A Distributed Intrusion Detection System for IoT-Enabled Network and Devices using Hybrid Technique

Davies, I. N, and Taylor, O. E., Anireh V.I.E., Bennett E.O.
Department of Computer Science
Faculty of Science
Rivers State University, Port-Harcourt, Nigeria.
Contact: +2348069059716
Corresponding author email: isobo.davies@ust.edu.ng

DOI: 10.56201/ijcsmt.v10.no2.2024.pg141.156

Abstract
The advent of the Internet-of-Things (IoT) has revolutionized the realm of contemporary computing and networking. IoT-enabled devices which include smart home appliances and industrial sensors, have become extremely common, allowing for effortless connection and data sharing across different fields. However, in recent years, the rapid proliferation of IoT devices has created significant security challenges, necessitating robust and efficient intrusion detection and prevention systems. This study proposes a novel Distributed Intrusion Detection System (DIDS) for IoT-enabled networks and devices using a hybrid technique. The system integrates Case-Based Reasoning (CBR) as the primary detection engine with a Neuro-Fuzzy Inference System (NFIS) for tuning unknown traffic analysis, forming a Hybrid Case-Based Neuro-Fuzzy System (HCBNFS). Additionally, the system incorporates Elliptic Curve Cryptography (ECC) for device authentication and privacy preservation. The DIDS model was designed using the Object-Oriented Design Approach and evaluated using the CIC-IoT2022 dataset and a synthetic smart home dataset. The system achieved high performance metrics, including 99% accuracy and 99.5% precision, recall, and F1-score. This research contributes to enhancing cybersecurity in IoT environments by addressing the unique challenges posed by their distributed and heterogeneous nature, offering improved scalability, fault tolerance, and adaptability compared to traditional centralized intrusion detection systems.

Keywords: *Case-based Reasoning (CBR); Neuro-Fuzzy Inference System (NFIS); Elliptic Curve Cryptography (ECC); Intrusion Detection System (IDS); Distributed Intelligent Systems.*

1. INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) has transformed the landscape of modern computing and networking. IoT-enabled devices, ranging from smart home appliances to industrial sensor have become ubiquitous, enabling seamless connectivity and data exchange across various domains [10]. With IoT, objects are allowed to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency and accuracy [6]. However, due to rapid expansion, and the constraints in hardware capacity within IoT devices, it remains a considerable challenge to effectively introduce and utilize strong, efficient security and privacy measures in the IoT ecosystem [7]. As IoT systems often operate in resource-constrained environments and handle sensitive data, ensuring their security and resilience against cyber threats is of paramount importance [3].

Traditional centralized Intrusion Detection Systems (IDSs) have proven inadequate in addressing the unique challenges posed by the distributed and heterogeneous nature of IoT networks. These systems typically rely on a central monitoring point, which can become a bottleneck or single point of failure, limiting their effectiveness in detecting and responding to threats across a vast network of diverse devices.

To address these limitations, Information System (IS) researchers have proposed the development of Distributed Intrusion Detection Systems (DIDSs) tailored specifically for IoT environments. These systems leverage the collective intelligence and resources of multiple nodes within the network, distributing the tasks of monitoring, analyzing, and responding to potential intrusions. By employing a decentralized approach, DIDSs offer enhanced scalability, fault tolerance, and adaptability, making them better suited to the dynamic and resource-constrained nature of IoT networks.

One promising approach to designing effective DIDSs for IoT networks is the integration of hybrid techniques. Hybrid techniques combine the strengths of various methods, such as signature-based detection, anomaly-based detection, machine learning, and cryptographic encryption algorithms. By leveraging these complementary approaches, hybrid techniques can achieve more robust and comprehensive intrusion detection capabilities, addressing a wider range of known and unknown threats.

Technically, one relative technique that is attracting increasing attention is the Case-Based Reasoning (CBR). It is a subfield of Artificial Intelligence (A.I) which solves similar problems by simply remembering its previous solution [16]. According to researchers in their paper, they stated that adjusting the similarity measures, is one of the knowledge containers for its knowledge representation, along the case base, adaptation knowledge vocabulary [14]. Further, another buzzing technique is the Neuro-Fuzzy Inference System (NFIS). This approach is an amalgamation of Neural Network (NN) and Fuzzy Logic Systems (FLS). Prof. Zadeh provided a definition of fuzzy logic as a branch of logic that is centered on formal rules of approximate reasoning, considering precise reasoning as a constraining scenario [17].

Nevertheless, for this study, the aim is to develop a novel DIDS that employs hybrid intelligence techniques and a cryptographic algorithm to combat cyber-attack specifically tailored for IoT-enabled networks and devices. The objectives are as follows:

i. Design a DIDS model for detecting network anomalies using CBR as a primary detection engine,
ii. Tune the revise phase of the CBR to further investigate unknown network traffic packets using Takagi-Sugeno of NFIS,
iii. Integrate a roust lightweight encryption mechanism for node authentication and privacy preservation using Elliptic Curve Cryptographic (ECC), and
iv. Evaluate the performance of the developed application using standard metrics.

Our proposed model harnesses the power of distributed computing and leverage the collective intelligence of IoT nodes to detect and mitigate security threats in real-time. By combining different detection techniques, the system aims to achieve enhanced accuracy, adaptability, and resilience against evolving cyber threats.

The introduction of such a DIDS for IoT network holds significant implications for improving cybersecurity and safeguarding critical infrastructure, industrial processes, and personal data. By addressing the unique challenges posed by the IoT ecosystem, this study contributes to ensuring the secure and reliable operation of interconnected devices, fostering trust and enabling the full potential of IoT technologies.

