Strengthening IoT Intrusion Detection through the HOPNET Model

Chandrababu Majjaru[1] and K. Senthilkumar[2*]

[1]Research Scholar, School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore, India. majjaru.chandrababu2017@vitstudent.ac.in, Orcid: https://orcid.org/0000-0001-8117-3664

[2*]Professor, School of Computer Science Engineering, Vellore Institute of Technology, Vellore, India. ksenthilkumar@vit.ac.in, Orcid: https://orcid.org/0000-0001-6997-8398

Received: May 23, 2023; Accepted: July 04, 2023; Published: September 30, 2023

Abstract

The rapid growth of Internet of Things (IoT) applications has raised concerns about the security of IoT communication systems, particularly due to a surge in malicious attacks leading to network disruptions and system failures. This study introduces a novel solution, the Hyper-Parameter Optimized Progressive Neural Network (HOPNET) model, designed to effectively detect intrusions in IoT communication networks. Validation using the Nsl-Kdd dataset involves meticulous data preprocessing for error rectification and feature extraction across diverse attack categories. Implemented on the Java platform, the HOPNET model undergoes comprehensive evaluation through comparative analysis with established intrusion detection methods. Results demonstrate the superiority of the HOPNET model, with improved attack prediction scores and significantly reduced processing times, highlighting the importance of advanced intrusion detection methods for enhancing IoT communication security. The HOPNET model contributes by establishing robust defense against evolving cyber threats, ensuring a safer IoT ecosystem, and paving the way for proactive security measures as the IoT landscape continues to evolve.

Keywords: Intrusion Detection, Neural Networks, Intrusion Type Classification, Cloud Security, Internet of Things, Feature Extraction.

1 Introduction

In recent times, the widespread utilization of the internet, especially in the business industry, has led to significant growth (Khan, M. A., 2020). However, with the growth of IoT applications, ensuring the security and protection of sensed data has become a critical concern (Mebawondu, J.O., 2020). Sensor technology's application across various fields has unleashed the potential of IoT facilities, but it has also led to a rapid increase in intrusion incidents, making cybersecurity a vulnerable aspect (Zhou, Y., 2020). User-oriented applications, including web browsers, operating systems, web servers, and databases, are particularly susceptible to a range of attack types (Subba, B., 2021). These intrusions, namely Denial of Service, probe, snort, r2l attacks, aim to exploit data for unauthorized access (Waskle, S., 2020). As a

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 14, number: 3 (September), pp. 89-102. DOI: *10.58346/JOWUA.2023.I3.007*

*Corresponding author: Professor, School of Computer Science Engineering, Vellore Institute of Technology, Vellore, India.

result, such attacks can cause network disruptions, shutdowns, and non-linear behavior, straining IoT networks' computation and resource costs.

Addressing these cybersecurity challenges, Intrusion Detection Systems (IDS) play a crucial role in overseeing network operations and promptly notifying users upon the detection of malicious conduct (Benisha, R.B., 2020). While anomaly-centric IDS focuses on detecting abnormal behaviors, signature-centric IDS relies on predefined patterns to identify potential intrusions (Kasongo, S.M., 2020). However, existing anomaly-based detection often suffers from higher false-positive and false-negative rates (Dua, M., 2020). To achieve better detection rates and lower false positive rates, hybrid IDS systems combine both approaches (Sethi, K., 2020). Nevertheless, existing research primarily focuses on enhancing detection accuracy and computation time (Sumaiya Thaseen, I., 2021).

The objective of this research is to address the limitations faced by current IDS in IoT networks. The effectiveness of intrusion detection can be compromised due to the severity of attacks and the distinctive movement patterns of IoT devices. Therefore, this paper introduces an enhanced intrusion detection framework for IoT networks, known as the HOPNET model (Hyper-Parameter Optimized Progressive Neural Network).

Key Contributions:

This research article makes significant contributions to the advancement of intrusion detection in IoT networks:

- Nsl-Kdd Dataset Collection: The research is based on the Nsl-Kdd dataset, a standard source, which serves as the foundation for the proposed system's training data.
- HOPNET Model Design: The paper introduces the innovative HOPNET model, incorporating essential intrusion detection parameters.
- Data Preprocessing and Feature Extraction: Within the HOPNET's preprocessing phase, the dataset undergoes a meticulous filtration process, ensuring the utilization of error-free data for subsequent feature extraction and classification.
- Intrusion Feature Detection: The HOPNET model effectively extracts and classifies both normal and malicious features, enabling the detection and classification of intrusion types.
- Performance Validation: The novel HOPNET model is thoroughly evaluated using key performance metrics.

