International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group| 9th ICAILLMBA (ALLAM) 2025-Conference Proceedings
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.ICAILLMBA-103

Original Article

Enhancing Security and Trust in IoT Networks with Blockchain-Enabled OGANN for Malicious Node Detection and Trust Management

Koda Dileep Kumar[1], Prof. Kunjam Nageswara Rao[2], Repaka Hanudeep[3]
[1]Research Scholar, Department of CS & SE, Andhra University College of Engineering, Andhra University, Visakhapatnam, India.
[2]Professor, Department of CS & SE, Andhra University College of Engineering, Andhra University, Visakhapatnam, India.
[3]Student, Department of CSE, Rajiv Gandhi University of Knowledge Technologies, Srikakulam, India.

***Abstract* - *The Internet of Things (IoT) connects a large number of devices to exchange data and support different applications. As the number of connected devices increases, security problems such as fake nodes, malicious behavior, and lack of trust among devices are becoming more common. These issues mainly arise because IoT networks are distributed in nature and do not rely on a centralized authority. To address these challenges, this paper presents a security framework that uses Blockchain technology along with an Optimized General Additive Neural Network (OGANN). In this approach, information related to a node, such as its identity details and behavior during communication is taken as input. When a new IoT node tries to enter the network, its identity is checked through smart contracts on the Blockchain which helps in stopping unauthorized access. After joining the network, the behavior of the node is continuously monitored and given to the OGANN model to identify malicious activities. Based on the model output, the node is classified and a trust value is assigned accordingly. All important events such as authentication results, trust updates, and detection alerts are stored on the Blockchain so that the records cannot be altered. Nodes whose trust value goes below a fixed threshold are considered suspicious and may be isolated from the network. Simulation results show that the proposed method improves security and helps in maintaining trust among IoT devices while reducing incorrect detection.*

Keywords* - *Iot Security, Blockchain, Generalized Additive Neural Networks, Malicious Node Detection, Trust Management, Identity Management.

1. Introduction

The Internet of Things (IoT) is expanding rapidly as a large network of different devices that connect and communicate data everywhere. These devices are used in areas like smart homes, factories, healthcare, and transportation. Although IoT offers immense benefits, such as turning data into useful actions, this massive connectivity makes security very difficult. The system is simply vast and spread out. We cannot use old traditional security methods that focus on protecting just one central border.

A big problem is that IoT devices are all different having very limited resources (such as small batteries or weak processors). This makes them easy targets for smart cyber-attacks such as spoofing (pretending to be another device), denial-of-service (DoS) attacks (shutting down the network), stealing data, or Sybil attacks (creating fake identities). Also, relying on one main (centralized) security point does not work. If that single point fails, the whole system is at risk. This method cannot handle all the fast, huge amounts of data. We need a strong, decentralized system to check identities and keep track of which devices can be trusted.

Blockchain technology is a great solution to these trust issues. It offers a de-centralized, non-temporary, and public record that securely saves device identities and trust scores. Using smart contracts, Blockchain lets devices prove their identity and manage trust openly without needing one central authority, thus removing the risk of a single point of failure. However, Blockchain is too slow to find complex new threats in real-time, and blockchain cannot do it alone. The time and power needed to check blocks and agree on the network state means it cannot act as a quick alarm system.

To fix this gap, we need smart learning systems. Machine learning (ML) models are needed to look at complex network traffic and find irregular actions that signal new attacks. We use General Additive Neural Networks (GANNs) because they can model complex data accurately while remaining easy to understand. Our research uses an Optimized General Additive Neural Network (OGANN). We improve the OGANN with special tuning methods to make it very accurate at finding bad actions, while still being fast enough for resource-limited IoT devices.

This paper introduces the Blockchain-OGANN (BC-OGANN) security system. It uses the best parts of both technologies: Blockchain keeps the device identities and trust records safe and decentralized, while the OGANN quickly and accurately detects bad behavior in real-time. Our main goal is to create a strong, self-managing system where new trust scores are written securely onto the Blockchain. This framework aims to be scalable, intelligent, and strong enough to manage device trust and fight new security threats as they happen.

This proposed system influences the strengths of Blockchain in maintaining resistance identity and trust records, and OGANNs in detecting malicious node behavior with high accuracy and low computational overhead. The agenda to build an extensible, intelligent and resilient IoT network framework that can autonomously manage trust and identity, and reduce security threats as they emerge.

