Mitigating Sinkhole Attacks in MANET Routing Protocols using Federated Learning HDBNCNN Algorithm

Sherril Sophie Maria Vincent

Department of Information Technology, Loyola-ICAM College of Engineering and Technology, Chennai, India

Corresponding author: sherrilvincent1512@gmail.com

Abstract

In network topology, the sinkhole attacks ensue while a malicious node deceives it's adjust mode in the routing traffic and it results a predominant interruptions like amplified latency, depletion of energy with conceded data reliability. Moreover a decentralized feature of MANETs are specifically exposed to treats and emphasize the necessity of distinct solutions The proposed study introduces an innovative approach to detecting sinkhole attacks by utilising a Hierarchical Deep Belief Network Convolutional Neural Network (HDBNCNN) integrated with Federated Learning. This integration not only enhances the efficiency of detection but also maintains data privacy by allowing training on multiple nodes without the need to share sensitive information. To further improve the process of identifying sinkhole attacks, the research incorporates the seagull Adaptive Elephant Grey Wolf Optimization (GWO) algorithm for feature selection. This algorithm ensures that only the most relevant attributes are used during the detection phase, increasing the accuracy of the detection process. By combining state-of-the-art Machine Learning (ML) techniques with federated learning, the study aims to not just improve security measures but also tackle the challenges posed by sinkhole attacks in wireless sensor networks. Hence, the proposed study has obtained an accuracy of 99.23, precision, recall and F1-score with 99.72 in detecting sinkhole attacks compared with the traditional methods, significantly increasing the resilience of MANET routing protocols from vulnerabilities. The proposed study aims to enhance the reliability and efficiency of MANETs in attack situations when minimizing overhead from malicious traffic management.

Keywords: Sinkhole Attacks, MANETs, Federated Learning, HDBNCNN Algorithm, Routing Patterns, Decentralized Network, Routing Protocols, Data Privacy, Wireless Sensor Networks

1. Introduction

An ad hoc network refers to a decentralised wireless network that facilitates direct connection and communication between devices, without the need for existing infrastructure like routers or access points [1]. Such a network is able to configure itself and can be formed spontaneously, allowing peer-to-peer communication among devices. Moreover, the networks possess several distinctive features that govern their functionality and operation. The dynamic topology enables nodes to freely move, resulting in frequent changes within the network structure, forming either unidirectional or bidirectional links [2]. These networks demonstrate autonomy by operating independently of fixed infrastructure, making them well-suited for temporary or emergency scenarios. Multi-hop communication plays a crucial role, as data is transmitted through various nodes that function as routers to reach the intended destination. Moreover, many nodes within these networks have limited energy resources, relying on batteries, thus necessitating effective energy management to sustain network operation [3]. These attributes provide ad hoc networks with flexibility and self-organising capabilities, but also introduce challenges like security vulnerabilities and resource constraints. Whereas, Mobile Ad Hoc Networks (MANETs) represent a specific type of ad hoc network characterised by mobile nodes that frequently alter their connections. Both types of networks operate autonomously and are beneficial for temporary or emergency situations [4]. However, MANETs encounter additional difficulties in routing and communication owing to their dynamic topology.

Nowadays, mobile Ad Hoc Networks (MANETs) signifies a section of wireless networks, where it is considered as dynamic topology with the distributed framework [5]. Contrast with traditional networks depend on secure infrastructure, MANETs empowers the nodes to transfer the data to another directly and forms a transition networks. Moreover, MANETs have a crucial and popular research portion due to its challenges they present to the associated protocols. That is considered as an evolving technology that permits network users to communicate without relying on any central infrastructure irrespective of their geographical location. Because of this characteristics that network are often describes

as an infrastructure-less network [6]. MANETS have been a vibrant area of research, driven by the pressing need to offer operators networks that are simple and easy to use [7]. MANETs are helpful in most of the applications such as military emergency rescue or exploration missions [8]. Their origin date back to the 1970s when they are applied in military applications, indicating that they are not new inventions and their commercial success has been obtained because of the advancement in wireless technology. Standards for routing in MANETs have been established. The new group for MANETS has been managed by the Internet Engineering Task Force (IEFT) [9]. The contribution in development of smaller and faster tools makes MANETs the fastest growing area in networking [10]. Although, the mobility of nodes is fast and erratic over time, like all wireless networks, MANETs are more susceptible to attacks and vulnerabilities compared with wired networks. In multi-hop networks the constraints of the wireless network could be serious, while multimedia streams are affected by the cumulative impact of every link associate with a node to node route [11].

The mobility of node could affect the regular path breaks in MANETs, updating routes are more time consuming, and hence packets maybe lost in bursts since they are transmit via non -working paths [12]. To attain an acceptable Quality of service (Qos), the network must be lower susceptible to security attacks, as security vulnerabilities can degrade the QoS of MANETs.The greatest issue in MANETs is the absence of a robust security that can secure them from routing attacks. The design solutions required should not impose limitations on bandwidth and battery power [13]. The significance of the MANETs could be the self-organizing functionality and their security weakness as it leaves room open for both passive and active attacks [14]. MANETs composed by many susceptibilities in which few are affected by their dynamic topology, inadequate energy supply, limited bandwidth, and adaptability [15]. Due to its vulnerability can't be used prevailed architecture adopted from wire network so that required implementing robust security framework that solely function on MANETs [16]. The security goals such as availability, integrity, safety, anonymity, confirmation and confidentiality should be obtain by all QoS-aware security frameworks. Need to develop a customed-designed protocol to attain a safety and QoS-aware network.MANETs are dynamic nature, because of this issue they won't have combined solutions to safety and QoS-based. Thus, the study concentrates on sinkhole attacks by altering protocol in order to ensure better security measures while maintaining quality of service in real time [17].

Sinkhole attacks pose a serious threat to routing systems in Mobile Ad Hoc Networks (MANETs as they allow a malicious node to falsely claim to be the best path to a destination, redirecting all traffic through itself. This can result in data loss, delays, and communication disruptions. Detecting these attacks is challenging due to their subtle manipulation of routing tables without directly affecting data flow. Sinkhole attacks are simpler to carry out than more complicated threats like Sybil or Wormhole attacks, making them a focal point of initial research. The impact of sinkhole attacks on common routing protocols such as AODV and DSR is evident in abnormal routing patterns, making them useful benchmarks for testing security measures and creating effective detection and prevention strategies in MANETs.