The organization of this research article is as follows: Section 2 provides an in-depth overview of related works concerning IDS in IoT networks. The challenges associated with traditional IDS are discussed in Section 3. The innovative HOPNET solution, designed to address these challenges, is outlined in Section 4. The model's performance is evaluated and summarized in Section 5, followed by a comprehensive conclusion and discussion of research achievements in Section 6. Through this work, we aim to significantly contribute to the enhancement of intrusion detection mechanisms for IoT networks, ensuring a secure and reliable IoT ecosystem.

2 Literature Survey

In recent times, researchers have made substantial contributions to the advancement of Intrusion Detection Systems (IDS) in IoT networks. A comprehensive literature survey reveals several notable approaches, each with its strengths and limitations. For instance, Jianwu Zhang et al. (Zhang, J., 2020) proposed the Multiscale Convolutional Neural model, which effectively explored spatial features in intrusion datasets and employed spatial-temporal features for classification. While the model exhibited

improved accuracy and reduced False Positive Rate (FPR), it suffered from longer training times due to the backpropagation technique.

Shuokang Huang and Kai Lei (Huang, S., 2020) introduced a comprehensive network that integrated imbalanced control parameters to handle skewed intrusion databases. Although this model yielded remarkable intrusion prediction results, its design demanded substantial resource allocation.

Lu Lv et al. (Lv, L., 2020) presented a precise and efficient Intrusion Detection System (IDS) employing an extreme learning machine with a Hybrid Kernel Function, fine-tuned through the gravitational search algorithm. This method showcased a notable 3.45% accuracy enhancement compared to alternative approaches. Nonetheless, the system encountered difficulties in detection performance due to convergence speed.

Dongzi Jin et al. (Jin, D., 2020) introduced an IDS incorporating a boosting mechanism to mitigate network traffic contributing to malicious incidents. This strategy yielded elevated detection rates for malicious events within IoT networks; however, its intricate nature presented challenges in system design.

Preethi Devan and Neelu Khare (Devan, P., 2020) exhibited an XGBoost deep parameters-based categorization model for IDS. Integrating XGBoost with a Deep Neural Network (DNN), the model achieved consistent 97% classification accuracy for network intrusion. However, the model's limitation was its inability to handle multiclass categorization of intrusion networks.

Aws Naser Jaber and Shafiq Ul Rehman (Jaber, A.N., 2020) outlined an IDS that amalgamated fuzzy clustering (FC) and support vector models, resulting in heightened detection accuracy within wireless communication systems. The approach outperformed existing mechanisms but required more iterations in FCM methods, leading to increased computation time.

This research aims to contribute to this growing body of knowledge by introducing a novel optimized deep features-based intrusion detection framework, HOPNET, specifically designed for Internet of Things networks. By conducting thorough assessments and comparative analyses, we establish the efficiency and effectiveness of the HOPNET model, effectively addressing the limitations evident in current methodologies. Our research is committed to augmenting the security and dependability of IoT communication systems, thereby pushing the boundaries of intrusion detection in IoT applications.

3 System Model and Problem Statement

In the realm of IoT communication systems, establishing resilient intrusion detection is crucial for safeguarding sensitive data and maintaining a defined level of privacy within the communication channel (Liloja, 2023). Existing Intrusion Detection Systems (IDS) deployed in IoT networks often rely on pre-defined features, limiting their ability to predict only common attack patterns. This can leave the network vulnerable to new and evolving threats when an attack feature does not match the saved features, as illustrated in Figure1.

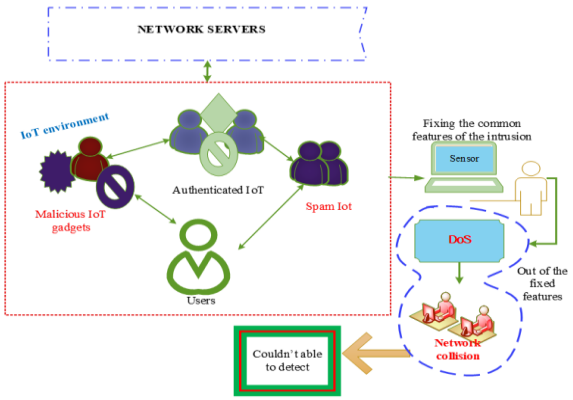

Figure 1: System Model with Problem

In many digital applications, IDS typically employs fixed sensors to predict intrusion behavior based on pre-trained malicious features. However, this approach may fail to recognize certain malicious behaviors initially displayed as normal authorized user actions, revealing their malicious intent later during network communication. These undetected malicious events can significantly compromise the security and performance of IoT systems.

This research focuses on solving the problems found in standard intrusion detection systems (IDS) for IoT communications. It does this by adding a function that fine-tunes certain settings through a smart optimization process within the model.