2. Problem Statement

The security and trust integrity of IoT networks are increasingly compromised by malicious nodes that exploit system vulnerabilities. Existing trust and identity management systems are often centralized, making them prone to single points of failure, and they lack adaptability to dynamic threats. Blockchain provides a decentralized and tamper-proof framework for identity management and trust establishment, eliminating dependence on a single authority. At the same time, Deep Learning neural networks OGANN can be used for intelligent malicious detection, analyzing features like packet transmission rates, data flow consistency, energy consumption, and communication frequency to accurately distinguish between benign and malicious nodes. By combining blockchain's decentralized trust with DL-based anomaly detection, the system achieves scalable, secure, and adaptive protection for IoT networks.

3. Related Work

Researchers have put more effort into using Blockchain for secure IoT systems. Some works mainly focus on decentralized identity management with smart contracts, while others use Blockchain for secure data transmission and discovery. For example, Conoscenti et al. [1] carried out a detailed review showing that Blockchain is well suited for decentralized IoT applications, as it removes single points of failure and improves transparency.

On the machine learning side, anomaly detection has been widely used to find abnormal activities in IoT networks. Models such as SVM, Random Forest, and CNN have shown good results in finding different attacks. For example, Median et al. [2] showed that deep autoencoders can catch IoT botnet traffic with pretty high accuracy. However, these methods still face problems such as high false positives, and they do not adjust well to the fast-changing nature of IoT systems.

In recent years, some work has tried to mix Blockchain with ML. Lu and Xu [3], for instance, proposed a Blockchain-based system that uses ML algorithms for adaptive IoT security. It worked well, but the issue is that deep learning models often need heavy computation, and public Blockchains come with their own scalability limits.

When it comes to trust and identity management, most older systems rely on centralized or rule-based methods. These are not very strong against evolving threats. Newer work introduced behavior-based trust scoring, but these still lack the flexibility and intelligence required for dynamic IoT networks. In general, while progress has been made, there is still a gap in connecting lightweight, interpretable, and optimized neural models with decentralized trust and identity frameworks. Few studies consider optimization strategies for neural networks along with Blockchain based dynamic trust management. Our work aims to fill this gap by presenting an OGANN driven malicious node detection system that is embedded in a Blockchain network for real time, decentralized identity and trust handling in IoT.

4. Literature Survey

4.1. N. Anita and M. Vijayalakshmi, "Blockchain security attack: a brief survey," ICCCNT, 2019

This paper presents a concise survey of security attacks targeting blockchain systems. It categorizes attacks across different layers (network, consensus, smart contracts, etc.) and explains how issues such as double spending, selfish mining, and 51\% attacks can undermine the reliability of blockchain based applications. The main understanding is that the threat surface of blockchain itself rather than on IoT scenarios. While highly useful to understand potential vulnerabilities of the underlying ledger that our framework relies on, it does not propose a concrete defense architecture for IoT or a data driven malicious node detection mechanism.

- Merits: Provides a structured classification of blockchain specific attacks, helping designers understand where blockchains can fail. Highlights limitations of common consensus protocols and smart contract vulnerabilities. Serves as a reference for selecting appropriate mitigation strategies when integrating blockchain into larger systems (like IoT).
- Demerits: Does not target IoT networks or trust management explicitly focus on blockchain only. Lack of quantitative or experimental evaluation analysis is primarily descriptive. Does not integrate machine learning or anomaly detection no end-to-end security framework is proposed.

4.2. P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," FGCS, 2018

Sharma and Park propose a hybrid network architecture for smart cities that combines blockchain with traditional cloud and edge components. The architecture separates data into different layers (e.g. public vs. private chains) to improve scalability and manage heterogeneous smart city applications. The work shows how blockchain can provide integrity and auditability for smart city services but concentrates on high level system design rather than fine grained malicious node detection. Compared to our OGANN based model, this architecture does not embed an intelligent trust scoring or anomaly detection component for IoT nodes.