In the study, the effective integration of the HDBNCNN algorithm with federated learning provides a robust solution for addressing sinkhole attacks in MANETs. Sinkhole attacks occur when deceitful nodes misguide traffic by falsely claiming to have the shortest routes, posing a threat to network integrity. Utilizing federated learning allows individual nodes to train local models using their routing behaviour data without the need to reveal sensitive information, thereby enhancing privacy and reducing dependency on a central server. These local models are then combined to create a global model capable of identifying complex attack patterns. This approach not only enhances detection accuracy and scalability but also enables quick adaptations to emerging threats, representing a significant advancement in protecting MANETs from such vulnerabilities.

The research contribution of the proposed study is depicted,

- To detect and prevent the sinkhole attacks when observing towards the privacy and data security policies inherent in MANET architectures.
- Usage of Federated Learning allows nodes to train the modules without sharing significant data and improve its privacy.
- The implementation of HDBNCNN algorithm is used to examine traffic patterns and identify anomalies analytic of sinkhole attacks effectually.
- To attain high performance metrics such as throughout, Packet Delivery Ratio (PDR) along with end-to-end delay.

1.1 Paper Organization

The rest of the paper is categorized into four separate sections. Where, Section II deliberates some of the existing sinkhole attack detection in MANET models. Section III deliberates the comprehensive methodology adapted of the entire study with their corresponding algorithms. Followed by the section IV deliberates the overall results and the outcomes obtained after the implementation. Finally the section V briefing a conclusion and adaptable future work for the proposed study.

2. Literature Review

The increasing dependency on both wired and wireless technologies has heightened the importance of security within Mobile Ad Hoc Networks (MANETs), which are particularly vulnerable to a range of attacks. Prominent threats include wormhole, grey-hole, sinkhole, and black hole attacks [18] . A wormhole attack entails an assailant intercepting packets at one point and redirecting them to another, disrupting regular routing procedures. During a grey-hole attack, a deceitful node initially operates normally but selectively discards packets later on, making detection challenging [19].The sinkhole attack occurs when a foe lures traffic towards itself by portraying as having the optimal route, resulting in packet interception or loss. Conversely, a black hole attack involves a malevolent node falsely advertising a legitimate route and discarding all incoming packets, leading to data loss [20]. These attacks take advantage of the dynamic network structure and absence of centralised control in MANETs, underscoring the critical need for robust security measures to ensure dependable communication and preserve network efficiency.

In the study [21] Particle Bee Colony Swarm (PBCS) algorithm is used for identifying the shortest path and the AdaBoost-RF algorithm has been used for attaining better accuracy with minimal loss. For the secured smart city, the study [22] is Clustering Multi-Layer Security Protocol (CL-MLSP) with AdHoc On-Demand Vector (AODV) and Advanced Encryption Standard (AES) algorithm is used for encryption and decryption and attain better performance metrics. The study [23] considered the optimization of routing path for sinkhole through Ant Colony optimization and it is detected by particle swarm optimization method and Message Digest (MD5) is used for hashing along with voting for positioning the nodes. The prevailing study [24] AODV and Adaptive Weighting Based AODV (AWBAODV) and scalable-dynamic elliptic curve is utilized to detect attack and consumed low energy. By using the Fuzzy Q-Learning based method, the sinkhole attacks are minimized in MANET structure [25]. The existing study [26] has been possessed sinkhole detection, the homomorphic encryption and Objective Modular Network Testbed in C++ (OMNET++) simulation is used to calculate the metrics such as delay, packet delivery and throughput. In the study [27], the incoming packets are dropped deliberately by malicious node among the intermediary nodes and it has applied DSR protocol for better throughput, packet delivery across the network. Moreover, K-AOMDV routing protocol is evaluated by ML method to forecast optimal routes along with delay and attacks. Through the application of multi-paths and dynamic nodes. The adaptability of the protocol and the multi-path reduces the black hole and sinkhole attack [28]. The existing study [29] has showed that M-path Sinkhole Attack Detection (MSAD) algorithm is used to find the sinkhole detection, where the clustering concept is applied for detection and it is evaluated with LEACH algorithms and attained 97% of accuracy rate. The hybrid detection structure is designed by Proportional Coinciding Score (PCS) along with MK algorithm, which is applied to increase the accuracy of finding the attacks and minimizing the computational complexities [30].

Correspondingly, in the study [31], Securing IoT Against Sinkhole Attack Using Routing Protocol for Low-Power and Lossy Networks (SoS-RPL) contains dual sections of sinkhole findings, in the first stage position of the RPL is carried out depends on the distance. The second stage has the ability to identify the malicious scores of IoT network under the NS3 settings. The effective attack detecting method can be implemented for securing the data packet that are broadcasted from source to destination. Then, the Proportional Overlapping Score-Based Minkowski K-Means (POS-MKC) is applied to increase attack detection accuracy and to reduce computational difficulties [32]. The prevailing Radio Frequency (RF)Trust method [33] is used to provide the trust-oriented lightweight solution to ensure the safety measures in network. For finding the sinkhole attack RF and Subjective Logic (SL) is utilized to enhance the performance of network. The prevention and detection of sinkhole is done by agent based algorithm. Where, agents are utilized to offer the details about the nodes through the consistent adjacent nodes by elimination steps. So, the attention is not paid by the nodes during the traffic done by sinkhole attacks [34]. The prevailing study [35] is implemented for detecting the sinkhole by Optimized Link State Routing Protocol (OSLR), the structure is used to delete the mischievous routes along with optimization of bandwidth. The outcomes has shown the throughput of 70% and delay with 85%. The multi-routing path is used to detect the sinkhole with QoS and obtained a better results [36]. The dynamic Trusted AODV (TAODV) is used to find the optimal path and false route delay. The NS-2 simulator is utilized to calculate the different protocols and provided better results[37]. The distinct mobile agent-based techniques [38] is used to detect the trust value of the sensors and its repetitive adjacent nodes. The model has given a better results by detecting the sinkhole in Wireless Sensor Network (WSN). For evaluating the security issues Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol is used to infer the effects of network efficiency. The approach has been processed with WSN-Detection System (WSN-DS) dataset and attain better outcomes [39].In the study [40] the CICIDS2017 and UNSW NB15 datasets are used in cluster labelling K-means clustering method and it is implemented in binary classification, then it has attained 0.191 localization error.

