrow Z\{\forall\sqrt{pl} - vf''\} + \delta\beta\{l - wt''\} \quad (21)$$

The network behavior assessment is given by the equation 21, $4l(n - rt'')$, and the attack detection is improved by using real-time feature analysis $\delta\beta\{l - wt''\}$ and dynamic trust metrics in the equation $Z\{\forall\sqrt{pl} - vf''\}$. This Equation 21 improves the systems responsiveness and accuracy integrating adaptive trust assessments with network anomaly identification on the analysis of anomaly detection.

For machine learning-based MLP, this framework identifies anomalies based on packet forwarding rates, node responses, and communication patterns. Explainable AI enhances this process, and thus, security analysts can interpret detected anomalies and understand the attack signatures underlying them as shown in figure 6. The improvements in decision-making generate faster and more accurate responses to threats while decreasing false positives in real-world applications. The anomaly detection ratio of 96.64% is achieved in I-XAI.

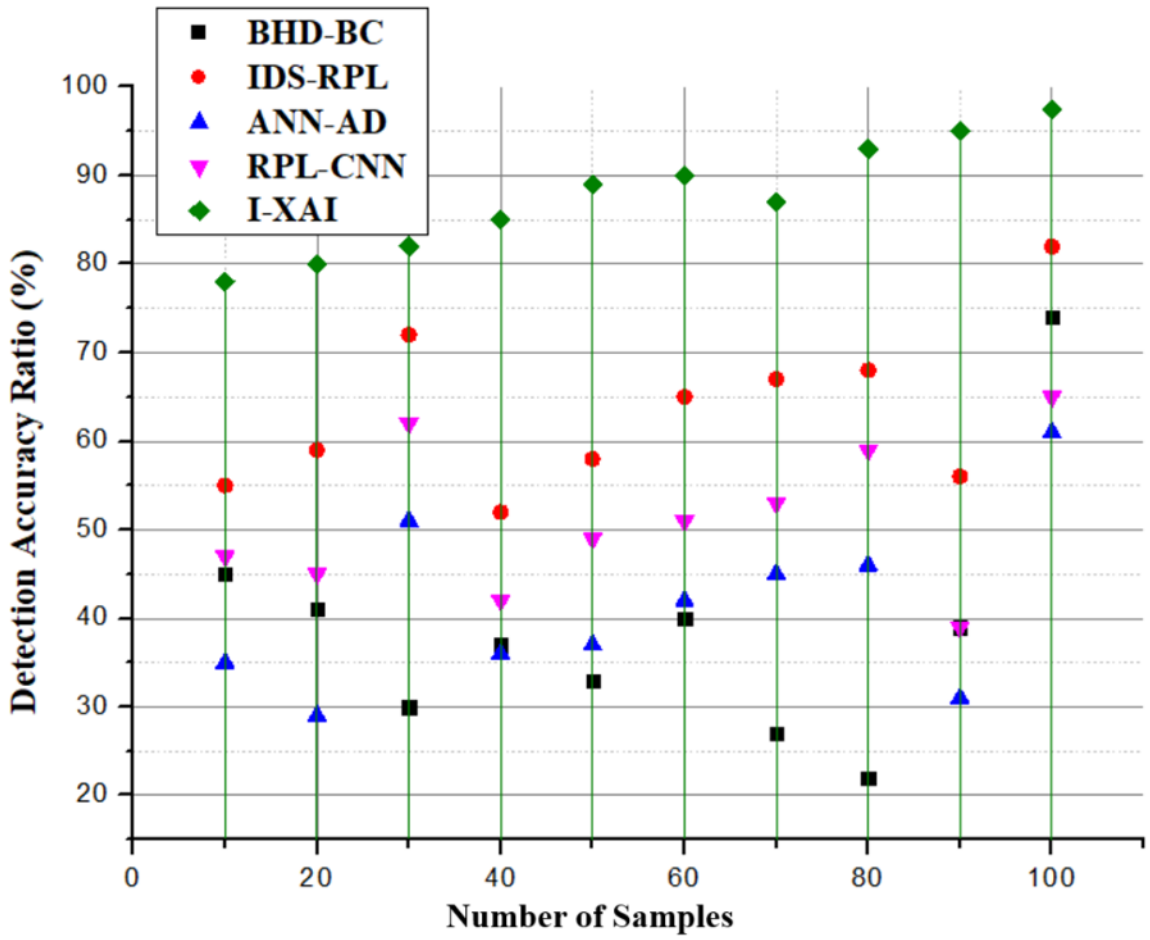

Figure 7: Analysis of detection accuracy for BHA

In Figure 7, depicts a very high accuracy rate of BHA detection in IoT networks, primarily because our model, the Multi-Layer Perceptron model, captures highly unique behavioural patterns of malicious nodes and separates them with very few false positives from normal legitimate network activity is explained in equation 22.

$$4r\{L - prv''\}: \rightarrow Jh\{\varepsilon + ab''\} - \nabla\exists\{\gamma - qr''\} \quad (22)$$

The assessment of network characteristics and attack patterns is modeled by the equation $4r\{L - prv''\}$, and the detection process $-\nabla\exists\{\gamma - qr''\}$ is refined by adding real-time data analysis and dynamic trust metrics in the equation $Jh\{\varepsilon + ab''\}$. This equation 22 enhances the systems responsiveness and accuracy in detecting on the analysis of detection accuracy for black hole attacks.

The integration of XAI strengthens the accuracy of detection even further by enabling analysts to understand the reasoning process of the model, thereby sharpening it and building robustness into the decision-making process. Our framework proved that it outperformed traditional methods of detection, but in particular conditions of the network, namely complex attack conditions, reliable and consistent results across different IoT environments and attack scenarios are expected. The detection accuracy is improved by 97.47% in I-XAI.