- Merits: Introduces a hybrid blockchain architecture (public/private) suitable for large scale smart city environments. Addresses scalability and interoperability among heterogeneous IoT services in urban settings. Demonstrates how blockchain can support data integrity and secure sharing among multiple stakeholders.
- Demerits: Focuses mainly on architectural design little attention to detecting malicious IoT nodes or dynamic trust management. No integration of machine learning models for anomaly detection or adaptive security. Evaluation is limited, with few detailed performance metrics under adversarial conditions.

4.3. L. Liu, Z. Ma, and W. Meng, "Detection of multiple mix attack malicious nodes using perceptron-based trust in IoT networks," FGCS, 2019

This work directly tackles malicious node detection in IoT by proposing a perceptron-based trust model. It computes trust scores from multiple behavioral features (e.g., packet forwarding, communication reliability) and uses a perceptron classifier to identify nodes performing multiple mixed attacks. The model is relatively lightweight and suitable for constrained IoT devices. However, trust values and decisions are still managed in a largely centralized manner, and the interpretability and optimization of the neural component are limited compared with our OGANN based approach embedded in blockchain.

- Merits: Specifically addresses multiple mixed attacks from malicious IoT nodes rather than single attack scenarios. Uses a simple perceptron-based trust model that is computationally light and suitable for resource constrained devices. Provides quantitative results showing improved detection compared with purely rule based trust schemes.
- Demerits: Trust and identity information are not anchored on blockchain hence, they remain vulnerable to tampering and single points of failure. The Perceptron model is less expressive and less interpretable than optimized generalized additive neural networks. Evaluation is typically on limited scale testbeds scalability and resilience in large, highly dynamic IoT environments are not fully validated.

4.4. H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: a survey," IEEE IoT J., 2019

Dai et al. provide a comprehensive survey of how blockchain can be applied to IoT, covering architectures, consensus mechanisms, security features, and application domains such as smart homes, smart grids, and supply chains. The paper systematically examines benefits (decentralization, immutability) and challenges (scalability, latency, energy) when blockchains are integrated into IoT. While very valuable as a conceptual mapping of the field, the survey does not design or experimentally evaluate a particular malicious node detection or trust management solution, and machine learning driven approaches are only discussed at a high level.

- Merits: Offers a broad and structured overview of blockchain IoT integration, including architectural patterns and use cases. Clearly summarizes key challenges such as scalability, privacy, and resource constraints, which inform the design of practical frameworks. Helps position new solutions (like our Blockchain OGANN framework) within the broader research landscape.
- Demerits: Purely survey oriented no concrete implementation or performance evaluation is provided. Does not go deeply into ML based anomaly detection or optimized neural architectures for IoT security. Limited discussion of fine-grained trust management combining behavioral analytics and blockchain storage.

4.5. M. T. Hammi et al., "Bubbles of Trust: A decentralized blockchain based authentication system for IoT," Comput. Secur., 2018

Hammi et al. propose "Bubbles of Trust," a decentralized authentication system in which IoT devices are grouped into logical "bubbles." Every bubble uses blockchain to control identities and authentication operations in a well distributed way hence removing the central authority and reducing single point of failure risks. The model is effective for safe identity verification of devices. However, the focus is primarily on authentication; it does not maintain dynamic behavior-based trust scores or integrate ML models for detecting malicious actions after authentication, which is an important aspect taken care of in our OGANN based framework.

- Merits: Introduces a decentralized, blockchain backed authentication mechanism specially made for IoT environments. "Bubble" organization increases scalability and localizes trust decisions and so improves manageability. Reduces dependency on centralized identity providers and improves resistance to identity spoofing attacks.
- Demerits: It mainly focuses on initial authentication and group management but not on continuous monitoring of node behavior. Lacks a machine learning or anomaly detection component for detecting affected nodes within a bubble.

Trust is largely static (based on membership) so without dynamic scoring or feedback from network behavior as in our Blockchain OGANN scheme.

5. Proposed Framework

Our framework mainly brings together three big parts to make IoT networks safer and more trustworthy:

- A blockchain based identity and trust system,
- An OGANN-powered malicious node detection engine, and
- A feedback-driven trust evaluation setup.

The full design is decentralized and lightweight, so it can run well even on limited IoT devices.

5.1. OGANN-Based Detection Module

The detection model uses an Optimized Generalized Additive Neural Network (OGANN). It combines the nonlinear linear capabilities of neural networks with interpretability of Generalized Additive Models. This model is trained on various features like packet transmission rates, data flow consistency, energy consumption patterns, and communication frequency.