2. RELATED WORKS

The number of actors, expenditures, and incidents associated with internet criminality has been on the rise over the past few years because of the increasing connectivity of numerous devices in our daily lives to the internet. The concept of "security by design" is becoming more recognized in the field of software engineering. However, it should not be assumed that it can address all security concerns, as the variety of potential security flaws and the ingenuity of attackers appear to be limitless. As a result, researchers suggest the implementation of a multi-agent case-based reasoning system to identify malicious traffic within an internet connection [14]. The objective of their study is to identify and notify the security engineer of a company about any malicious network traffic, enabling them to take appropriate measures, such as blocking the source IP address of the possible attacker. Their system achieved a successful detection rate of 70% for attacks, with an average true-positive rate of 82.56%. The system identified and flagged the remaining attacks for additional analysis and potential enhancements.

Researchers contend that the digital footprints left by a human assailant during an unauthorized access attempt can be utilized to construct a comprehensive profile of the individual in question. To demonstrate this idea, they developed a methodology employing case-based reasoning that indirectly assesses an assailant's attributes for specific attack scenarios. The findings of their study demonstrate that case-based reasoning has the capability to aid security and forensic investigators in the process of profiling human attackers [11].

In recent years, there has been a growing interest among academics in improving the structure and safety of IoT systems by utilizing Machine Learning (ML) techniques to serve as Intrusion Detection Systems (IDSs) and enhance security features. Researchers had suggested an innovative DIDS which relies on machine learning (ML) techniques to identify assaults in IoT and reduce the impact of harmful incidents [5].

Distributed Denial of Service (DDoS) attacks have been used to limit end-user services recently. Thus, an effective detection method for this type of assault is urgently needed. Due to this, researchers proposed a Fuzzy Logic Anomaly-based Intrusion Detection System. Their fuzzy logic inference system could detect DDoS attacks. Their approach was tested using an open-source dataset of DDoS attacks. Their experimental findings indicate that the Anomaly-based Intrusion Detection system, which incorporates Fuzzy Logic and employs the InfoGain features selection method, achieves a true-positive rate of 91.1% and a false-positive rate of 0.006% [1].

[8] proposed a Fuzzy-based Intrusion Detection System (IDS), which uses fuzzy logic to represent and identify malicious behavior. In addition, the Base Station applies a filtering process to select the option based on the calculation of fuzzy values. The parameter values that influence their proposed technique was determined by conducting thorough simulations. Both analytical and simulation results provide evidence that the suggested strategy surpasses existing methods.

A novel Intrusion Detection and Prevention System (IDPS) was developed using an Adaptive Hybrid Case-Based Neuro-Fuzzy System (HCBNFS). The CBR is used as a major detection engine in HCBNFS to identify network traffic patterns. NFIS is also used to tune unknown traffic analysis and improve CBR reverse phase inquiry. They trained and tested their model using CIC-IoT2022. Their intrusion detection model was 99% accurate. Additionally, its precision, recall, and F1-Score were 99.5% [4].

Machine Learning (ML) offers efficient IDS solutions for diverse situations. Researchers utilizing ML techniques proposed an efficient and time-saving IDS architecture for IoT environments. They analyzed data from network traffic and real-time sensors in an IoT-enabled smart environment to classify and forecast potential network anomalies or threats. They evaluated their model using various machine classifiers on an open source ‘DS2OS’ dataset, which includes both ‘normal’ and ‘anomalous’ network traffic. Their proposed IDS were validated using machine learning metrics such as train and test accuracy, time efficiency, error-rate, TPR, and FNR [13].

Attacks on Fog server can manifest in several ways, including DDoS attacks that significantly impact the dependability and accessibility of fog services. To tackle this problem, researcher authors proposed countering SYN Flood DDoS attacks in fog computing by employing an Adaptive Neuro-Fuzzy Inference System (ANFIS) which receives aid from software defined networking (SDN) through FASA. Their experiment findings demonstrate that their proposed technique or system surpasses other algorithms in terms of accuracy, precision, recall, and F1-score [2].

The endeavour to guarantee the security of Homes has attracted considerable attention from both the business and academics, leading to the development of several techniques for handling keys and authentication. However, most methods demonstrate inefficiency due to either an excessive amount of communication or a high level of computing complexity. To address these problems, author proposed a streamlined approach to key management and mutual authentication in smart home contexts, employing ECC (Elliptic Curve Cryptography). The evaluation of the recommended protocol's performance was carried out by considering aspects such as communication cost, calculation overheads, throughput, and end-to-end delays (EED). The security of the proposed protocol was evaluated using the Dolev-Yao and Canetti-Krawezyk models. The experimental results demonstrated that the proposed protocol had the lowest communication and computation costs compared to other systems and had the least impact on both throughput and end-to-end delay (EED) [12].

There has been a recent rise in the rate of digitization and information transmission in the industrial technology industry. This typically makes the following stages of dispersed networks more responsive and efficient. Researchers had emphasized the importance of finding a security solution that is both efficient and lightweight such as the ECC. To improve the security of transmitted data, they proposed to create an authentication system that is both lightweight and extensible. Their new protocol utilized the XOR, concatenation, and hash functions. The AVISPA was used for evaluation, and the experimental findings demonstrated that the method achieved a computational cost of 7.96 bits and a communication cost of 834 bits [15].

3. METHODOLOGY

We base our study on the Design Science Research Method (DSRM) [9], which aims to increase human's knowledge of how to create new artefacts with the goal of resolving practical issues. However, in terms of building the DIDS's framework, the Object-Oriented Design Approach (OODA) is utilized.

Dataset Description

Our model utilizes a sample Canadian Institute for Cybersecurity (CIC-IoT2022) data and a synthetic smart home dataset generated from synthetic dev. For this study, the relevant network traffic features selected form these datasets is the source IP, destination IP, protocol, source port, and destination port.

System Design

Our proposed DIDS model was developed using a task-based approach, where different system components were divided into self-contained and reusable objects. Each object contains the necessary data and behavior specific to itself. The proposed system's architectural design is depicted in Figure 1.