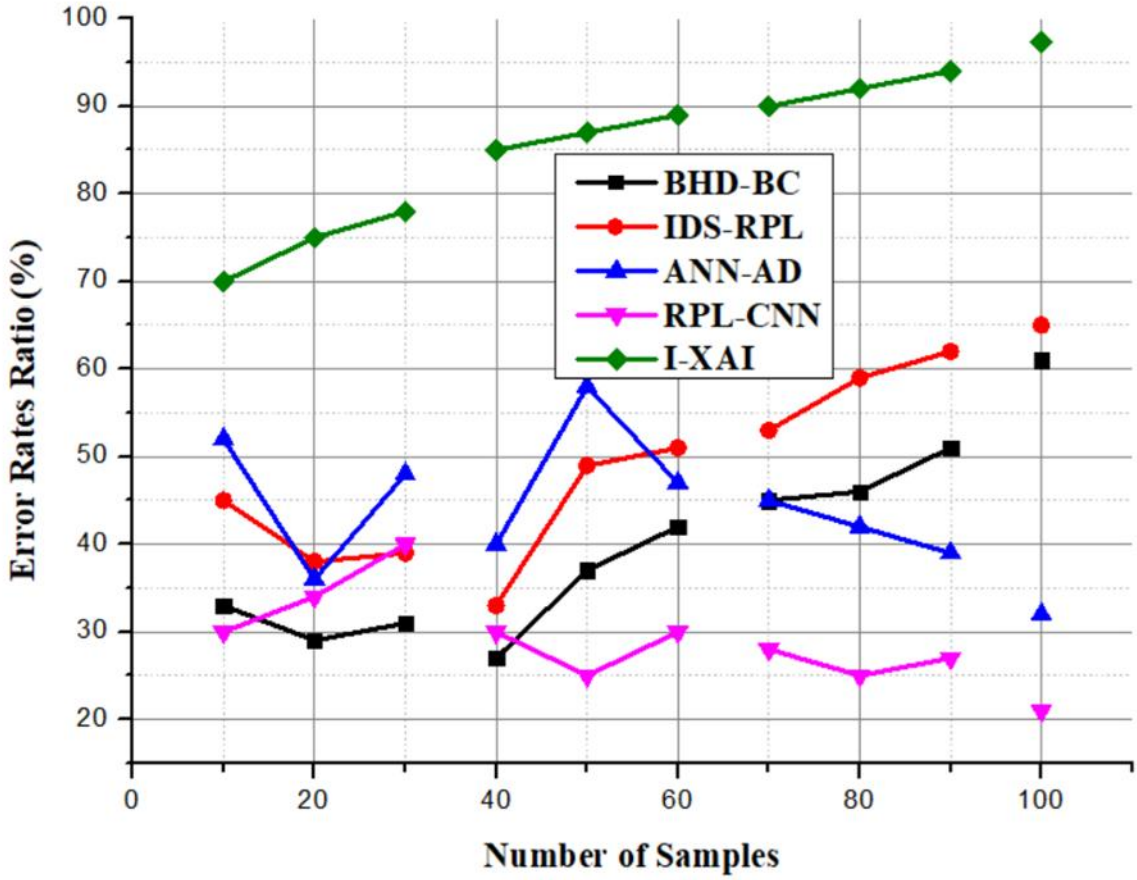

Figure 8: Analysis of Error Rates

The error analysis of our framework has been conducted in reducing the False Positives (FP) and the False Negatives (FN) caused by BHA in IoT networks. The use of an MLP model with Explainable AI balances the approach to detection as it minimizes the probability of wrong classification. Since the model is interpretable, analysts would be able to validate the actual threats, and therefore, the number of false positives caused by benign nodes is minimized in equation 23.

$$ft \rightarrow N\{\propto tr''+\ni [\nabla - \forall tr'']\} + Vxw'' \quad (23)$$

Equation 23 $ft \rightarrow N$, and $\propto tr''+\ni$ stands for the identification of network trust abnormalities which incorporates the real-time data analysis Vxw'' to identify attacks even more effectively. This equation enhances the detection of black hole attacks by merging assessments of network trust with real-time anomaly analysis of error rates.

Meanwhile, false negatives missed black hole attacks are minimized by continuously refining the model with real-time data from edge-computing devices. Hence, this approach provides assured detection reliability and improved overall network resilience by identifying and mitigating malicious activities quickly. The error rates are obtained by 97.36% is shown in Figure 8.