Optimization techniques like Genetic Algorithms (GA) or Particle Swarm Optimization (PSO) are used to fine-tune the neural network parameters to improve accuracy and adaptability. This makes the model differentiate between normal and anomalous behaviors of nodes effectively despite network conditions being changed with time. The detection process consists of:

- Feature extraction from IoT node behavior.
- OGANN-based classification of nodes as benign or malicious.
- Continuous learning through online training mechanisms.

5.2. Trust Management System

Trust in this framework is dynamically evaluated based on both past behavior and real-time detection outcomes. Each node is assigned a trust score, which is calculated by combining:

- Historical data (past interactions and reputation)
- OGANN detection output (real-time anomaly score)
- Peer feedback (consensus from neighboring nodes)

Trust scores are modified periodically and sorted on the Blockchain. Nodes with constantly low scores are noted and scheduled from network communication until reapproved. This trust mechanism also supports recovery strategies for falsely noted nodes, increasing fairness and resilience.

- A new IoT node tries to join the network.
- The Blockchain layer verifies the identity of the node using smart contracts and authenticates.
- The node's behavior is supervised continuously and fed into the OGANN detection model.
- Based on the OGANN output result the node is classified and its trust score updated.
- All relevant transactions (authentication, trust update, anomaly alert) are updated on the Blockchain.
- Nodes with trust scores below a certain threshold are pointed for further inspection or isolation.

This multi-layered approach enables real-time, intelligent, and tamper-proof security operations in IoT networks.

6. Methodology

The proposed method uses blockchain based authentication and a learning driven mechanism combinely for detecting malicious nodes in Internet of Things (IoT) networks. The total workflow includes IoT network simulation, secure identity management using a permissioned blockchain, malicious node detection using an Optimized Genetic Artificial Neural Network (OGANN), and hyperparameter tuning with help of Particle Swarm Optimization (PSO).

6.1. IoT Network Simulation and Data Collection

An IoT network was simulated to study node behavior under both normal and adversarial conditions. The simulation includes 500 nodes in total, where 450 nodes operate as legitimate devices and 50 nodes exhibit malicious behavior. Malicious nodes were designed to perform actions that are commonly seen in IoT attacks, including excessive packet transmission, selective packet dropping, identity spoofing, and message manipulation.

During network operation, communication and operational parameters were recorded and noted for each node. Based on this data, a set of features was extracted to mimic node behavior. These features consist of transmission rate, energy consumption, message integrity, frequency of communication with neighboring nodes, and routing consistency. The chosen features capture differences in traffic patterns, abnormal energy usage, and inconsistencies in routing behavior, which are signs of malicious activity.

6.2. Blockchain-Enabled Authentication and Trust Handling

To ensure secure authentication and tamper proof trust management, a permissioned blockchain framework was deployed using Hyperledger Fabric. The permissioned architecture limits the network participation only to authenticated nodes, hence reducing the possibility of unauthorized access.

Smart contracts were designed to oversee node identities and maintain trust scores. Each node is given a unique identity at the time of registration. Whenever a node is involved in network communication, its identity is confirmed and verified through the blockchain. Trust scores are updated based on observed behavior and detection results, and all updates are recorded on the distributed ledger. This mechanism ensures transparency, integrity, and prevention of single point failures in trust management.

6.3. OGANN-Based Malicious Node Detection

To ensure secure authentication and tamper proof trust management, a permissioned blockchain. Malicious node detection is performed using an Optimized Genetic Artificial Neural Network. The extracted feature vectors are used as inputs to the neural network model. The dataset is divided into training and testing subsets, in 70:30 ratio respectively with 70\% of the data is used for training and the remaining 30\% is for testing.

Let input feature vector be expressed as

$$\{\ \mathrm{X}\ \} = [\ X_1, X_2, \ldots., X_n\ ] \tag{1}$$

Where n denotes the number of features.

The activation of a hidden neuron is computed as

$$h_j = f\left(\sum_{i=1}^{n} w_{ij}x_i + b_j\right) \tag{2}$$

Where w_{ij} represent connection weight and b_j is bias term, and $f(.)$ is the activation function.