4 Proposed Hopnet IDS for the IOT Networks

This research presents the innovative HOPNET model, designed to efficiently detect malicious events within IoT networks. The model follows a systematic approach, starting with training the dataset and passing it through a preprocessing layer to remove noisy data with high accuracy. The subsequent stage involves inputting the clean data into the classification framework of the deep belief model, enabling feature extraction and the recognition of malicious incidents. Intrusion prediction is accomplished by contrasting the extracted features with the standard ones. When the test data's features deviate from the regular ones, the system identifies it as an intrusion. The suggested approach employs IoT data as input for the Intrusion Detection System (IDS). The complete process is illustrated in Figure 2.

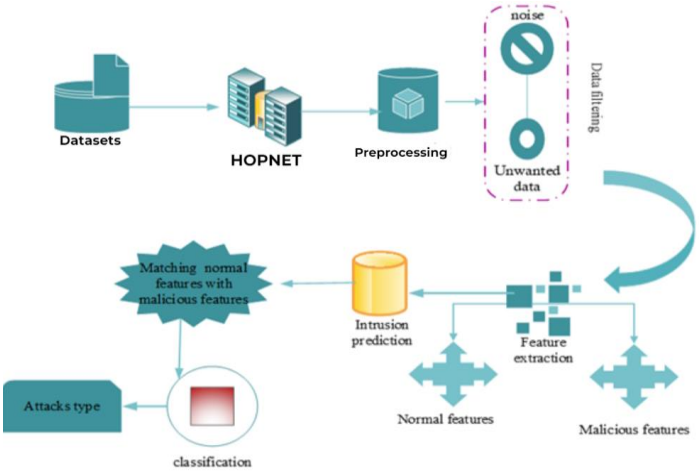

Figure 2: Proposed Architecture

Through this novel HOPNET model, the research aims to enhance the accuracy and efficiency of intrusion detection in IoT networks. By effectively filtering out noise and identifying malicious events, the proposed model contributes significantly to securing IoT communication systems, ensuring a safe and reliable digital ecosystem.

Design of HOPNET Layers

The newly devised HOPNET model comprises five distinct layers: the input layer, hidden layer, classification layer, parameter tuning phase, and output layer, visually represented in Figure 3. This approach ingeniously merges the frog leaping algorithm (Liu, Y., 2021) with a deep neural model (DNM) (Folino, F., 2021), orchestrating performance optimization across all tiers. The frog leaping algorithm is harnessed to enhance the fitness evaluation of frogs within each layer, facilitating parameter refinement and culminating in enhanced outcomes.

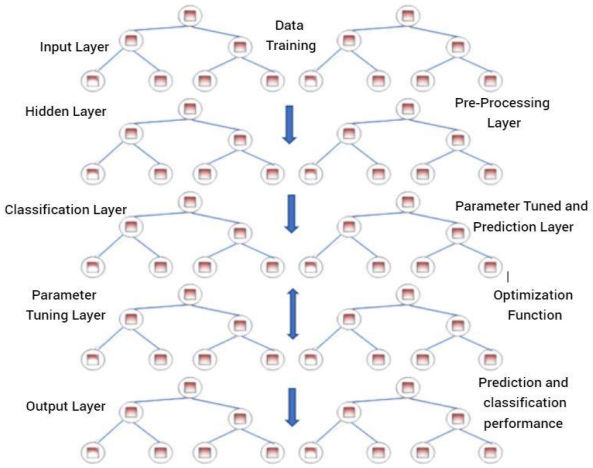

Figure 3: Layers of HOPNET Method

Within the input layer, the trained dataset finds its place, followed by the hidden layer undertaking the crucial preprocessing task to eliminate errors and noise from the data. The outcome of this preprocessing phase furnishes error-free data, subsequently channeled into the classification layer. Hereafter, the classification layer identifies relevant features by implementing a designated threshold value. Post feature extraction, the system proceeds to identify and categorize malicious features into various types.

The HOPNET model's integration of frog leaping optimization and deep neural models enables it to effectively detect and classify malicious events in IoT networks, contributing to enhanced intrusion detection performance and ensuring a more secure IoT communication paradigm.

- **Preprocessing**

Noise removal from the raw dataset plays a crucial role in achieving accurate prediction results. In this current work, the preprocessing function is performed using a Deep Learning (DL) method, which yields superior error removal outcomes compared to conventional models. The training function is defined as *f(ds)* in Equation (1), Here, *"ds"* stands for the dataset, and we have *"f1," "f2," "f3,"* and so on up to "fn". which represent multiple datasets.

$$f\ (ds) = \{f_1, f_2, f_3, f_4 \cdots\cdots, f_n\} \quad (1)$$

Equation (2) features *"tn"* which signifies the tracked noise, and *"Ea"* representing the preprocessing factor. When we use Equation (2), it helps eliminate the current noise, effectively refining the data and producing the filtered version noted as A*. Following this, the data without errors is then directed to the classification layer.

$$E_a = f(ds) - tn(ds) = A^* \quad (2)$$

The utilization of DL-based preprocessing ensures that the finest quality of data is obtained, which significantly enhances the overall performance of the model. The removal of noise and error from the dataset allows the HOPNET model to achieve more accurate and reliable intrusion detection, contributing to the strengthened security and efficiency of IoT networks.