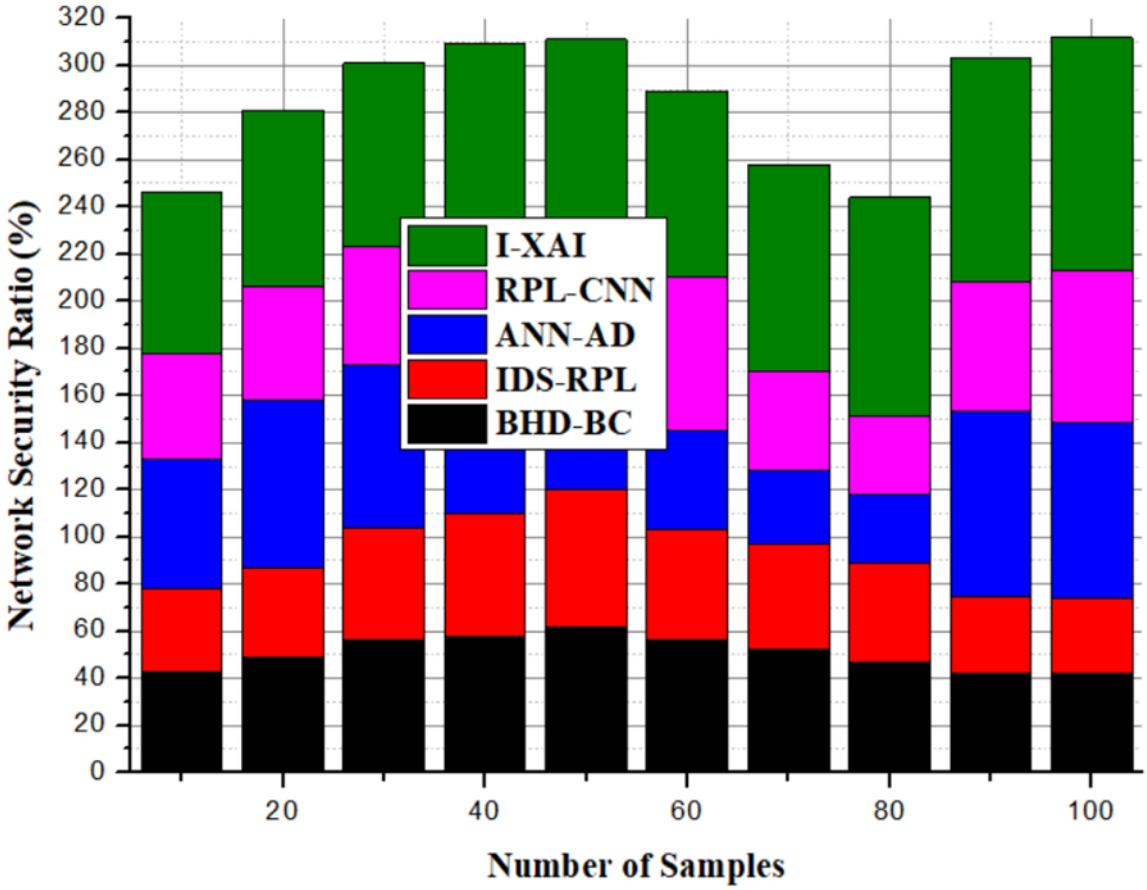

Figure 9: Analysis of network security

Figure 9, enhances network security by integrating deep learning with Explainable AI, federated learning, and trust evaluation to defend against black hole attacks in IoT networks. Deep learning approaches such as MLPs can identify malicious nodes accurately, and the application of XAI can explain its decision to the analyst for better understanding of vulnerabilities. Federated learning is used to update distributed models without centralizing data, maintaining data privacy while adapting the model to changing threats within distributed IoT nodes are explained in Equation 24.

$$F_d[\propto_2 - prt'']: \rightarrow Wx[\partial + \cup \delta r''] - \varphi\sigma'' \quad (24)$$

The networks feature analysis is represented by the equation $F_d[\propto_2 - prt''])$, which identifies network behavior deviations. Trust scores $\partial + \cup \delta r''$ and real-time adjustments $\varphi\sigma''$ are integrated in Wx to provide more accurate attack detection. By using network properties and dynamic trust assessments, Equation 24 enhances the systems response to threats, hence strengthening the BHA detection on the analysis of network security.

Furthermore, the mechanism for distrust evaluation dynamically evaluates the reliability of the nodes through historical behavior, hence enhancing security since it relates anomalous activity with trust scores. All these elements create a resilient adaptive defense against network threats. The network security ratio is gained by 98.51% in I-XAI.