Genetic operations such as crossover, selection and mutation are applied to make the neural network parameters better. The fitness of each candidate solution is calculated based on classification performance, allowing the model to progressively improve detection accuracy while avoiding premature convergence.

6.4. Hyperparameter Optimization Using Particle Swarm Optimization

To make the learning efficiency of the OGANN model better, Particle Swarm Optimization is used to optimize key hyperparameters, including learning rate, number of hidden neurons, and activation function choice. In PSO, each particle represents a potential hyperparameter configuration.

The velocity and position of a particle are updated according to

$$v_i^{t+1} = wv_i^t + c_1r_1(p_i^t - x_i^t) + c_2r_2(g_i^t - x_i^t) \tag{3}$$

$$x_i^{t+1} = x_i^t + v_i^{t+1} \tag{4}$$

Where 'w' represents the inertia weight, c_1 and c_2 represents acceleration coefficients, r_1 and r_2 are random values in the interval [0,1], p_i is the personal best position, and g is the global best position.

The fitness function is described using detection accuracy on validation data. Through repeated updates, PSO converges toward an optimal set of hyperparameters that makes classification performance much better.

6.5. Decision Feedback and Trust Update

After classification, the detection output for each node is sent to the blockchain layer. Based on the result, the related smart contract changes the node's trust score. Nodes classified as malicious experience a decrease in trust and are restricted from connecting to the network communication, while benign nodes retain or improve their trust values. This process between the detection model and blockchain ensures continuous security enforcement and trusted authentication within the IoT network.

7. Critical Survey

The existing literature on blockchain enabled IoT security presents valuable contributions. Traditional blockchain surveys such as Anita and Vijayalakshmi [4] primarily focus on vulnerabilities in blockchain architectures but do not propose remedies for securing IoT nodes or detecting behavioral anomalies. Although these analyzes improve understanding of blockchain limitations, they do not provide mechanisms for trust evaluation or adaptive attack detection within IoT ecosystems.

Sharma and Park [5] demonstrate hybrid designs for smart cities that give importance to scalable blockchain integration but lack tools for monitoring node activity. These architectures are more prone to insider attacks and gradual changes of malicious behavior. Similarly, Liu et al. [6] present a perceptron-based trust model to detect mixed attacks however, the simplicity of the perceptron limits expressiveness, decreasing detection accuracy under high data difference. The absence of decentralized trust storage makes your system more vulnerable to tampering and single-point failures.

Surveys like Dai et al. [7] provide a deeper overview of blockchain IoT convergence, but did not specify operational security solutions that use blockchain with machine learning based malicious detection. Adding Hammi et al. 's "Bubbles of Trust" [8] provides a decentralized authentication technique that addresses simply identity verification rather than continuous harmful conduct. The static nature makes the solution not good for contexts in which nodes may become compromised after authentication.

Overall, the major limitations identified across existing research include:

- Absence of non-static malicious node detection after initial onboarding.
- Lack of intelligible ML architectures capable of capturing sophisticated IoT behavior.
- Limited integration of trust computation with decentralized records.
- Scalability issues in existing frameworks due to centralization or weak trust maintenance.
- Lacking required standards of protection against mixed and modern attack strategies.

The proposed Blockchain OGANN architecture addresses these problems by using an optimized generalized additive neural network to describe behavioral trust in an interpretable and adaptive way. The design prevents tampering by recording trust values, notifications, and interactions on a blockchain, which eliminates the need for a central authority. When compared to conventional perceptron-based models, the OGANN model outperforms between mixed attacks more accurately. Moreover, the decentralized structure allows for scalability across continual behavior-driven and massive IoT installations and trust updates provide real-time recognition. Through this approach, the proposed system provides strong, scalable, and transparent safety that outperforms existing methods.

8. Comparative Synthesis

In this section the responsible AI (RAI) techniques for fraud detection are synthesized. Here we deploy a comparative table of real-world deployments and an integrated system architecture which show RAI methods that are implemented and used in the industry.