- **Feature Tracking and Extraction**

To effectively track present features in the trained dataset, Equation (3) is employed in this research. The feature tracking function, denoted as B, helps to distinguish between normal features (*l*) and malicious features (*m*). We term this procedure as *"Ff"* wherein the data without errors (A*) is inserted to monitor and track features.

$$B(l,m) = (-1+f(A^*))Ff(l,m) \quad (3)$$

After concluding the feature tracing procedure, the identified malicious features are isolated using Equation (4). The feature extraction is performed utilizing the fitness of the best frog obtained from the optimization algorithm.

$$F_{ext} = B(l,m) > T_{max} \quad (4)$$

To identify the malicious behavior, the threshold variable T_{max} is employed. The feature extraction function, denoted as F_{ext}, is responsible for extracting the features based on the optimized fitness value. Subsequently, the gathered features are stored in the memory designated for feature selection, while the outcomes from the feature selection layer become the input for the classification layer.

By employing these feature tracking and extraction mechanisms, the proposed HOPNET model effectively identifies and isolates malicious events in IoT networks. The utilization of the optimization algorithm and deep neural model ensures the accurate extraction and classification of features, contributing to a robust and reliable intrusion detection system for IoT communication.

- **Classification of Intrusion Types**

In this study, the intrusion categories are divided into Denial of Service (DoS), R2L/U2R and probe. To classify these attacks, the bad frog prediction function is employed, and this function is executed using 5th Equation.

$$C(m) = \frac{td}{probe + DoS + REl - U/R} \quad (5)$$

$$C(td) = td = 1 \quad (6)$$

To classify Denial of Service (DoS) attacks, Equation (6) is put into action. When conducting tests, if the test data (*td*) is marked as 1, it is identified as a DoS intrusion.

$$C(td) = td = -1 \quad (7)$$

Likewise, the identification of probe malicious events is represented by Equation (7). When the test data's label is -1, it is characterized as containing probe malicious attributes.

Algorithm:1 HOPNET

Start

{

int $f_1, f_2, f_3, \ldots f_n$

// initializing the dataset variables

$ds = f_1, f_2, f_3, \ldots f_n)$

// Triggering Neurons

Preprocessing function ()

{

Ea = Filtering noise $\rightarrow A^*$

// Precise information has been obtained without any mistakes.

}

Feature tracking ()

{

$B \rightarrow F_f(l, m(A^*))$

// Monitoring and identifying normal and malicious features

$tracked \quad features \Rightarrow B$

// In this scenario, the features are stored in the variable B.

}

Feature selection ()

{

Feature Extraction $\rightarrow B(m)$

// During this stage, the harmful characteristics were identified and separated, while the regular attributes were placed within the feature tracked layer.

}

classification process ()

{

Intrusion categories = $C_m \rightarrow td = l$

// Initiating the matching function during the intrusion detection phase.

If (*td>0)*

{

Dos

// If the specified condition is met, it is classified as a Denial of Service (DoS) attack.

} else if(*td <0)*

{

R2L and U2R

}endif (*td =0)*

{

Probe

} else (normal)

}

}

Stop

For Probe attack types, in the event that the test information highlight is marked as 0, it is identified as probe as depicted in Equation (8). This successfully determines the different assault types present in the NSL KDD dataset.

$$C(td) = td = 0 \quad (8)$$

Algorithm1 outline the operational procedure of the HOPNET novel model. This neural model incorporates various intrusion detection modules, harnessing their efficacy against current attacks. The optimization process, guided by Frog fitness, fine-tunes the neural parameters, thereby enhancing the precision of intrusion prediction outcomes.

Through this comprehensive classification process, the HOPNET model demonstrates its capability to accurately identify and categorize various intrusion types, thus bolstering the overall security and reliability of IoT networks.

5 Outcomes and Discussions

This section presents the evaluation outcomes of the proposed HOPNET model, followed by a comparative analysis with existing intrusion detection methods. The model's performance is assessed in terms of accuracy, false positive rate (FPR), false negative rate (FNR), precision, and processing time. The evaluation aims to showcase the efficacy and superiority of the HOPNET model in detecting and classifying intrusion types in IoT communication networks.