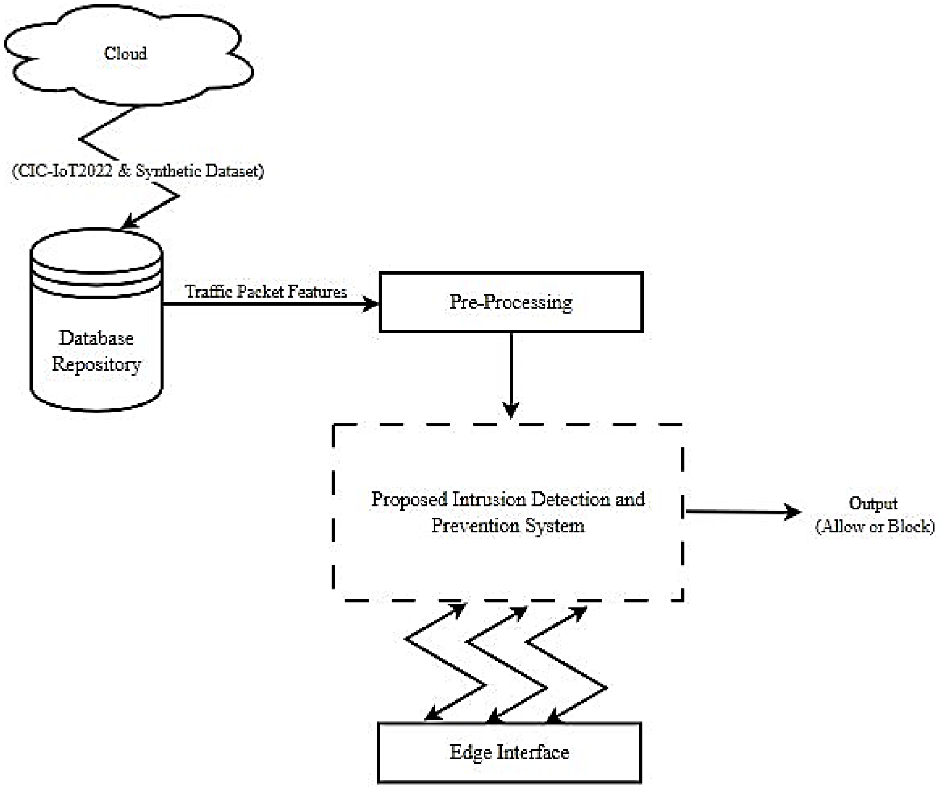

Figure 1: Architecture of the system

An overview of the proposed system's architectural architecture is shown in Figure 1. It captured the process by which the traffic features pre-proposed from the chosen dataset to a format suitable for model training and testing. The system will return a defuzzified value between 0 and 1, which indicates whether to permit or prohibit the device or packet of network traffic. Our proposed Intrusion Detection and Prevention System module for this study includes multiple additional modules, which should be mentioned. For that reason, this study will continue to break down these modules or components and their functions into smaller parts to make them easier to read and understand.

Intrusion Detection and Prevention System (IDPS) Module

Embedded in the proposed IDPS module includes the device management and the Hybrid Case-Based Neuro-Fuzzy System (HCBNFS) modules. The device manager module is implemented to effectively manage trusted network devices and their cryptographic keys, while the HCBNFS is implemented as an innovative hybrid machine learning technique for identifying and blocking anomalies or malicious traffic on the network. We utilized the anomaly-based approach to construct the proposed Intrusion Detection and Prevention System (IDSP). This approach is employed because of its efficacy in identifying unfamiliar intrusions on the network. Figure 2 depicts the schematic overview of our proposed approach.

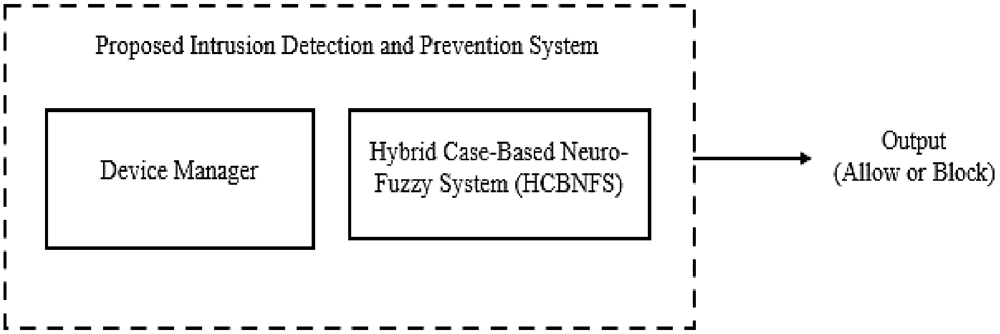
Proposed Intrusion Detection and Prevention System
Device Manager
Hybrid Case-Based Neuro-Fuzzy System (HCBNFS)
Output
(Allow or Block)

Figure 2: Proposed Imtrusion Detection System

Device Manager Module

Effective management of trusted network devices is crucial for guaranteeing the security and dependability of modern networks. This study utilizes SQL server as a comprehensive framework for managing network device credentials. Upon joining the network, the new IoT device transmits its information, including device ID, Model, and initial authentication credentials, to the device manager module. The device manager module currently stores this information in the SQL Server database. The data encompasses device metadata, ownership particulars, and any additional pertinent properties. During the authentication process, devices attempting to join to the network transmit their authentication credentials (such as username/password or certificate) to the SQL server for verification. The server authenticates these credentials by comparing them to the data stored in the database. If the provided credentials are verified, the device is authenticated and granted permission to access the network; otherwise, access is refused. Furthermore, for the cryptographic key generation, this study utilized the secp256r1 ECC parameter, which belongs to the Suite B collection of cryptographic curves widely employed in cryptography, especially in protocols adhering to the National Institute of Standards and Technology (NIST) standards.