2.1 Problem Identification

The problems are identified in the existing studies and it is depict,

- The collaboration detection among the nodes are not applied in flexible network from sinkhole attacks, advocating and supports for a decentralized methods across centralized systems [41].

- Due to the data sparse, the learning process is delayed which may affects the overall efficiency of the attack prediction [25].
- Because of the robust nature of WSNs, the nodes may frequently leave or join the network and hence it may complicate the detection procedure. Thus the algorithm cannot adapt the network quickly [39].

3. Proposed Methodology

MANET's contains mobile devices that can be communicated without the centralized structure or fixed base stations. Then, the centralized framework have a highly flexible range of implementation and more vulnerable security threats especially sinkhole attacks. Moreover, if there is lack in the central authority in handling security makes a robust, distributed security measures for protecting data and routing reliability. Moreover, the MANET nodes are frequently lacking in resources such as power, bandwidth, and processing, and with a network structure that is constantly shifting due to the movement of nodes, the task of identifying and thwarting attacks becomes more challenging. Malicious attacks can quickly cause disruptions in communication, and the absence of a centralised control system makes it hard to deploy conventional security measures. This highlights the urgent requirement for advanced security solutions that are capable of functioning effectively in an unpredictable and hostile setting. For these issues, the proposed approach is implemented for the detection and prediction of sinkhole attacks in Mobile Ad Hoc Networks (MANETs) integrates ML, federated learning, and simulation tools to enhance network security and it is depict in figure 1.

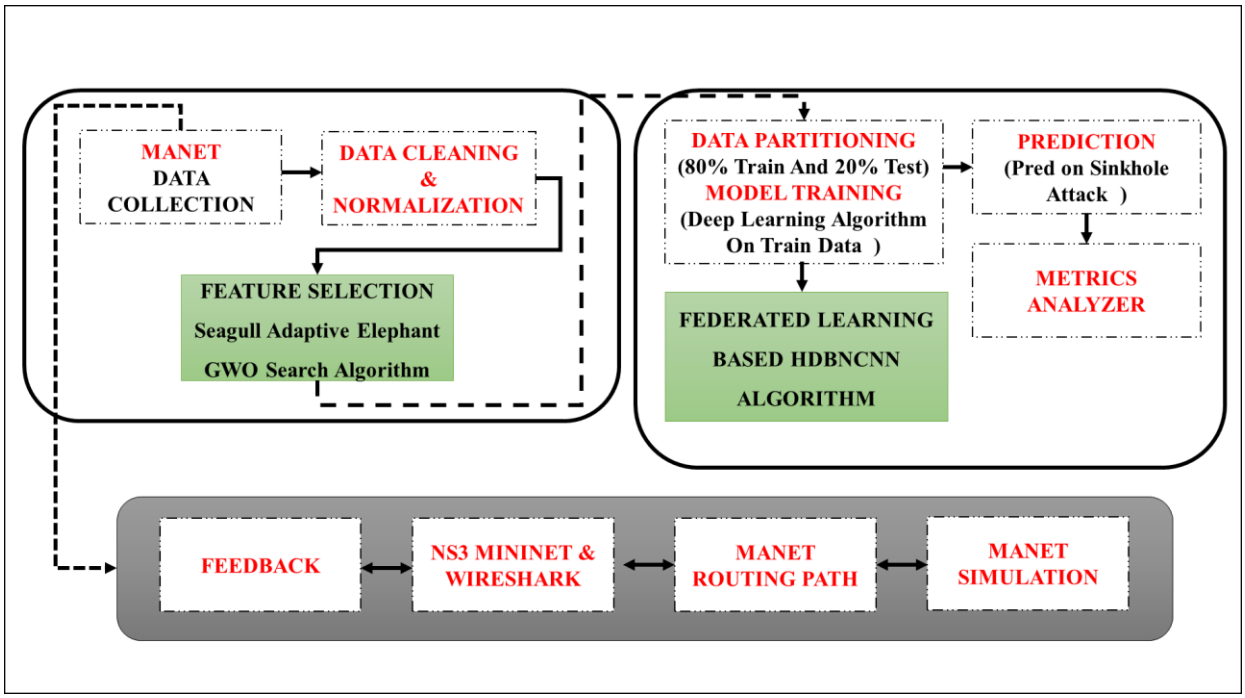

Figure.1 Overall Flow of Proposed Model

Figure.1 illustrates the process initiates by collecting data from the MANET environment, including critical information such as network traffic logs and routing protocols. The initial data is then processed and standardised to eliminate errors and ensure consistent formats, facilitating precise model training. Following this, sophisticated algorithms like the Seagull Adaptive Elephant Algorithm and GWO algorithm are employed for feature selection to identify the most relevant data attributes for optimal model performance. Besides, the data are split into training and testing sets for comprehensive evaluation, followed by model training using a focussed algorithm tailored specifically for sinkhole attack detection. Moreover, the proposed Federated Learning-Based HDBNCNN Algorithm combines federated learning principles with a hierarchical deep learning structure to enhance confidentiality and scalability in decentralised environments. When training is completed, the model is applied to test data for predictive purposes, aiming to efficiently detect malicious activities. Then, the effectiveness of the model is assessed through various metrics, including accuracy and F1-score, during the metrics analysis stage. For further validation of the model's performance, a simulated MANET environment is created using tools such as NS3 Mininet and Wireshark, allowing controlled testing of routing paths under potential attack scenarios. The capability of routing algorithms to maintain communication during possible sinkhole attacks is examined. Eventually, perceptions obtained from the simulation are integrated back into earlier stages of the process to continually improve the detection system, ensuring adaptability and enhanced security against sinkhole attacks in MANETs.