8.1. Visualization

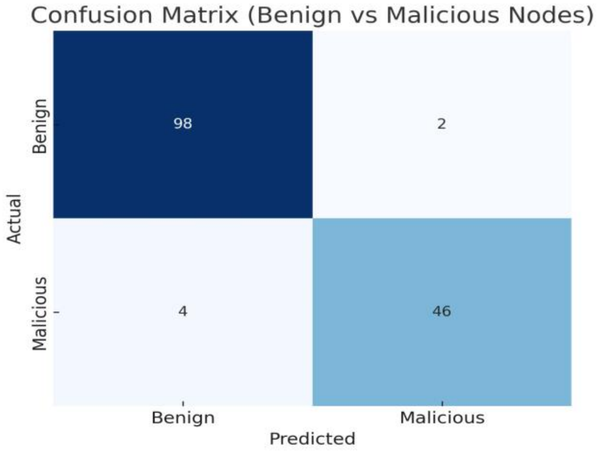

Fig 1: Confusion Matrix of the Model

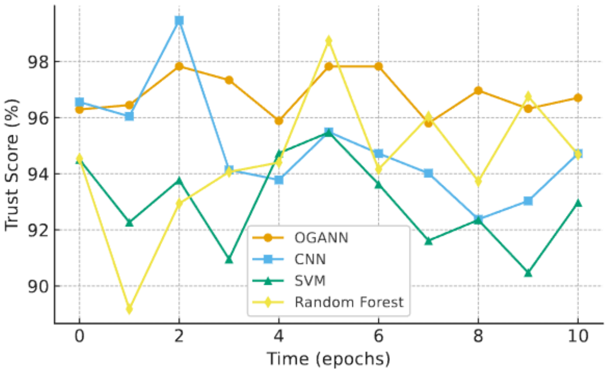

Fig 2: Trust Scores of the Models

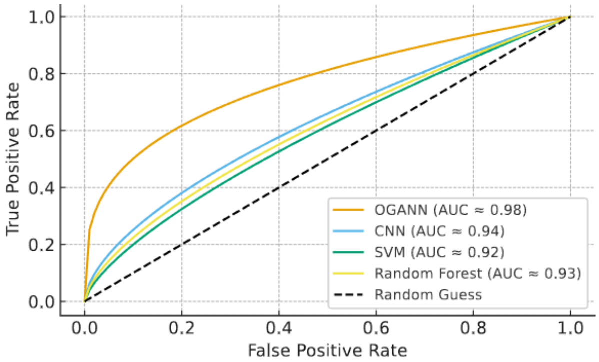

Fig 3: ROC Curve of the Models

8.2. Experimental Setup

- IoT Simulation Environment: We set up a simulated IoT network with 500 nodes in total. Out of these, 450 were normal (benign) and the remaining 50 were configured as malicious nodes.
- Attack Scenarios: The malicious nodes were programmed to carry out harmful actions like flooding the network with data, dropping packets, using fake identities, and tampering with messages.
- Feature Set: From the activity of each node, we extracted features such as transmission rate, energy consumed, message integrity, how often they talk with neighbours, and route consistency.
- Training and Testing Split: About 70% of the dataset was used to train the OGANN model, while the other 30% was kept aside for testing how well it performs.
- Blockchain Implementation: Hyperledger Fabric was used to simulate a permissioned Blockchain setup. On top of it, we developed smart contracts to validate identities and update trust scores in a secure way.
- Optimization Technique: To fine-tune OGANN hyperparameters like learning rate, number of hidden neurons, and activation functions, we used Particle Swarm Optimization (PSO).

8.3. Evaluation Metrics

To measure how well the system performs, the metrics used are accuracy, precision, recall, F1-Score, False positive rate (FPR) and True positive rate (TPR).

9. Results and Analysis

The metrics considered for evaluation are Accuracy, Precision, Recall, F1-score, FPR, Trust Score Dev.

Table 1: Performance Comparison of Models

Metrics	OGANN	CNN	SVM	RF
Accuracy (%)	97.6	94.2	91.8	92.5
Precision (%)	96.8	92.3	90.1	91.2
Recall (%)	97.9	93.7	89.4	90.6
F1 Score (%)	97.3	93.0	89.7	90.9
FPR (%)	1.8	3.9	5.2	4.8
Trust Score Dev. (%)	± 2.1	± 5.7	± 6.3	± 5.9

The results show that our proposed Blockchain-OGANN framework works much better than the usual models in catching malicious activities, while still keeping the trust evaluations stable. By using PSO optimization, the model became more adaptive, and with Blockchain in place, the trust scores are managed in a secure and transparent way. Also, the low false positive rate and very small trust deviation highlight that the framework is reliable and effective, especially for real-time IoT environments.