Hybrid Case-Based Neuro-Fuzzy System (HCBNFS) Module

To counteract the ever-changing cyber-threat landscape, the novel HCBNFS method integrates the adaptabilities of the NFIS with the CBR capabilities of applying past solutions to new, comparable problems. Part of the proposed HCBNFS model for this research includes an IDS that uses CBR as its primary detection engine and a tuning factor that acts as an Intrusion Prevention System (IPS) that makes use of NFIS. Figure 3 depicts the study's proposed Hybrid Case-Based Neuro-Fuzzy System (HCBNFS) module in a schematic and full overview.

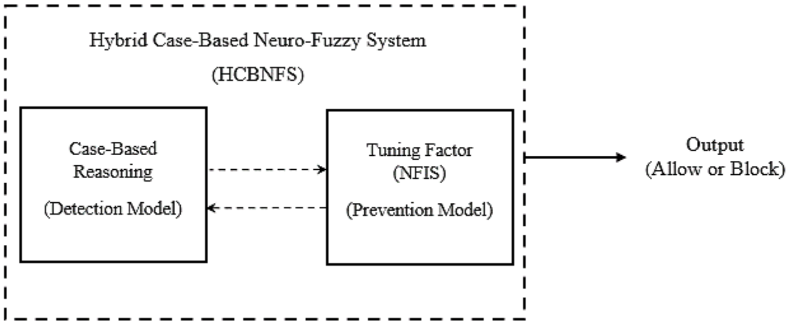

Figure 3: Hybrid Case-Based Neuro-Fuzzy System (HCBNFS) Module

The IP address studied in this study is in the Class-C IPv4 format, which consists of four decimal integers separated by periods (e.g., 192.168.1.0). Understanding the structure of IPv4 addresses is crucial for precise fuzzification in this study. The Class-C IPv4 is composed of four octets, with each octet having a range from 0 to 255. It is important to understand that the fuzzification process entails the allocation of each octet of the IP address to one of the linguistic variables (Low, Medium, or High), based on its numerical value. Consequently, the process of fuzzification in the IP address field entails transforming the precise IP addresses into predetermined fuzzy groupings. This is accomplished by partitioning the whole IP address range into distinct linguistic variables, which are determined by the four separate octets of IP addressing. In this study, the term "Low" refers to IP addresses that fall below a specified value (0-63), "Medium" refers to IP addresses within a moderate range (64-191), and "High" refers to IP addresses that exceed another specified value (192-255). This split allows the system to effectively manage imprecision and unpredictability. This enhances the ability of the IPS module to analyze the incoming IP addresses in a more adaptable manner.

This study utilizes a mixture of linguistic variables (High, Medium, or Low) derived from the values in each of the four octets to represent the IP address variable. The linguistic variables of each individual octet are combined using a predetermined mapping or set of rules to determine the linguistic value for the complete IP address.

The linguistic variable representing the IP address can be associated with a particular combined value (e.g., "High-Medium-Low-High") by applying predetermined rules. For example, if the first octet has a "High" value, the second octet has a "Medium" value, the third octet has a "Low" value, and the fourth octet has a "High" value. Subsequently, by using the given criteria, the linguistic variable of the IP address might be associated with a specific composite value (e.g., "High-Medium-Low-High") according to the predetermined rules of the system.

Table 1 presents the input variables to the NFIS along with their corresponding membership functions (MF).

Table 1. Input Variables and their corresponding MF.

Input Variable	**Membership Function (MF)**	**Range**
Source IP	Low, Medium, and High	Low = 0-63, Medium = 64-191, and High = 192-255.
Destination IP	Low, Medium, and High	Low = 0-63, Medium = 64-191, and High = 192-255.
Source Port	Low, Medium, High	Low = 0-16383, Medium = 16383-32767, and High = 32767-65535.
Destination Port	Low, Medium, High	Low = 0-16383, Medium = 16383-32767, and High = 32767-65535.
Protocol	Low, and High	Low = Unknown, and High = Known

We employed the weighted average defuzzification method to transform the fuzzy output into a crisp value representing either to block or allow the traffic based on their mapping output membership. These values are classified as “Final Decision” using the following equation:

$$FinalDecison_{Output} = \begin{cases} Normal & 0 \leq y \leq 0.3 \\ MiTM & 0.3 \leq y \leq 0.5 \\ Scanning & 0.5 \leq y \leq 0.7 \\ DoS & 0.7 \leq y \leq 0.9 \\ MiraiBotnet & 0.9 \leq y \leq 1 \end{cases} \qquad (1)$$

In equation (1), we defined the boundaries so that each range is exclusive of the upper bound and inclusive of the lower bound. Meaning that if the value of y falls exactly on a boundary, it will be assigned to the corresponding category.

Figure 4 is used to capture the interaction between the various components in our proposed model.