3.1 MANET Data collection

In MANET, an effectual data collection is important for upholding the performance and security, specifically in mitigating threats such as sinkhole attacks. Herein, the nodes constantly collect the data based on the routing concepts, comprising the metrics namely end-to-end delay and packet delivery ratios, whereas the feedback mechanisms permit it to provide the interpretation on routing paths, enabling combined learning with variation for evolving threats. Subsequently, the simulation tools such as NS3 and Mininet remain decisive in analysis the MANET protocols, whereas NS3 delivers a complete background for demonstrating the behaviour of dynamic nodes and evaluating several routing protocols. While Mininet follows mobile node settings over the virtual hosts. Furthermore, Wireshark is a network analyser, which is used to analyse flow of packet flows in the network, assist in finding irregular patterns revealing of sinkhole attacks. The routing paths in MANET are dynamically recognised as nodes there are connected to segment Route Request (RREQ) and responses (RREP), wherein the mischievous nodes can provide the procedures through deceptively promoting the optimum routes. By combing these elements a complete structure is created for analysing MANET, improving a kind of routing dynamics and establishing protection beside susceptibilities by analyse of real-time data and hand-on detection approaches.

3.2 Feature Selection- Seagull Adaptive Elephant GWO Search Algorithm

In the proposed model, for selecting the features Seagull Adaptive GWO Search algorithm is applied for mitigating sinkhole attacks in MANETs. Where, the algorithm combines searching behaviour of seagulls, the social framework of elephant and hunting methods of grey wolves for optimizing the feature selection and tom enhance performance of routing protocol. Initially the procedures starts with population initialization of elephants and seagulls and setting the key parameters like determined iterations with population size. During the iteration, each individual elephant's fitness is calculated depend on classification accuracy, permitting the process to ascend the elephants consistent with the efficiency. Subsequently, the locations are updated till it attains the best solutions. Wherein, every seagull has selected a random elephant as destination and updating its location depend on the determined position along with its individual fitness. Further, this repetition procedure continuous till the process congregates and ensuing the optimal feature selection, which improves the routing protocol and flexible against the sinkhole attacks. The algorithm for the feature selection is expressed below.

Feature Selection : Seagull Adaptive Elephant GWO Search Algorithm
Initialize population of elephants and seagulls Set parameters: max_iterations, population_size, etc. For each iteration from 1 to max_iterations: Evaluate fitness of each elephant using a fitness function (e. g. , classification accuracy) Sort elephants based on fitness Update positions of elephants based on the best solutions found For each seagull in the population: Select a random elephant as a target Update the seagull's position based on the target's position and its own fitness Apply adaptive strategies to enhance exploration and exploitation Update the best solution found so far Return the best features selected based on the final positions of the elephants and seagulls

This algorithm is used for selecting the features by a structured repetitive procedures, which integrates the robustness of seagull and elephant manners with GWO process. At first, the algorithm sets the population of elephants and seagulls when initializing the parameters like optimum iterations and population size. In every iterative process, the every elephant's fitness in calculated by fitness function and it is normally depends on classification accuracy and it is mathematically expressed as

$$F = w_1.Acc - w_2.err\_rate \quad (1)$$

Here, w_1 and w_2 signifies the weights, which can balance accuracy and error rates. Moreover, the elephants are arranged depend on the fitness value, empowering the algorithm by updating the position in accordance with the best solutions. On the other hand, for every seagull located in the population, a random elephant is designated as a target. The position of elephant is updated depend on the position of the target and the seagull's individual fitness and it is denoted as:

$$A_{SG}^{N} = A_{SG}^{O} + r.(A_T - A_{SG}^{o}) + c.(A_{best} - A_{SG}^{O}) \quad (2)$$

Here, r signifies a random factor and c denotes adaptive approaches to improve its investigation and utilization. During this process, the algorithm constantly updates the best solution is established based on the progressing of seagull and elephant. After the completion of the process, the algorithm has shown the final positions of the agents. Besides, it effectively detects the subsets of features that optimizes classification efficiency when reducing the redundancy and

unrelated data. Thus, the method increases the accuracy and computational efficiency through minimizing the dimensionality of used datasets in ML tasks.

3.3 Sinkhole Attack Detection - Federated Learning Based HDBNCNN Algorithm

Correspondingly, the model that proposed a federated learning Based HDBNCNN Algorithm provides an effectual results in finding sinkhole attacks in MANET and exploiting the decentralized feature of federated learning in improving the security for the routing protocol and the flowchart is given in figure.2.