10. Mathematical Intuition

To understand the mathematical intuition behind the Optimized General Additive Neural Network (OGANN) used in the framework, let's break it down into simple ideas without technical overload.

10.1. Generalized Additive Models (GANs)

The target output is represented using Generalized Additive Models by the summation of multiple smoothing functions. This can be expressed as mathematical formula as:

$$\boldsymbol{Y = f_1(x_1) + f_2(x_2) + \ldots + f_n(x_n) + \epsilon} \tag{5}$$

10.2. Neural Networks

Neural networks are computational models composed of interconnected processing units known as neurons. These networks learn complex, non-linear relationships through forward propagation and weight optimization. In the context of IoT security, the neural architecture learns normal versus anomalous behavioral patterns from features such as data transmission frequency, energy consumption, and packet metadata.

10.3. OGANN: A Hybrid of Interpretability and Learning Power

The OGANN combines both ideas. It keeps a simple understanding of the structure of GAMs using the adaptability of Neural Networks. This methodology leads to better understanding of complex relationships between IoT features.

10.4. Trust Score Computation and Blockchain Integration

Once the Neural network architecture (OGANN) classifies the behavior of an IoT node as trustworthy or suspicious. To ensure that trust is trustworthy and prevent malicious activities, the trust scores are stored in a blockchain ledger.

11. Discussion

The proposed framework is a combination of Blockchain and OGANNs. This system provides a dual-layered security technique. The Blockchain for data integrity and OGANNs for precise threat detection. The decentralized nature of the system guarantees resilience, while the optimized neural networks improve detection of malicious nodes in real-time. Unlike the conventional ML models, OGANNs offer superior interpretability and modularity, which is very essential for dynamic IoT environments.

12. Conclusion and Future Work

This study provides a complete framework of OGANNs and Blockchain technology for improving the security in the IoT networks. The system provides better security and better detection of malicious nodes and by the inclusion of the Blockchain it also maintains a secure and trustworthy environment through dynamic trust and identity management. Future work will have the real-time deployment of the framework with addition of privacy-preserving methods like zero-knowledge proofs and expanding the support to cross-domain IoT networks.

References

[1] M. Conoscenti, A. Vetrò, and J. C. De Martin, ``Blockchain for the Internet of Things: A systematic literature review," IEEE/ACS, 2016. Google Scholar | Publisher Site

[2] Y. Meidan et al., ``N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders," IEEE Pervasive Computing, 2018. Google Scholar | Publisher Site

[3] Q. Lu and X. Xu, ``Adaptable Blockchain-Based Systems for Secure IoT Communications," Future Generation Computer Systems, vol. 92, pp. 799--810, 2019. Google Scholar | Publisher Site

[4] N. Anita and M. Vijayalakshmi, ``Blockchain security attack: a brief survey," in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019. Google Scholar | Publisher Site

[5] P. K. Sharma and J. H. Park, ``Blockchain based hybrid network architecture for the smart city," Futur. Gener. Comput. Syst., vol. 86, pp. 650--655, 2018. Google Scholar | Publisher Site

[6] L. Liu, Z. Ma, and W. Meng, ``Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks," Futur. Gener. Comput. Syst., vol. 101, pp. 865--879, 2019. Google Scholar | Publisher Site

[7] H. N. Dai, Z. Zheng, and Y. Zhang, ``Blockchain for internet of things: a survey," IEEE Internet Things J. 6, 8076--8094, 2019. Google Scholar | Publisher Site

[8] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, ``Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Comput. Secur., vol. 78, pp. 126--142, 2018. Google Scholar | Publisher Site

[9] Altaf, Ayesha, Haider Abbas, Faiza Iqbal, and Abdelouahid Derhab, ``Trust models of internet of smart things: A survey, open issues and future directions," Journal of Network and Computer Applications, Vol. 137, pp. 93--111, 2019. Google Scholar | Publisher Site

[10] Roman, Rodrigo, Jianying Zhou, and Javier Lopez, ``On the features and challenges of security and privacy in distributed internet of things," Computer Networks, Vol. 57, No. 10, pp. 2266--2279, 2013 Google Scholar | Publisher Site