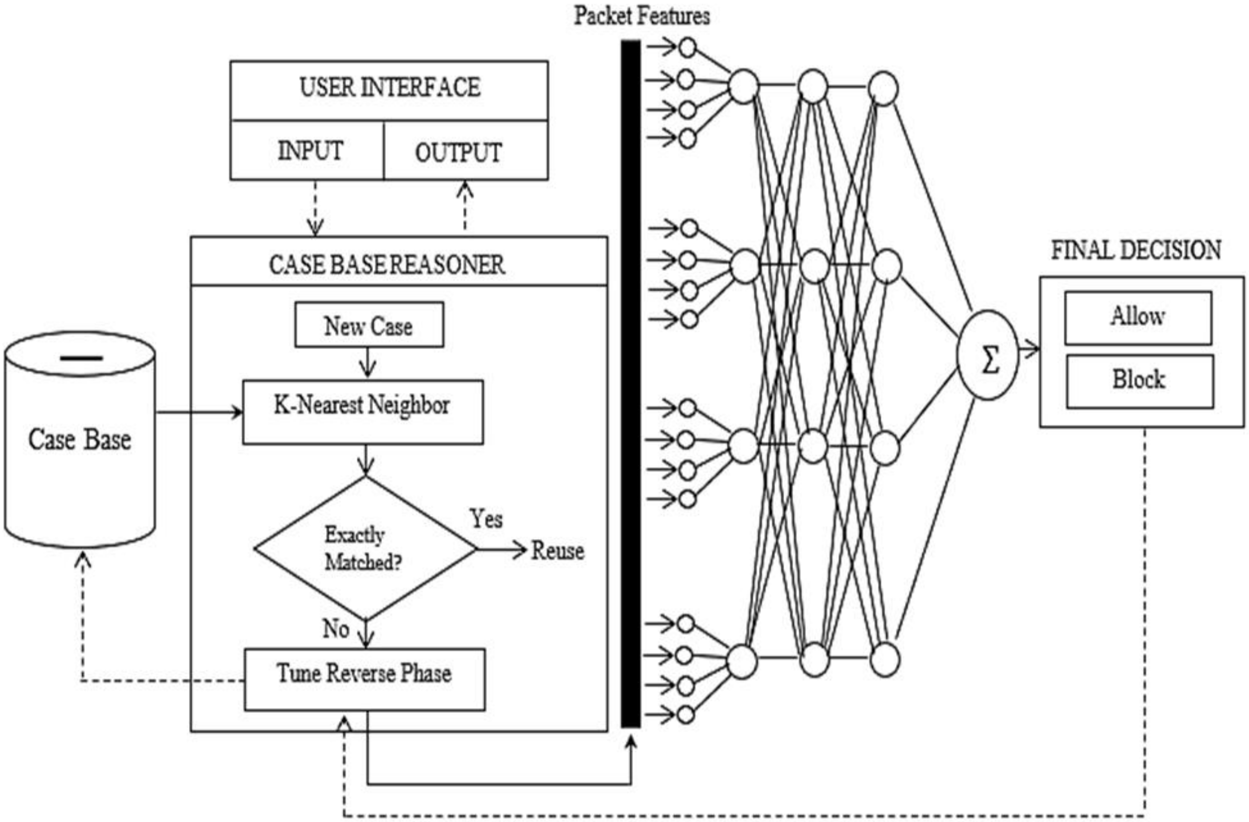

Figure 4: Interactions between the embedded components in the proposed system.

Figure 4 above captures the how the traffic features are entered from the system's user interface to the CBR. These traffic features are used to form a new to the CBR, which then searches its case based for similar matching case using the K-nearest neighbor search technique. If an exact match is found in case base, its solution will be reused. Else, the system will apply the NFIS as a tuning factor to the CBR's reverse phase. The final decision (allow or block) of the tuning factor will now be adopted as the solution to the new case and be retained in the proposed system's case base.

4. RESULTS

Presentation of ECC Results

Encryption Speed: For a 1KB data size, Device ID SHD001 completed ECC encryption and decryption operation in 0.6ms and 0.8ms respectively. Device ID SHD002 and SHD003 completed their operations in 0.7ms and 0.5ms, 0.9ms and 0.7ms respectively. However, similar trends were observed for larger data size. The time taken for each edge device to perform its encryption and decryption operations using the Curve P-256 is captured and presented in Table 2. While Figure. 5 is a line graph representation of the various ECC encryption and decryption time.

Table 2. Encryption and Decryption time for each edge device using Curve P-256

Device ID	Encryption Time	Decryption Time	ECC Parameter
SHD001	0.6ms	0.8ms	Curve P-256
SHD002	0.7ms	0.5ms	Curve P-256
SHD003	0.9ms	0.7ms	Curve P-256

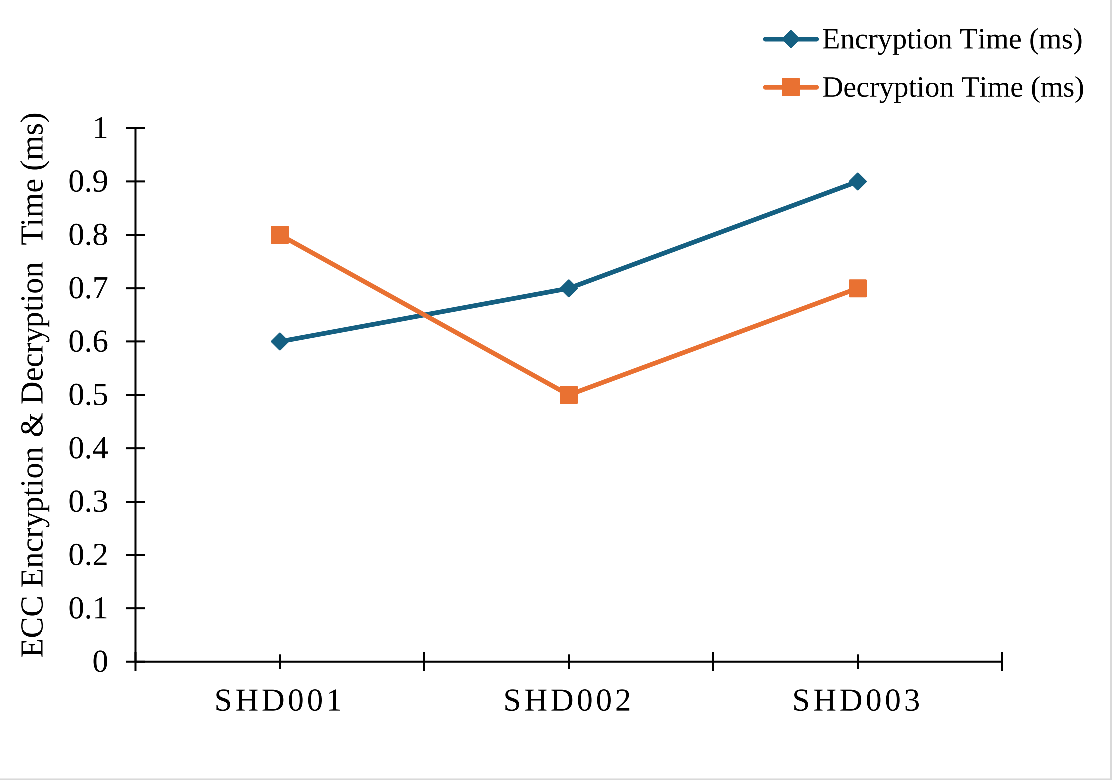

Figure. 5 Line graph showing the various ECC Encryption and Decryption Time.