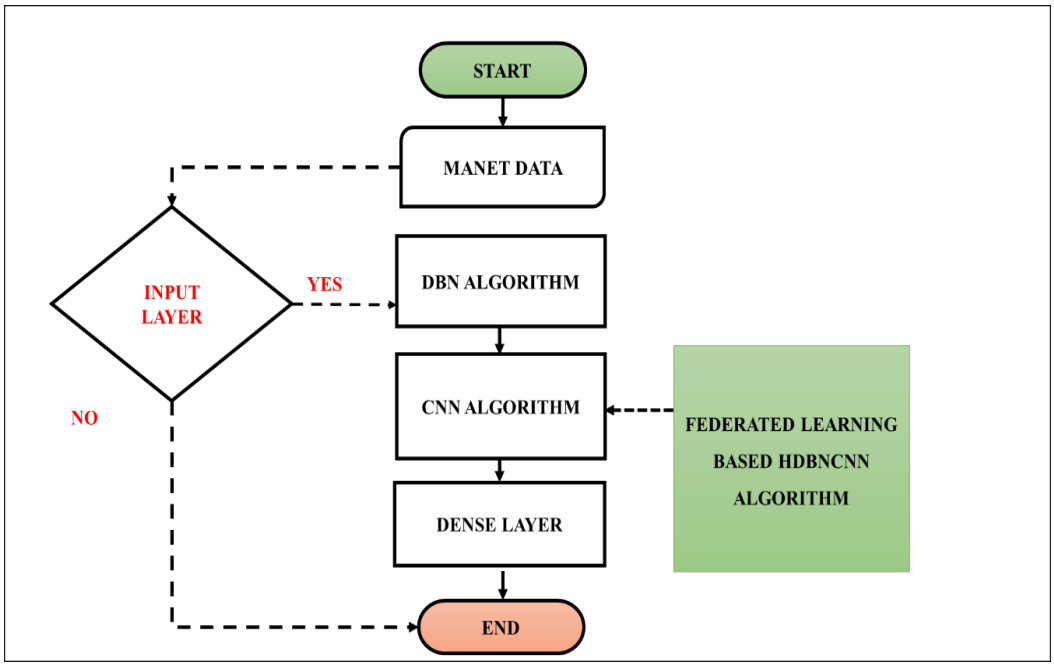

Figure.2 Flowchart of Proposed Federated Learning Based HDBNCNN Algorithm

Figure.2 illustrates a flow of the proposed federated learning based HDBNCNN algorithm. The algorithm involves Deep Belief Network (DBN) and CNN algorithm and dense layer. Initially, the MANET data is refined by the Seagull Adaptive GWO search algorithm, where the MANET data is cleaned and normalized. The redefined data is loaded to the DBN, which serves in extracting the high-level features. It is made of multiple layer of assumptive, hidden variables that assist in taking complication patterns in the data. After that, the output from the DBN is fed to the CNN layer, where the spatial hierarchies are recognised during the feature extraction. And it acts as a filter in detecting patterns and features related to sinkhole attack detection. Then, the output of CNN is managed by the dense layers. The layers are applied to perform the classification tasks through CNN that incorporates the learned features in predicting the presence of sinkhole attack or not. Hence, in the dense layer produces the possibilities of every class and attains the effectual decision making for network security. As a result, dense layer predicts sinkhole attacks by informing nodes about threat or changing the routing path away from negotiated nodes. Moreover, the algorithm of Federated Learning Based HDBNCNN Algorithm is depict below.

Federated Learning Based HDBNCNN Algorithm

Initialize global_model parameters
Set num_clients, num_rounds, local_epochs, learning_rat
For each round in 1 to num_rounds:
Initialize list of client_updates = []
For each client in 1 to num_clients:
Load local_data for client
Initialize local_model with global_model parameters
For each epoch in 1 to local_epochs:
For each batch in local_data:
Perform forward pass on local_model
Compute loss
Backpropagate to update local_model parameters using learning_rate
# Collect the updated model parameters from the client 	
client_update = Get model parameters from local_model
client_updates. append(client_update)

```
# Aggregate the updates from all clients
global_model = Aggregate(client_updates)
# Optionally evaluate global_model on validation data
If round % eval_frequency == 0:
Evaluate global_model on validation_data
Return global_model
```

The proposed algorithm begins with the initialization of model parameters θ and sets hyperparameters such as number of clients (N), training iterations (R), local epochs (E) and learning rate η. For every round r, the empty list is generated for client updation. Besides, every client i is loaded to the local data D_i and sets the local model parameters using the global model. In the training phase, for every epoch e, the local model procedures groups of data, executing forward passes to evaluate prediction by $y_{pred} = f(x_b; \theta_i^{e-1})$, evaluating the loss $L_b = L(y_b, y_{pred})$, and the parameters are updated by the model parameters and adds it to updated list. When the clients have completed the updates, the algorithm collects the updates, normally by averaging $\theta^r = \frac{1}{N}\sum_{i=1}^{N} C_{update_i}$. In case the round is a multiple of the estimation frequency, the global model is calculated by validation data. The procedure processed till the complete rounds are completed, results in a refined global model θ^R, which effectively decentralized data when protecting its privacy.

Hence, the prevention of sinkhole attacks in MANETs can be effectively accomplished by incorporating the Seagull Adaptive Elephant Grey Wolf Optimization (GWO) Search Algorithm for feature selection and a Federated Learning-based HDBNCNN for detecting attacks. The Seagull Adaptive Elephant GWO algorithm can identify the most relevant features that impact network performance and security in real-time, adjusting to changing conditions to improve the selection process. In the meantime, the HDBNCNN uses federated learning to train detection models across multiple nodes without sharing sensitive information, which enhances privacy and security measures. This integrated approach not only enhances detection accuracy by utilizing advanced deep learning methods, but also maintains data confidentiality and decreases computational burden. Further, the model performs in dynamic situations can be done using performance metrics like throughput, network energy consumption, routing efficiency, and overhead caused by federated learning or mitigation actions such as traffic redirection. Furthermore, assessing the model's scalability and its capability to manage high volumes of traffic, mobility, and different types of attacks will offer more understanding of its effectiveness in practical applications.

4. Result and Discussion

4.1 Performance Metrics

The performance of the proposed model is defined by a following metrics and it is discussed in detail.

A. Energy Efficacy and Network Lifetime

- Energy efficacy: It is defined as proportion of useful work completed by the network to the energy consumed and it is expressed as:

$$Energy\ Efficacy = \frac{Useful\ work}{Energy\ consumed} \quad (3)$$

- Network Lifetime: It is defined as a time period where the network is operational formerly whichever node reduces its energy resources. It is formulated as:

$$Network\ Lifetime = \frac{Total\ energy\ of\ network}{Average\ energy\ consumption\ rate} \quad (4)$$

B. Throughput

It calculates ample amount of data that are successively transmitted between one position to other position of the network through a definite time period and it is defined in bits per second (bps).

$$Throughput = \frac{Total\ Data\ tramitted\ bits}{Total\ time\ seconds} \quad (5)$$

C. Delay and Latency

- Delay: It is defined as an accumulation of transmission delay, propagation delay, queening delay and processing delay.
- Latency: It is measured in milliseconds and it has a significant effect on user particularly under real-time applications.

D. Accuracy

It is referred as the ratio between the true results with the total number of cases is evaluated.

E. Packet Loss

Packet loss occurs when one or more data packets do not successfully reach their intended destination during transmission. This can be caused by various factors such as network congestion, faulty hardware, or external interference. High levels of packet loss can negatively impact applications that rely on real-time data transmission, resulting in decreased performance and user satisfaction**.**

F. Confusion metrics

Confusion metrics are information obtained from a confusion matrix, which provides an overview of the effectiveness of a classification algorithm by displaying the numbers of TP, FP, TN, and FN. These metrics are useful for evaluating the accuracy of a model in distinguishing between various categories.

G. Classification Report

A classification report offers thorough analysis of a classification model's performance, showing significant metrics like precision, recall, F1-score, and support for each category**.**

H. Loss

Assessing loss is a method used to determine the accuracy of a model's predictions in comparison to the actual results. It measures the difference between predicted and actual values during model training. Decreasing loss is crucial for improving the accuracy and efficiency of a model, particularly in tasks such as identifying attacks in MANETs.