Case Study

The main objective of this research is to develop an Intrusion Detection System (IDS) tailored for IoT applications, particularly focusing on securing sensitive data and ensuring data privacy in the communication medium. The novel approach introduced in this study is the HOPNET model, specifically designed to forecast contemporary malicious attributes within the trained NSL KDD dataset. For the mathematical validation of the equations as presented in the study, let's assume that a dataset denoted as f(ds) equals 20, and the tracked noise tn(ds) originating from the dataset amounts to 8. By applying these values to Equation (2), we obtain Equation (9), resulting in error-free data, 12, after removing the noise content from the trained dataset, effectively reducing the dimensionality to 12.

$$Ea = 20\text{-}8=12 \quad (9)$$

Subsequently, the feature tracking function is employed by utilizing Equation (3) with the values $l=0$ for normal features and $m=1$ for malicious features.

$$B(0,1) = F_f(0,1)(-1 + f(0,1)) \quad (10)$$

By substituting these values, Equation (10) is obtained. The feature tracking function successfully identifies and removes unwanted data, indicated as $1\text{-}f(0,1)$, utilizing the learning parameter of the frog (-1).

$$F_{ext} = B(0,1) > 0 \quad (11)$$

To validate the prediction of malicious features, Equation (4) is utilized with $T_{max} = 5$, resulting in Equation (11). The output of Equation (4) confirms the extraction of features, and the classified features are then fed into the classification layer.

By following this approach, the proposed HOPNET model effectively predicts and classifies malicious events, enhancing the security and privacy of IoT applications. The study's case study

demonstrates the mathematical validation of the model's performance and its ability to accurately detect and classify various types of attacks in IoT networks.

BM-KMA Performance Analysis

We gauged the efficacy of the innovative HOPNET approach through a comparative analysis, benchmarking it against established models such as DBM, RNM, DNM, and CNM. All evaluations were performed on the same Java platform for consistency. HOPNET outperformed other models in accuracy, sensitivity, specificity, and precision. Its noise removal and feature tracking capabilities contributed to better intrusion detection and faster prediction times. The HOPNET model's adaptability and robustness with the frog leaping algorithm made it effective in handling new attack patterns. Overall, HOPNET demonstrated superior performance, enhancing IoT network security and privacy.

- **Time for Detection**

Within the Intrusion Detection System (IDS), evaluating the duration of the detection process holds paramount importance in gauging the resilience of the proposed approach. Consequently, time-related metrics have been incorporated into this research. In order to assess the reduction in time consumption, performance comparisons were drawn against alternative existing techniques, namely Kernel Nearest Model (KNM), Fuzzy Clustering (FC), and Mean Shift Method (MSM).

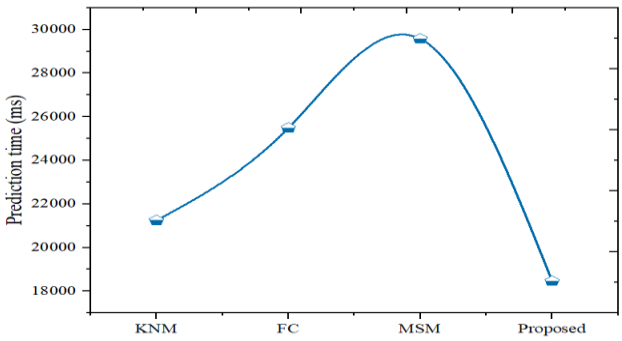

Figure 4: Prediction Time Assessment

The novel HOPNET model showcased the most efficient time utilization, boasting a detection time of 18457ms. In contrast, the Kernel Nearest Model (KNM) registered a detection time of 21247ms, Fuzzy Clustering (FC) exhibited a duration of 25487ms, and the Mean Shift Method (MSM) demonstrated a prediction time of 29574ms, as outlined in Figure 4.

The significantly lower time consumption of the HOPNET model highlights its efficiency and suitability for real-time intrusion detection in IoT networks. Its ability to achieve faster detection times contributes to enhancing the overall performance and responsiveness of the intrusion detection system.

- **Accuracy and Precision**

Ensuring the accuracy and precision scores are well-founded is essential for assessing the resilience of the designed model. The current intrusions are assessed through a comparison between the predicted features *p(m)* and the total attack features *t(m)*, as depicted in Equation (12). This evaluation approach is integral to determining the model's efficacy.

$$accuracy = \frac{p(m)}{t(m)} \tag{12}$$

Here attack prediction score is calculated by dividing the number of anticipated malicious features by the overall count of attack features.

$$Precision = \frac{B}{B + C} \quad (13)$$

Metrics B (true positive) and C (false positive) are harnessed in the computation of precision, a measure denoting the accuracy of predictions across multiple iteration rounds. This is encapsulated in Equation (13).