Presentation of Results using the HCBNFS

The results of our proposed HCBNFS are tabulated in Table 3. The table captured the interpretations of the produced results together with their recommended action. Here, SrcIP is the source IP, DesIP is the destination IP, SrcPort is the source Port, and DesPort is the destination Port number.

Table 3. Interpretation of Results

SrcIP	DesIP	Protocol	SrcPort	DesPort	Output	Interpretation	Recommended
192.168.0.16	192.168.0.13	TCP	49784	9020	0.2	Normal	Allow
104.118.134.215	192.168.0.24	TCP	433	56373	0.9	MiraiBotnet	Block
192.168.0.13	222.169.172.174	TCP	554	2760	0.7	DoS	Block
172.217.25.99	192.168.0.14	UDP	433	54028	0.2	Normal	Allow
193.168.0.13	163.152.127.148	UDP	56361	10101	0.9	MiraiBotnet	Block
192.168.0.24	163.152.1.1	DNS	59784	53	0.9	MiraiBotnet	Block
192.168.0.23	224.0.0.251	DNS	5353	5353	0.6	Scanning	Block
192.168.0.16	192.168.0.13	ICMP	53182	9020	0.4	MiTM	Block
46.51.222.63	192.168.0.16	TCP	443	61865	0.4	MiTM	Block
192.168.0.24	139.150.252.50	HTTP	51586	80	0.9	MiraiBotnet	Block
163.152.1.1	192.168.0.24	UDP	53	59310	0.9	MiraiBotnet	Block
111.238.226.143	192.168.0.13	TCP	6588	554	0.7	DoS	Block
97.186.0.16	192.168.0.13	UDP	49784	9020	0.2	Normal	Allow
192.168.0.16	18.136.162.179	TCP	57217	433	0.2	Normal	Allow
108.177.97.189	192.168.0.14	UDP	443	50510	0.2	Normal	Allow
163.152.1.1	192.168.0.16	DNS	53	50788	0.9	MiraiBotnet	Block
192.168.0.16	31.13.76.16	TCP	56358	443	0.9	MiraiBotnet	Block
3.0.72.236	192.168.0.16	TCP	443	61854	0.9	MiraiBotnet	Block
210.124.177.97	192.168.0.23	TCP	9600	36762	0.6	Scanning	Block
192.168.0.15	192.168.0.13	TCP	33306	8194	0.6	Scanning	Block
192.168.0.13	192.168.0.15	TCP	44443	33306	0.6	Scanning	Block
192.168.0.15	192.168.0.24	TCP	35878	700	0.6	Scanning	Block

From Table 3. the membership value ranges are interpreted as the degree to which the system classifies the network traffic or activity by analyzing them and assigning membership values or scores to the different types of traffic or attacks either to allow or block the traffic.

Performance of Evaluation

We employed various performance metrics to determine the efficiency of our model. These metrices includes the accuracy, precision, recall, and F1-score. The formula for calculating these metrics is given in the following equations:

$$IDPS_{Accuracy} = \frac{(TP+TN)}{(TP+TN+FP+FN)} \tag{2}$$

Where, $IDPS_{Accuracy}$ is the accuracy rate, *TP* is the true positive value, *TN* is the true negative value, *FP* is the false positive value, and *FN* is the false negative value.

With regards to the IDPS for this study, the system's precision is determined by how many of the predicted intrusions cases were correctly predicted. It measures the number of true positive instances divided by the sum of true positive and false positives. This however represents the accuracy of the positive predictions made by our IDPS. The formula for precision is given as.

$$IDPS_{Precision} = \frac{TP}{(TP+FP)} \tag{3}$$

Where $IDPS_{Precision}$ is the precision of the IDPS, *TP* and *FP* are the true and false positives values respectively.

For this study, recall is regarded as the baseline for truth. That is, given all intrusion truth samples, how many of these intrusions were correctly captured. It measures the number of true positive instances divided by the sum of true positive and false negatives. This will be used to represent the ability of the IDPS to correctly identify all relevant instances. The formula for Recall is given as follows.

$$IDPS_{Recall} = \frac{TP}{(TP+FN)} \tag{4}$$

Where $IDPS_{Recall}$ is the recall value of the developed IDPS, *TP* and *FN* are the true positive and false negative values respectively. The "harmonic mean" of the developed IDPS precision and recall values is the F1-score value. It is a metric commonly used in classification tasks. It measures the developed IDPS accuracy, considering both precision and recall. It is commonly considered as a balance between precision and recall based on the system's goals and priorities. For this study, F1-score is computed using the following:

$$IDPS_{F1Score} = 2 \times \frac{IDPS_{Precision} \times IDPS_{Recall}}{IDPS_{Precision} + IDPS_{Recall}} \tag{5}$$

The computed values of the accuracy, precision, recall, and F-score for the developed IDPS for this study is captured in Table 4.

Table 4: Computed values of the various performance metric.

Performance Metric	Value
$IDPS_{Accuracy}$	0.99
$IDPS_{Precision}$	0.995
$IDPS_{Recall}$	0.995
$IDPS_{F1score}$	0.995

Performance Evaluation of the System

The performance of our IDPS was evaluated using accuracy, precision, recall, and F1-score. The computed values of these metrics were captured in Table 4. Our IDPS achieved an accuracy rate of 99%, precision, recall, and F1-score of 99.5% respectively. Hence, it actively demonstrated that it could serve as an efficient security system for IoT smart home network in terms of classification of network traffic, and the detection and prevention of anomalies on the smart home network. The line graph in Figure 6 is used to capture the level of performance of the various metrics.