4.2 Simulated Result

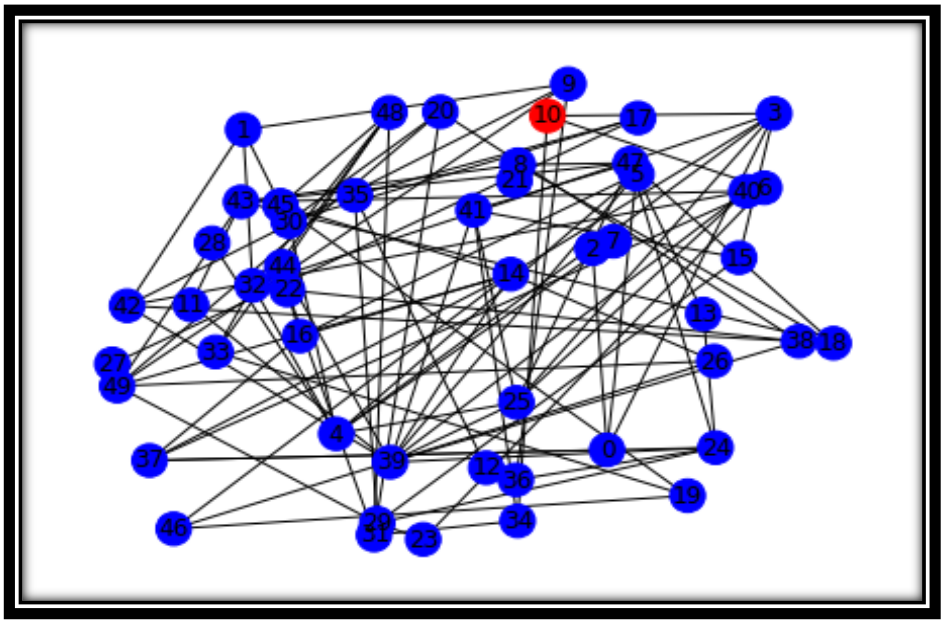

Figure.3 Network Topology

Figure.3 illustrates the connections between the nodes. Node 10 is acknowledged as a key and central node in the network, playing a vital role in how the network functions. This recognition signifies that Node 10 has strong connections with other nodes, allowing for smooth communication. In comparison to other nodes, Node 10 is seen as a crucial player in the data flow and resilience of the network. Its central location gives it the power to affect routing choices and improve the efficiency of information distribution. As a result, Node 10 is a focal point for examination and potential actions in managing the network.

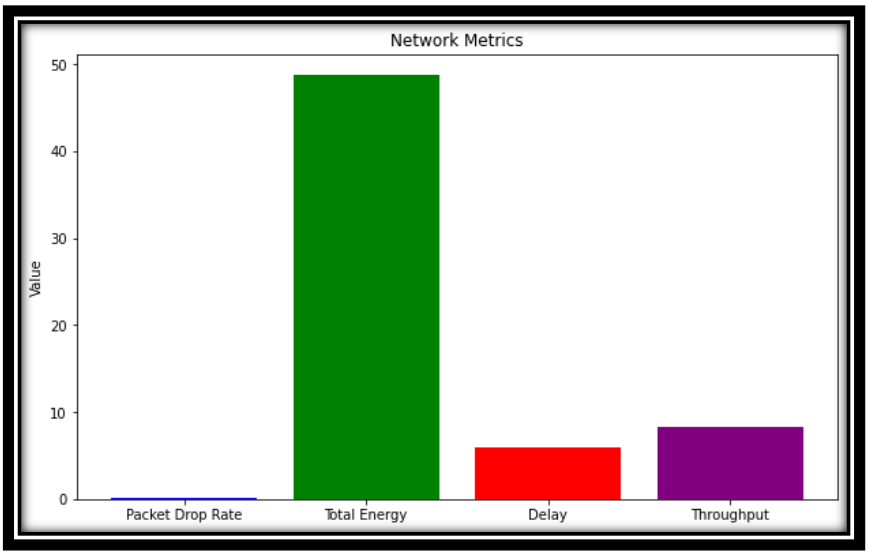

Figure 4 Network Metrics of Proposed Method

Figure 4 demonstrates the network measurements of the suggested model, showing that the network upholds notable efficiency with a low rate of dropped packets, minimal delays, high data transfer rate, and efficient use of total energy. These measurements imply that the suggested model boosts the efficiency and dependability of the network as a whole, leading to better communication and management of resources in the system.

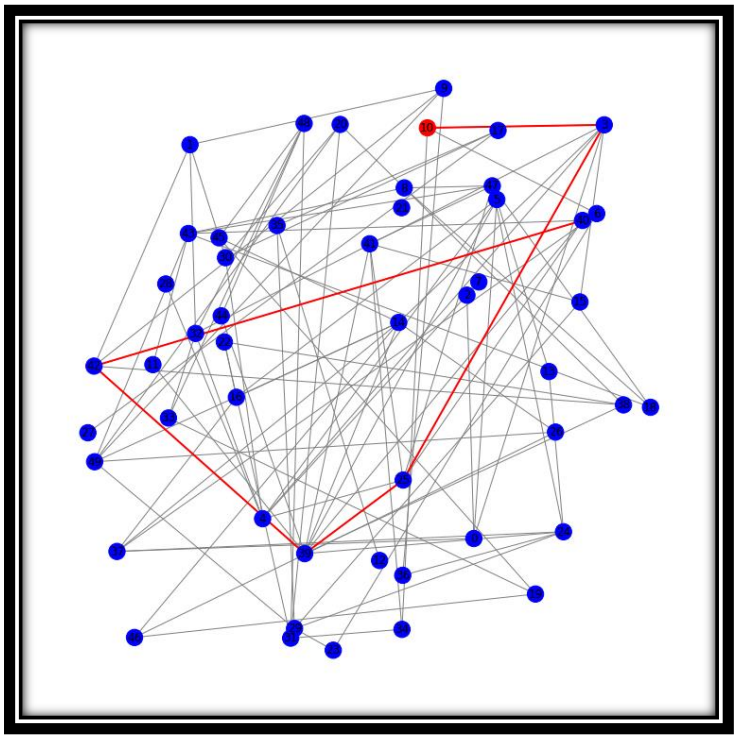

Figure.5 Network Topology of Proposed Method

The network layout shown in Figure 5 displays several linked nodes (0-49), with important nodes highlighted in red (nodes 3, 4, 10, 25, and 39). These specified nodes act as key elements for intricate routes in the network, demonstrating their significance in enabling effective communication. Furthermore, the layout underscores the need for strong duplication, as it offers numerous routes for transmitting data, thus improving the network's overall dependability. This arrangement guarantees that in case some routes are affected, other options are still accessible, enhancing the system's ability to withstand challenges and remain resilient.