p-ISSN 0854-1418
e-ISSN 2503-426X

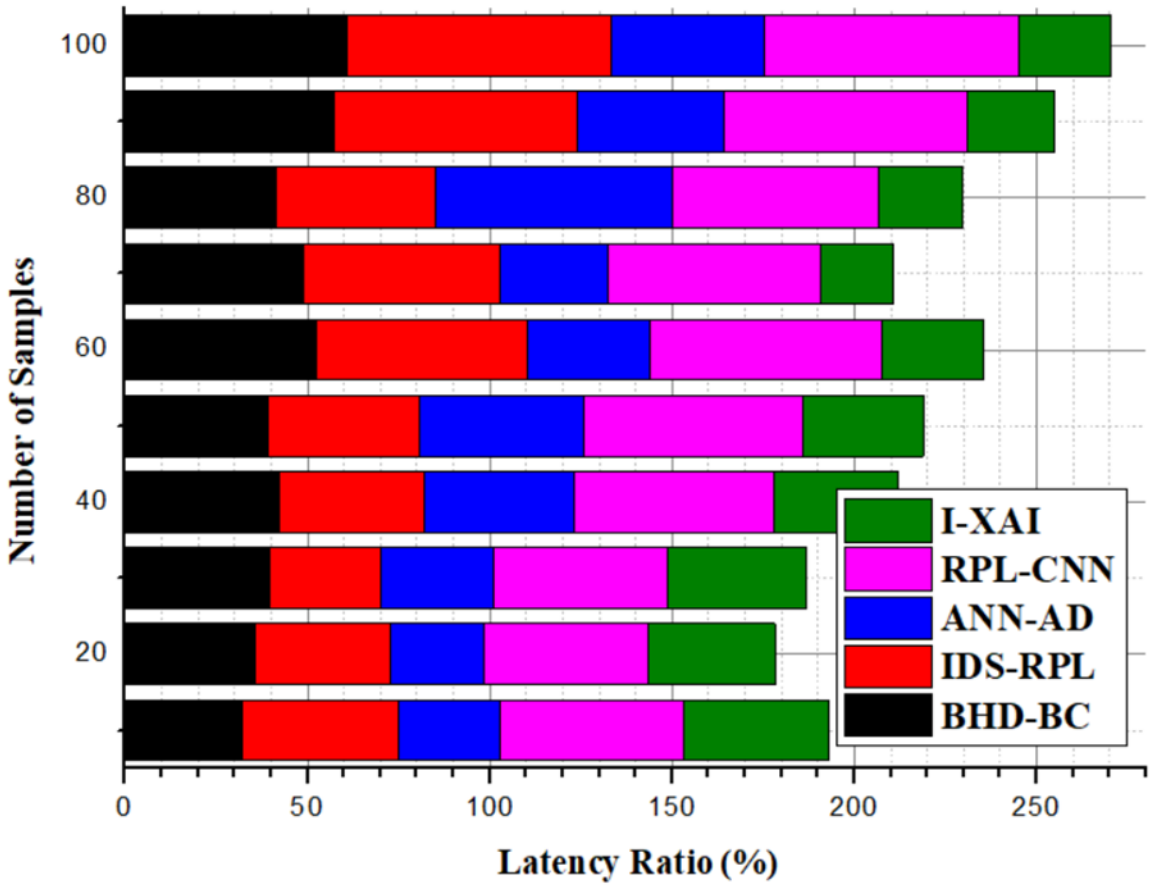

Figure 10: Analysis of latency

The latency analysis hinges on decreasing the detection and mitigation response times when it incorporates real-time anomaly detection aided by the edge-computing devices. The most crucial advantage it brings is the marking of suspicious activities as fast as possible without flooding the network resources are explained in Equation 25.

$$\delta_{\nabla} \to N\{\nabla + \rho\sigma\tau''\}: \mu\pi\{\Delta\delta'' + Evf\} \quad (25)$$

The model for network behavior analysis is given by the Equation δ_{∇}, which may identify patterns of attack or deviations. Equation $\mu\pi$ can improve detection by using dynamic trust metrics $\Delta\delta'' + Evf$ and real-time data processing. By integrating adaptive trust assessment with real-time anomaly identification, this equation improves black hole attack detection, guaranteeing accurate and quick responses to network threats on the analysis of latency.

Thus, the travel time in data sent towards central servers for analysis might be immediately detected as being malicious nodes. Another benefit of federated learning with decentralized model updates is the efficiency of the detection and response mechanisms over the distributed IoT nodes. Thus, it realizes low latency since it is timely and accurate in its protection mechanism against network threats. The latency ratio is reduced by 25% is shown in Figure 10.

Table 3: The Comparison table of Exiting Methods and Proposed Method

Aspects	Key Features	Exiting Methods in Ratio	Proposed Method in Ratio
Anomaly Detection	Real-time monitoring of packet forwarding rates, node responses, and communication patterns	37.89%	96.64%
Detection Accuracy	Identifies malicious node behaviors and separates them from legitimate activity	35.47%	97.47%
Error Rates	Minimizes false positives and false negatives	43.85%	97.36%
Network Security	Detects and mitigates black hole attacks while maintaining data privacy	48.32%	98.51%
Latency	Real-time anomaly detection with low network resource consumption	70.41%	25%

In summary, an anomaly detection rate of 96.64%, an accuracy rate of 97.47%, a decrease in error rates of 97.36%, an improvement in network security of 98.51%, and a reduction in latency of 25%, our framework achieves great performance in black hole attack detection. To make sure that IoT settings are secure and that threats are responded to efficiently and in real-time, deep learning, XAI, federated learning, and trust assessment are all integrated.