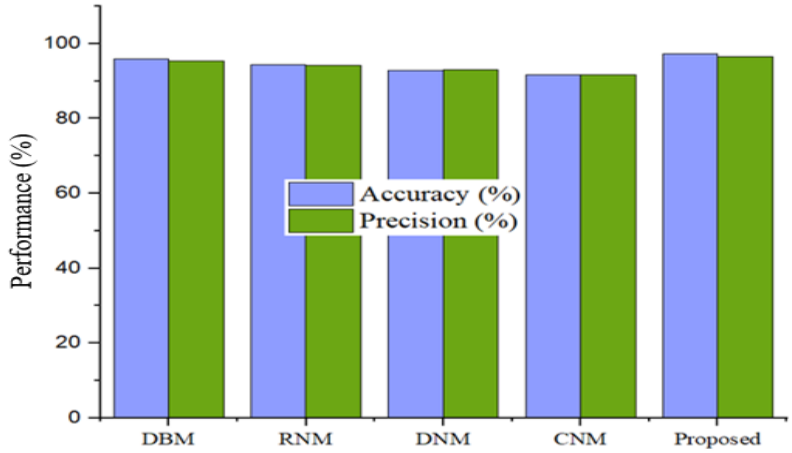

Figure 5: Accuracy and Precision Validation

When compared to other established methods, the proposed HOPNET model showcased remarkable performance. DBM achieved an accuracy score of 95.84% along with a precision of 95.38%. RNM demonstrated a malicious prediction precision of 94.17% and an accuracy of 94.32%. DNM excelled with the highest intrusion prediction precision of 92.96% and an accuracy of 92.84%. Lastly, CNM achieved a prediction accuracy of 91.74% paired with a precision of 91.75%. These statistical outcomes for accuracy and precision are visually presented in Figure 5.

The high accuracy and precision scores of the HOPNET model reinforce its effectiveness in accurately detecting and classifying intrusion events in IoT networks, making it a reliable and robust solution for enhancing network security.

- **Sensitivity, Specificity**

The sensitivity parameter, also known as recall, is utilized to measure the correct and wrong prediction rates, as depicted in Equation (14). Here, false negatives are denoted as *D*.

$$Sensitivity = \frac{B}{B + D} \quad (14)$$

Conversely, specificity serves as an evaluation metric for assessing the effectiveness of the feature extraction function in distinguishing between normal and malicious features. The specificity metric is computed utilizing Equation (15).

$$Specificity = \frac{B_n}{C + B_n} \quad (15)$$

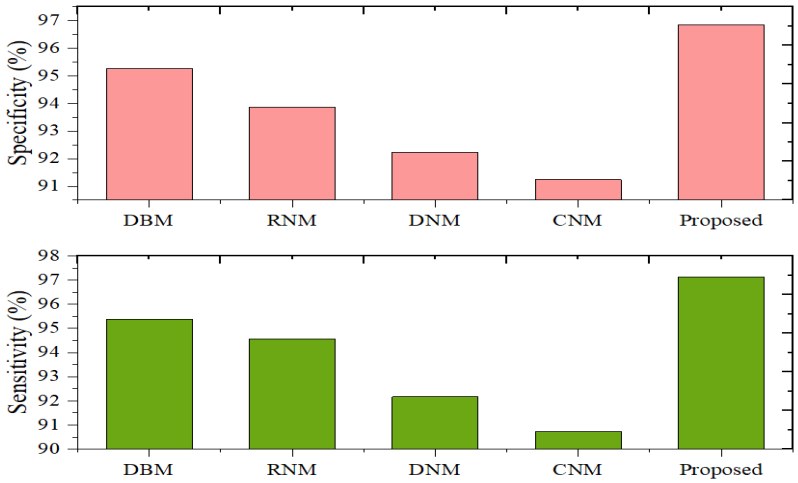

Figure 6: Sensitivity, Specificity Validation

When compared to other approaches, the DBM method achieved a sensitivity score of 95.39% and a specificity of 95.27%. RNM demonstrated the highest sensitivity score at 95.57% along with a specificity of 93.87%. In the case of the DNM technique, the sensitivity score reached 92.17%, and the specificity stood at 92.24%. The CNM method displayed a sensitivity of 90.74% and a specificity of 91.24%. Notably, the proposed HOPNET scheme surpassed all existing methods, achieving an improved sensitivity rate of 97.125% and a specificity rate of 96.85%. These statistical findings are visually depicted in Figure 6.

Discussion

Through a comprehensive assessment of performance, the proposed novel HOPNET model has exhibited superior results in comparison to the other evaluated methods, showcasing its prowess in accurately predicting intrusion events. This underscores the efficacy and dependability of the proposed model for intrusion prediction applications, particularly in early-stage intrusion detection before the data sharing process takes place.