.

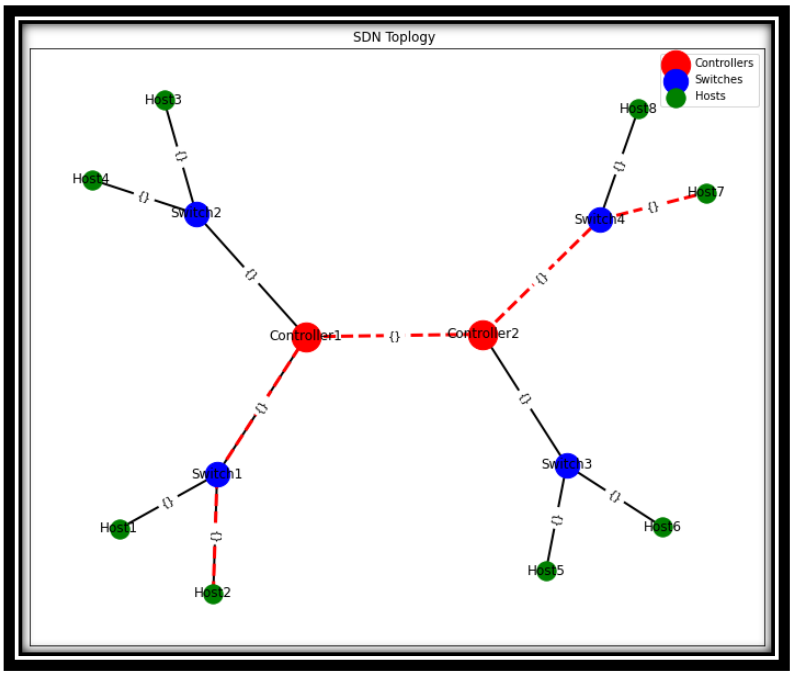

Figure.6 SDN Topology of Proposed Method

Figure 6 depicts a hierarchical network of Software-Defined Networking (SDN) with 2 controllers, 4 switches, and 8 hosts. The controllers, highlighted in red, oversee the switches, which handle data traffic for hosts 1 to 8. The high-priority links between controllers are indicated by red dashed lines, while the solid lines represent connections between switches and hosts. This setup enables efficient traffic management, improves redundancy, and enables the network to continue functioning even in the face of ongoing failures, ensuring dependable performance and reliability.

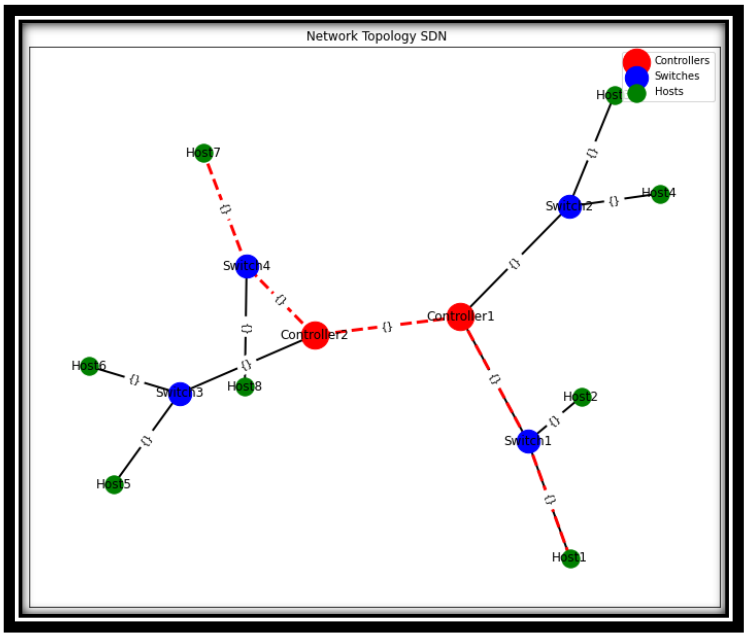

Figure.7 Network Topology of SDN

Figure 7 shows an altered SDN structure that improves manageability by including controllers, switches, and hosts. Hosts 3 and 4 are now linked to switch 2 in this setup, signalling a shift in how switches and hosts share connections. This modification enhances the distribution of loads and redundancy in the network, leading to better handling of data and utilization of resources. The design highlights how SDN can adapt to meet specific network needs, guaranteeing strong performance in different situations. By enabling better traffic control and redundancy, this layout enhances the overall strength and effectiveness of the network system.