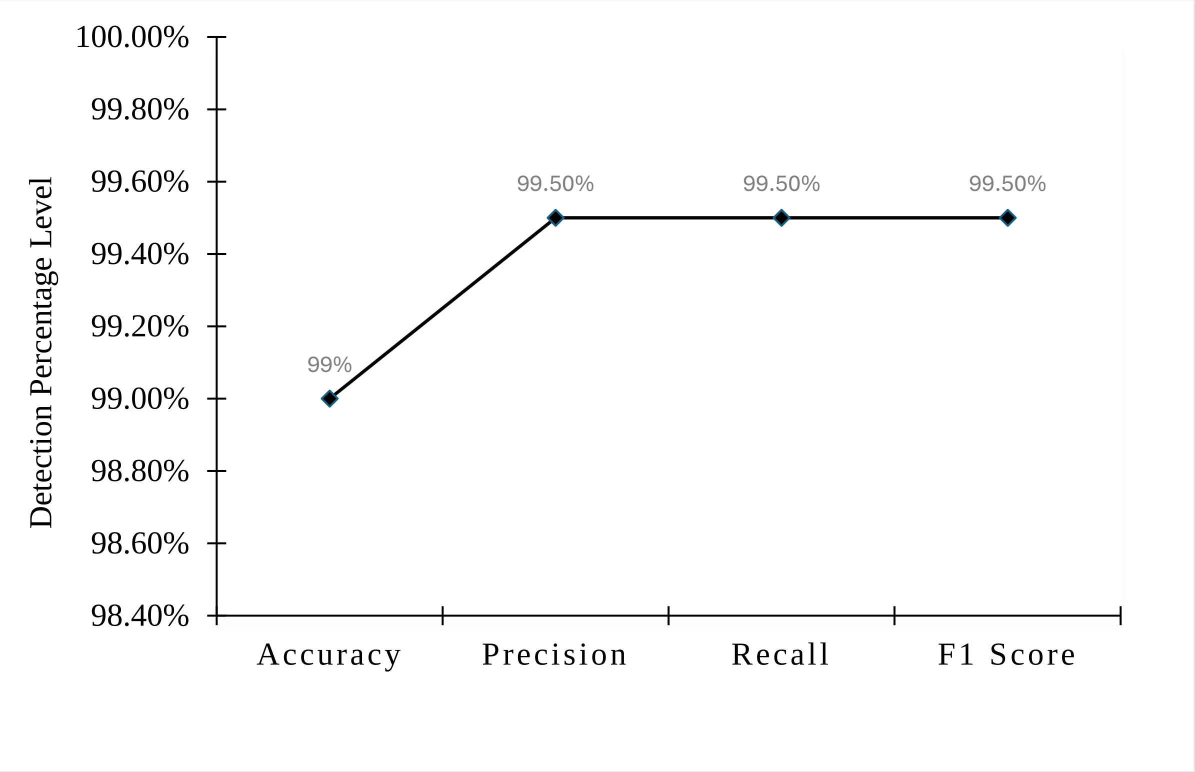

Figure 5. Line graph representation of the proposed system performance in detection

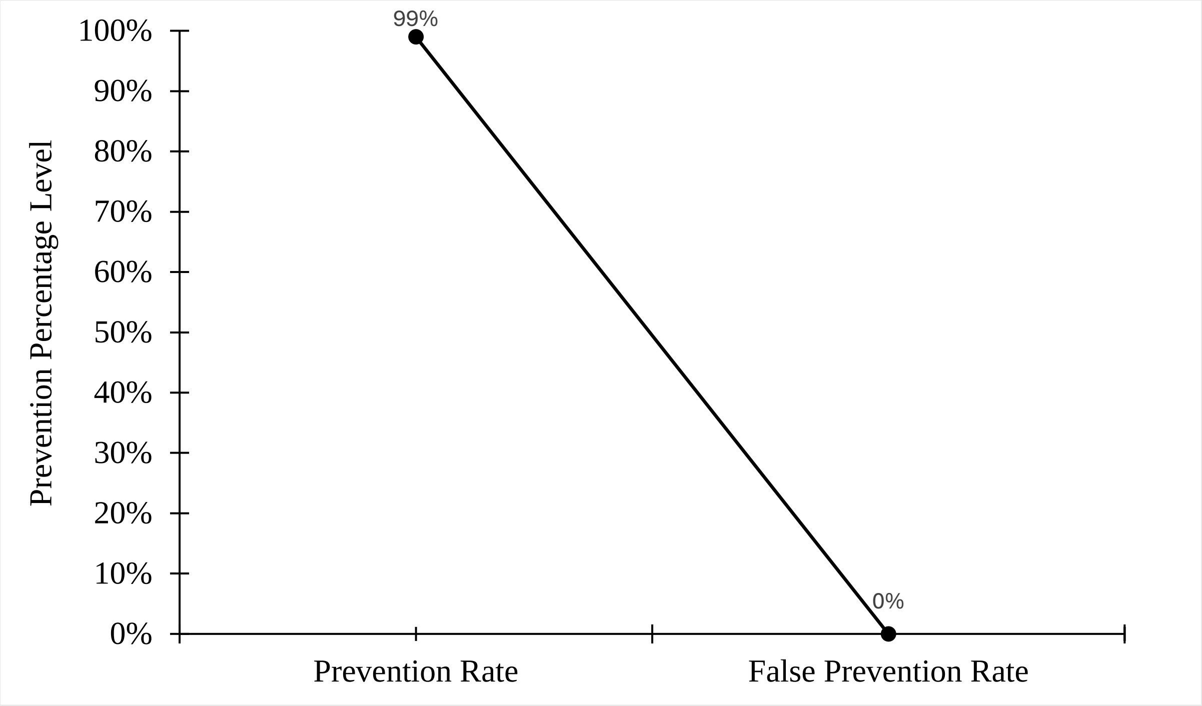

Figure 6: Line graph representation of the proposed system performance in prevention

5. CONCLUSION

The rapid proliferation of IoT devices has created significant security challenges, necessitating robust and efficient intrusion detection and prevention systems. This study successfully developed and implemented a novel Distributed Intrusion Detection System (DIDS) for IoT-enabled networks and devices using a hybrid technique.