Table 1: HOPNET Performance

Parameter	Validation score
Precision	96.47%
Accuracy	97.38%
Specificity	96.85%
Sensitivity	97.12%
Prediction time	18457ms

Table 1 provides a concise summary of the exceptional performance achieved by the designed HOPNET model. The prediction parameters have consistently earned high scores for all metrics, indicating a stable and reliable performance in predicting intrusion events.

The remarkable results obtained by the HOPNET model underscore its potential as a robust and efficient solution for intrusion detection in IoT networks. Its ability to accurately predict and classify malicious events at an early stage enhances the security and privacy of IoT applications. The stability of the model's performance further strengthens its suitability for real-world intrusion detection scenarios. In summary, the proposed HOPNET model signifies a noteworthy advancement in the realm of intrusion detection for IoT communication systems.

6 Conclusion

In this research, we introduce the HOPNET model, a pioneering intrusion detection framework meticulously tailored for IoT applications. Our empirical evaluations, carried out on the NSL KDD datasets, validate the model's adeptness in successfully predicting an array of attack types, spanning from DoS and U2R to R2L and probe attacks. A pivotal facet of our model lies within its preprocessing function, a mechanism adept at noise filtration and subsequent elevation of data quality. This pristine data is then harnessed in the classification layer, facilitating feature extraction and the classification of intrusion instances. Remarkably, the HOPNET model attains an outstanding intrusion prediction rate of 97.38%, notably surpassing the performance of preceding methodologies by a noteworthy 4% in terms of accuracy. Furthermore, its prowess is highlighted by a substantial reduction in prediction time, clocking in at an efficient 18457ms. This translates to a substantial 1300ms reduction in computation time compared to conventional approaches. Collectively, these findings underscore the remarkable effectiveness and efficiency embedded within the HOPNET model. Its innate capability to bolster IoT network security and elevate intrusion detection capabilities positions it as a significant stride forward in the domain of intrusion detection, warranting substantial consideration for future implementations.

References

[1] Alazzam, H., Sharieh, A., & Sabri, K.E. (2020). A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. *Expert systems with applications*, *148*.

[2] Almomani, O. (2020). A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms. *Symmetry*, *12*(6), 1-20.

[3] Benisha, R.B., & Ratna, S.R. (2020). Detection of data integrity attacks by constructing an effective intrusion detection system. *Journal of Ambient Intelligence and Humanized Computing*, *11*(11), 5233-5244.

[4] Devan, P., & Khare, N. (2020). An efficient XGBoost–DNN-based classification model for network intrusion detection system. *Neural Computing and Applications*, *32*, 12499-12514.

[5] Dua, M. (2020). Attribute selection and ensemble classifier based novel approach to intrusion detection system. *Procedia Computer Science*, *167*, 2191-2199.

[6] Dutt, I., Borah, S., & Maitra, I.K. (2020). Immune system based intrusion detection system (IS-IDS): A proposed model. *IEEE Access*, *8*, 34929-34941.

[7] Folino, F., Folino, G., Guarascio, M., Pisani, F.S., & Pontieri, L. (2021). On learning effective ensembles of deep neural networks for intrusion detection. *Information Fusion*, *72*, 48-69.

[8] Hu, N., Tian, Z., Lu, H., Du, X., & Guizani, M. (2021). A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks. *International Journal of Machine Learning and Cybernetics*, 1-16.

[9] Huang, S., & Lei, K. (2020). IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks. *Ad Hoc Networks*, *105*.

[10] Imrana, Y., Xiang, Y., Ali, L., & Abdul-Rauf, Z. (2021). A bidirectional LSTM deep learning approach for intrusion detection. *Expert Systems with Applications*, *185*.

[11] Jaber, A.N., & Rehman, S.U. (2020). FCM–SVM based intrusion detection system for cloud computing environment. *Cluster Computing*, *23*, 3221-3231.

[12] Jin, D., Lu, Y., Qin, J., Cheng, Z., & Mao, Z. (2020). SwiftIDS: Real-time intrusion detection system based on LightGBM and parallel intrusion detection mechanism. *Computers & Security*, *97*.

[13] Kasongo, S.M., & Sun, Y. (2020). A deep long short-term memory-based classifier for wireless intrusion detection system. *ICT Express*, *6*(2), 98-103.