[11] Zhang, PeiYun, MengChu Zhou, and Giancarlo Fortino, ``Security and trust issues in Fog computing: A survey," Future Generation Computer Systems, Vol. 88, pp. 16--27, 2019. Google Scholar | Publisher Site

[12] Colakovi, Alem, and Mesud Hadiali, ``Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Computer Networks, Vol. 144, pp. 17--39, 2018. Google Scholar | Publisher Site

[13] Souissi, Ilhem, Nadia Ben Azzouna, and Lamjed Ben Said, ``A multilevel study of information trust models in WSN-assisted IoT," Computer Networks, Vol. 151, pp. 12--30, 2019. Google Scholar | Publisher Site

[14] Lo, Sin Kuang, Yue Liu, Su Yen Chia, Xiwei Xu, Qinghua Lu, Liming Zhu, and Huansheng Ning, ``Analysis of Blockchain Solutions for IoT: A Systematic Literature Review," IEEE Access, Vol. 07, pp. 58822--58835, 2019. Google Scholar | Publisher Site

[15] Xie, Lixia, Ying Ding, Hongyu Yang, and Xinmu Wang, ``Blockchain-based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs," IEEE Access, Vol. 07, pp. 56656--56666, 2019. Google Scholar | Publisher Site

[16] Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini, ``Security, privacy and trust in Internet of Things: The road ahead," Computer networks, Vol. 76, pp. 146--164, 2015. Google Scholar | Publisher Site

[17] Kang, Kai, Zhibo Pang, Li Da Xu, Liya Ma, and Cong Wang, ``An interactive trust model for application market of the internet of things," IEEE Transactions on Industrial Informatics, Vol. 10, pp. 1516--1526, 2014. Google Scholar | Publisher Site

[18] Jeong, Seohyeon, Woongsoo Na, Joongheon Kim, and Sungrae Cho, ``Internet of things for smart manufacturing system: Trust issues in resource allocation," IEEE Internet of Things Journal, Vol. 05, No. 06, pp. 4418--4427, 2018. Google Scholar | Publisher Site

[19] Christidis, Konstantinos, and Michael Devetsikiotis, ``Blockchains and smart contracts for the internet of things," IEEE Access, Vol. 04, pp. 2292--2303, 2016. Google Scholar | Publisher Site

[20] Yu, Yong, Yannan Li, Junfeng Tian, and Jianwei Liu, ``Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," IEEE Wireless Communications, Vol. 25, No. 6, pp. 12--18, 2018. Google Scholar | Publisher Site

[21] Fernndez-Carams, Tiago M., and Paula Fraga-Lamas, ``A Review on the Use of Blockchain for the Internet of Things," IEEE Access, Vol. 06, pp. 32979--33001, 2018. Google Scholar | Publisher Site

[22] Awan, Kamran Ahmad, Ikram Ud Din, Mahdi Zareei, Muhammad Talha, Mohsen Guizani, and Sultan Ullah Jadoon, ``Holitrust-a holistic cross-domain trust management mechanism for service-centric Internet of Things," IEEE Access, Vol. 07, pp. 52191--5220, 2019. Google Scholar | Publisher Site

[23] Ferrag, Mohamed Amine, Makhlouf Derdour, Mithun Mukherjee, Ab-delouahid Derhab, Leandros Maglaras, and Helge Janicke, ``Blockchain technologies for the internet of things: Research issues and challenges," IEEE Internet of Things Journal, Vol. 6, No. 02, pp. 2188--2204, 2019. Google Scholar | Publisher Site

[24] Makhdoom, Imran, Mehran Abolhasan, Haider Abbas, and Wei Ni, ``Blockchain's adoption in IoT: The challenges, and a way forward," Journal of Network and Computer Applications, Vol. 125, No. 06, pp. 251--279, 2019. Google Scholar | Publisher Site

[25] Bhabendu K. Mohanta, Soumyashree S. Panda, Utkalika Satapathy, Debasish Jena, Debasis Gountia, ``Trustworthy Management in Decentralized IoT Application using Blockchain," 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2019. Google Scholar | Publisher Site

[26] M. K. I. Rahmani, ``Blockchain-based trust management framework for cloud computing-based Internet of medical things (IoMT): A systematic review," Comput. Intell. Neurosci. J., vol. 2022, 2022. Google Scholar | Publisher Site