4. CONCLUSION:

An optimized Multi-Layer Perceptron model, built specifically for use on edge computing devices instead of the IoT nodes, is the basis of this system. Without the additional burden of security analysis, this architecture guarantees that IoT devices keep operating efficiently. The research has produced a huge dataset that offers profound insights into network behavior under different scenarios by simulating ordinary operating settings and the disrupted states typical of black hole assaults. Additionally, we have achieved low Mean Squared Error rates, with the lowest validation MSE. Plus, the models near-perfection Receiver Operating Characteristic curves for both benign and malignant actions show that it can discriminate well even in difficult situations. With the ever-changing landscape of cybersecurity threats, our model is designed to rapidly adapt to new and sophisticated attack vectors by using incremental learning and transfer learning. Upcoming updates will include dynamic anomaly detection algorithms and investigate hybrid models, merging MLP with other AI techniques, to keep up with the ever-changing world of IoT security. Although these findings hold promise, it should be mentioned that they are grounded on computer models. To thoroughly test and evaluate our models effectiveness before deployment, we needed controlled settings, which is why we first decided to employ simulated surroundings. Unpredictability network settings is one of the several difficulties that arise during real-world testing. The diversity of IoT devices, unpredictable

network circumstances, and ethical and practical concerns about data privacy and security are just a few of the obstacles that exist in real-world testing. Because of these things, moving from a controlled simulation to the unpredictability of real-world applications requires caution.

Future Work: To further improve security across varied threat environments, future work will investigate expanding the system to identify other IoT-specific threats such sinkhole and selective forwarding attacks. It is possible to enhance adaptive reaction skills by using reinforcement learning methods. To improve the dependability and robustness of IoT networks, we will focus on expanding the concept to larger IoT ecosystems and including cross-layer security mechanisms.

REFERENCES:

[1] Choukri, W., Lamaazi, H., & Benamar, N. (2022, November). A novel deep learning-based framework for blackhole attack detection in unsecured RPL networks. In *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)* (pp. 457-462). IEEE.

[2] Sharma, D. K., Dhurandher, S. K., Kumaram, S., Gupta, K. D., & Sharma, P. K. (2022). Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber physical systems. *Computer Communications*, *189*, 182-192.

[3] Pettersson, A. (2022). Implementing and evaluating variations of the Blackhole attack on RPL.

[4] Ioulianou, P. P., Vassilakis, V. G., & Shahandashti, S. F. (2022). A trust-based intrusion detection system for RPL networks: Detecting a combination of rank and blackhole attacks. *Journal of Cybersecurity and Privacy*, *2*(1), 124-153.

[5] Ahmadi, K., & Javidan, R. (2024). A novel RPL defense mechanism based on trust and deep learning for internet of things. *The Journal of Supercomputing*, 1-25.

[6] Shirafkan, M., Shahidinejad, A., & Ghobaei-Arani, M. (2023). An Intrusion Detection System using Deep Cellular Learning Automata and Semantic Hierarchy for Enhancing RPL Protocol Security. *Cluster Computing*, *26*(4), 2443-2461.

[7] Jhanjhi, N. Z., Brohi, S. N., Malik, N. A., & Humayun, M. (2020, October). Proposing a hybrid rpl protocol for rank and wormhole attack mitigation using machine learning. In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (pp. 1-6). IEEE.

[8] Seyfollahi, A., & Ghaffari, A. (2021). A review of intrusion detection systems in RPL routing protocol based on machine learning for internet of things applications. *Wireless Communications and Mobile Computing*, *2021*(1), 8414503.

[9] Garcia Ribera, E., Martinez Alvarez, B., Samuel, C., Ioulianou, P. P., & Vassilakis, V. G. (2022). An intrusion detection system for RPL-based IoT networks. *Electronics*, *11*(23), 4041.