[14] Khan, M. A., & Kim, J. (2020). Toward developing efficient Conv-AE-based intrusion detection system using heterogeneous dataset. *Electronics*, *9*(11), 1-17.
[15] Kunhare, N., Tiwari, R., & Dhar, J. (2020). Particle swarm optimization and feature selection for intrusion detection system. *Sādhanā*, *45*, 1-14.
[16] Li, X., Chen, W., Zhang, Q., & Wu, L. (2020). Building auto-encoder intrusion detection system based on random forest feature selection. *Computers & Security*, *95*.
[17] Liloja & Dr. Ranjana, P. (2023). An Intrusion Detection System Using a Machine Learning Approach in IOT-based Smart Cities. *Journal of Internet Services and Information Security (JISIS)*, *13*(1), 11-21.
[18] Liu, Y., Heidari, A.A., Ye, X., Chi, C., Zhao, X., Ma, C., & Le, R. (2021). Evolutionary shuffled frog leaping with memory pool for parameter optimization. *Energy Reports*, *7*, 584-606.
[19] Lv, L., Wang, W., Zhang, Z., & Liu, X. (2020). A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. *Knowledge-based systems*, *195*.
[20] Mebawondu, J.O., Alowolodu, O.D., Mebawondu, J.O., & Adetunmbi, A.O. (2020). Network intrusion detection system using supervised learning paradigm. *Scientific African*, *9*.
[21] Mendonça, R.V., Teodoro, A.A., Rosa, R.L., Saadi, M., Melgarejo, D.C., Nardelli, P.H., & Rodríguez, D.Z. (2021). Intrusion detection system based on fast hierarchical deep convolutional neural network. *IEEE Access*, *9*, 61024-61034.
[22] Mighan, S.N., & Kahani, M. (2021). A novel scalable intrusion detection system based on deep learning. *International Journal of Information Security*, *20*, 387-403.
[23] Putra, G.D., Dedeoglu, V., Kanhere, S.S., & Jurdak, R. (2020). Towards scalable and trustworthy decentralized collaborative intrusion detection system for IOT. *In IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 256-257.
[24] Ramakrishnan, V., Chenniappan, P., Dhanaraj, R.K., Hsu, C.H., Xiao, Y., & Al-Turjman, F. (2021). Bootstrap aggregative mean shift clustering for big data anti-pattern detection analytics in 5G/6G communication networks. *Computers and Electrical Engineering*, *95*.
[25] Saranya, T., Sridevi, S., Deisy, C., Chung, T.D., & Khan, M.A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, *171*, 1251-1260.
[26] Sethi, K., Sai Rupesh, E., Kumar, R., Bera, P., & Venu Madhav, Y. (2020). A context-aware robust intrusion detection system: a reinforcement learning-based approach. *International Journal of Information Security*, *19*, 657-678.
[27] Srilatha, D., & Shyam, G.K. (2021). Cloud-based intrusion detection using kernel fuzzy clustering and optimal type-2 fuzzy neural network. *Cluster Computing*, *24*(3), 2657-2672.
[28] Subba, B., & Gupta, P. (2021). A tfidfvectorizer and singular value decomposition-based host intrusion detection system framework for detecting anomalous system processes. *Computers & Security*, *100*.
[29] Sumaiya Thaseen, I., Saira Banu, J., Lavanya, K., Rukunuddin Ghalib, M., & Abhishek, K. (2021). An integrated intrusion detection system using correlation-based attribute selection and artificial neural network. *Transactions on Emerging Telecommunications Technologies*, *32*(2).
[30] Wang, Z., Zeng, Y., Liu, Y., & Li, D. (2021). Deep belief network integrating improved kernel-based extreme learning machine for network intrusion detection. *IEEE Access*, *9*, 16062-16091.
[31] Waskle, S., Parashar, L., & Singh, U. (2020). Intrusion detection system using PCA with random forest approach. *In IEEE International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 803-808.
[32] Zhang, J., Ling, Y., Fu, X., Yang, X., Xiong, G., & Zhang, R. (2020). Model of the intrusion detection system based on the integration of spatial-temporal features. *Computers & Security*, *89*.
[33] Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2020). Building an efficient intrusion detection system based on feature selection and ensemble classifier. *Computer networks*, *174*, 1-21.

Authors Biography

Majjaru Chandrababu, a research scholar in the School of Information and Technology and Engineering at VIT Vellore, is a prominent figure in the field of Cloud Security utilizing a Machine Learning Approach. With a background in Computer Science and Engineering for his undergraduate studies and a postgraduate degree in Information Technology from Hyderabad, he is a respected authority in this domain. As a first author, his contributions have significantly advanced the understanding and application of Cloud Security within the context of Machine Learning.

Dr. SenthilKumar K, a distinguished professional with a PhD and extensive experience in both research and teaching, is a prominent figure in the fields of Cloud Computing and Machine Learning. His expertise is widely recognized, and he has a substantial publication record in esteemed international conferences and peer-reviewed journals. Currently holding the position of Associate Professor at the School of Computer Sciences and Engineering, VIT University, Vellore, he also serves as a mentor to research scholars across diverse IT domains. As the corresponding author, he plays a pivotal role in coordinating and communicating research efforts.