The proposed system's architecture, combining Case-Based Reasoning (CBR) with a Neuro-Fuzzy Inference System (NFIS), demonstrated remarkable efficacy in detecting and preventing network anomalies. The integration of Elliptic Curve Cryptography (ECC) further enhanced the system's security by providing efficient device authentication and privacy preservation.

The performance evaluation of the system yielded impressive results, with an accuracy rate of 99% and precision, recall, and F1-score all at 99.5%. These metrics underscore the system's high reliability in classifying network traffic and detecting anomalies in smart home networks. The system's ability to handle both known and unknown threats, thanks to the CBR's pattern recognition capabilities and the NFIS's adaptive learning, positions it as a robust solution for IoT security.

Moreover, the distributed nature of the system addresses the limitations of traditional centralized intrusion detection systems, offering enhanced scalability and fault tolerance. This is particularly crucial in the context of IoT networks, which are characterized by their heterogeneity and dynamic nature.

The study also demonstrated the effectiveness of ECC in providing lightweight yet strong encryption for IoT devices, with rapid encryption and decryption times even for resource-constrained devices. This aspect is vital for ensuring secure communication within IoT networks without significantly impacting performance.

While the results are promising, future work could focus on further optimizing the system for even more resource-constrained IoT devices and expanding the range of detectable attacks. Additionally, real-world deployment and testing in various IoT environments could provide valuable insights into the system's performance under diverse conditions.

Nevertheless, this study makes a significant contribution to the field of IoT security by providing a comprehensive, efficient, and adaptable solution for intrusion detection and prevention. The proposed DIDS model represents a step forward in securing IoT ecosystems, addressing the unique challenges posed by these networks, and paving the way for more secure and reliable IoT deployments across various domains.

REFERENCES

[1]. Almseidin, M., Al-Sawwa, J., & Alkasassbeh, M. (2021). *Anomaly-based Intrusion Detection System using Fuzzy Logic.* Paper presented at the 2021 International Conference on Information Technology (ICIT).

[2]. Bensaid, R., Labraoui, N., Abba Ari, A. A., Maglaras, L., Saidi, H., Abdu Lwahhab, A. M*., et al.* (2024). Toward a Real-Time TCP SYN Flood DDoS Mitigation Using Adaptive Neuro-Fuzzy Classifier and SDN Assistance in Fog Computing. *Security and Communication Networks, 2024*(1), 6651584.

[3]. Cook, J., Rehman, S. U., & Khan, M. A. (2023). Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions. *IEEE Access, 11*, 39295-39317.

[4]. Davies, I., Taylor, O., Anireh, V., & Bennett, E. (2024). Adaptive Hybrid Case-Based Neuro-Fuzzy Model for Intrusion Detection and Prevention for Smart Home Network. *12*(5), 01-10.

[5]. Gad, A. R., Haggag, M., Nashat, A. A., & Barakat, T. M. (2022). A Distributed Intrusion Detection System using Machine Learning for IoT based on ToN-IoT Dataset. *International Journal of Advance Computer Science and Applications, 13*(6), 548-563.

[6]. Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IoT. *International Advanced Research Journal in Science, Engineering and Technology, 5*(1), 41-44.

[7]. Hammi, B., Fayad, A., Khatoun, R., Zeadally, S., & Begriche, Y. (2020). A Lightweight ECC-based Authentication Scheme for Internet of Things (IoT). *IEEE Systems Journal, 14*(3), 3440-3450.

[8]. Hendaoui, F., Eltaief, H., & Youssef, H. (2017). *FID: Fuzzy based Intrusion Detection for Distributed Smart Devices.* Paper presented at the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA).

[9]. Johannesson, P., & Perjons, E. (2021). *An Introduction to Design Science* (2nd ed.). Switzerland: Springer.

[10]. Jurcut, A. D., Ranaweera, P., & Xu, L. (2020). Introduction to IoT Security. *IoT security: advances in authentication*, 27-64.

[11]. Kapetanakis, S., Filippoupolitis, A., Loukas, G., & Al Murayziq, T. S. (2014). Profiling Cyber Attackers using Case-based Reasoning.

[12]. Nyangaresi, V. O. (2021). *ECC based Authentication Scheme for Smart Homes.* Paper presented at the 63rd International Symposium ELMAR, Zadar, Croatia.

[13]. Rani, D., Gill, N. S., Gulia, P., Arena, F., & Pau, G. (2023). Design of an Intrusion Detection Model for IoT-enabled Smart Home. *IEEE Access, 11*, 52509-52526.

[14]. Schoenborn, J. M., & Althoff, K.-D. (2023). *A Multi-agent Case-Based Reasoning Intrusion Detection System Prototype.* Paper presented at the International Conference on Case-Based Reasoning, Aberdeen, UK.

[15]. Velliangiri, S., Manoharn, R., Ramachandran, S., Venkatesan, K., Rajasekar, V., Karthikeyan, P*., et al.* (2021). An Efficient Lightweight Privacy-Preserving Mechanism for Industry 4.0 Based on Elliptic Curve Cryptography. *IEEE Transactions on Industrial Informatics, 18*(9), 6494-6502.

[16]. Wenming, S. (2021). *Navigation Safety Early Warning Method Based on CBR and Millimeter Wave Radar.* Paper presented at the 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC).

[17]. Zadeh, L. A. (1988). Fuzzy logic. *Computer, 21*(4), 83-93.