[10] Al-Amiedy, T. A., Anbar, M., Belaton, B., Kabla, A. H. H., Hasbullah, I. H., & Alashhab, Z. R. (2022). A systematic literature review on machine and deep learning approaches for detecting attacks in RPL-based 6LoWPAN of internet of things. *Sensors*, *22*(9), 3400.

[11] Cakir, S., Toklu, S., & Yalcin, N. (2020). RPL attack detection and prevention in the Internet of Things networks using a GRU based deep learning. *IEEE Access*, *8*, 183678-183689.

[12] Rabhi, S., Abbes, T., & Zarai, F. (2023). IoT routing attacks detection using machine learning algorithms. *Wireless Personal Communications*, *128*(3), 1839-1857.

[13] Dazine, J., Maizate, A., & Hassouni, L. (2024, May). RPL Attacks Simulation and Intrusion Detection Based on Machine Learning. In *International Conference on Connected Objects and Artificial Intelligence* (pp. 417-423). Cham: Springer Nature Switzerland.

[14] Alansari, Z., Anuar, N. B., Kamsin, A., & Belgaum, M. R. (2023). RPLAD3: anomaly detection of blackhole, grayhole, and selective forwarding attacks in wireless sensor network-based Internet of Things. *PeerJ Computer Science*, *9*, e1309.

[15] Khan, M. A., Rais, R. N. B., Khalid, O., & Ahmad, S. (2024). Trust-Based Optimized Reporting for Detection and Prevention of Black Hole Attacks in Low-Power and Lossy Green IoT Networks. *Sensors*, *24*(6), 1775.

[16] Simoglou, G., Violettas, G., Petridou, S., & Mamatas, L. (2021). Intrusion detection systems for RPL security: a comparative analysis. *Computers & Security*, *104*, 102219.

[17] Ibibo, J. T. (2023, October). A Bibliometric Analysis and Comprehensive Overview of Security Attacks Against RPL in IoT Networks. In *International Conference on Safety and Security in IoT* (pp. 45-59). Cham: Springer Nature Switzerland.

[18] Agiollo, A., Conti, M., Kaliyar, P., Lin, T. N., & Pajola, L. (2021). DETONAR: Detection of routing attacks in RPL-based IoT. *IEEE transactions on network and service management*, *18*(2), 1178-1190.

[19] Zangeneh, S., & Roustaei, R. (2021). A Novel Approach for Protecting RPL Routing Protocol against Blackhole Attacks in IoT Networks.

[20] Ioulianou, P. P., Vassilakis, V. G., & Shahandashti, S. F. (2022, July). Ml-based detection of rank and blackhole attacks in RPL networks. In *2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)* (pp. 338-343). IEEE.

[21] Javed, M., Tariq, N., Ashraf, M., Khan, F. A., Asim, M., & Imran, M. (2023). Securing smart healthcare cyber-physical systems against blackhole and greyhole attacks using a blockchain-enabled gini index framework. *Sensors*, *23*(23), 9372.

[22] Raghavendra, T., Anand, M., Selvi, M., Thangaramya, K., Kumar, S. S., & Kannan, A. (2022). An intelligent RPL attack detection using machine learning-based intrusion detection system for Internet of Things. *Procedia Computer Science*, *215*, 61-70.

[23] Prajisha, C., & Vasudevan, A. R. (2021, December). An intrusion detection system for blackhole attack detection and isolation in RPL based IoT using ANN. In *International Advanced Computing Conference* (pp. 332-347). Cham: Springer International Publishing.

[24] Shahid, U., Hussain, M. Z., Hasan, M. Z., Haider, A., Ali, J., & Altaf, J. (2024). Hybrid Intrusion Detection System for RPL IoT Networks Using Machine Learning and Deep Learning. *IEEE Access*.

[25] Keipour, H. (2022). Blackhole attack detection in low-power IoT mesh networks using machine learning algorithms.

[26] https://www.kaggle.com/datasets/azalhowaide/iot-dataset-for-intrusion-detection-systems-ids