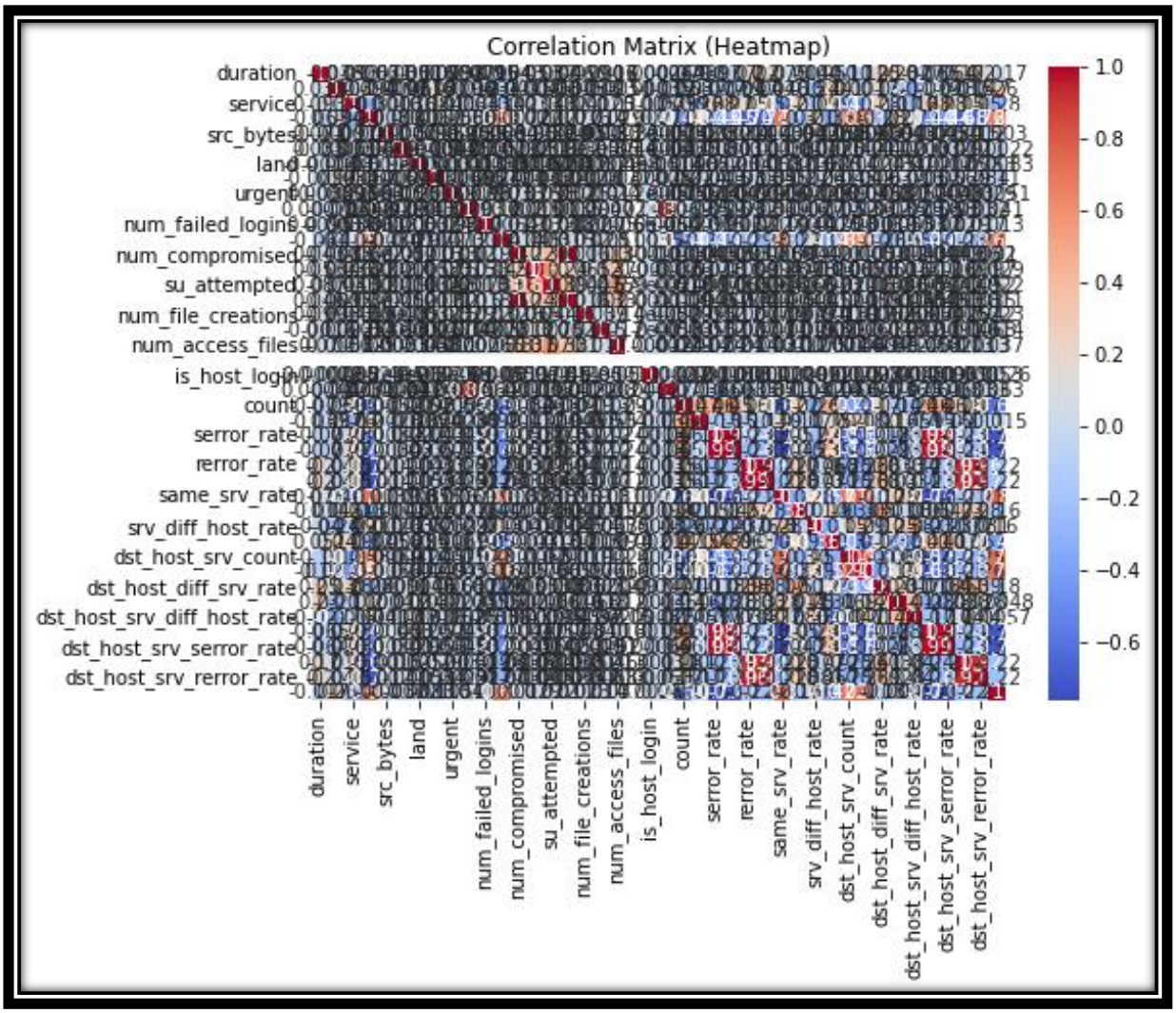

Figure.8 The correlation matrix (Heat map)

Figure.8 shows the correlation matrix (Heat map) is a graphical representation, which illustrates relationships among the variables in the dataset, through colour coding to express the strength and correlations directions. Here, the heat map diagonal components reflect the perfect self-correlation, whereas strong positive are represented in dark red and strong negative are shown in the dark blue colour. Moreover, the colour gradient makes a rapid identification of relationships and easier to select applicable features and reduction in the dimensionality of the former modelling. By emphasizing the robustness of the correlation the scale that ranges from strong negative (-1) and strong positive (+1) facilitates exploratory data analysis, empowering analyst to create an informed decision for feature enclosure, find the outliners and improves the efficiency of the model.

4.3 Experimental Result

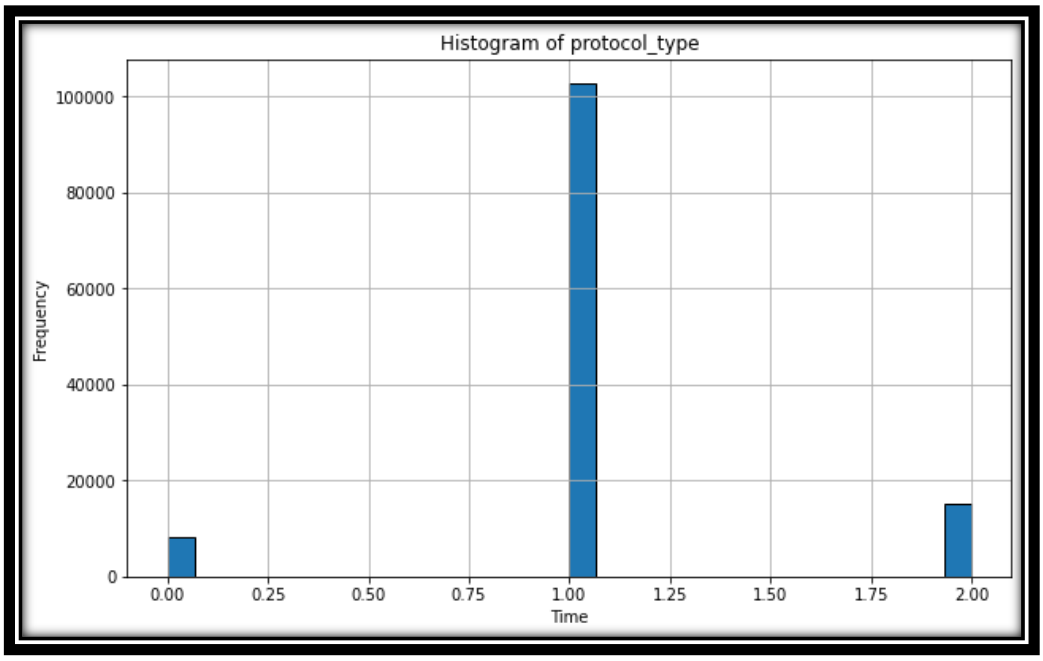

Figure.9 Illustration of Histogram of Protocol_Type

Figure 9 illustrates the distribution of the protocol_type variable over different time periods, classifying the protocols as 0, 1, and 2. The data shows that Protocol 1 is the most commonly used, with over 100,000 instances. On the other hand, Protocols 0 and 2 are used much less frequently. This histogram clearly shows that Protocol Type 1 is the dominant choice, highlighting its significance and prevalence in the dataset throughout the time periods.

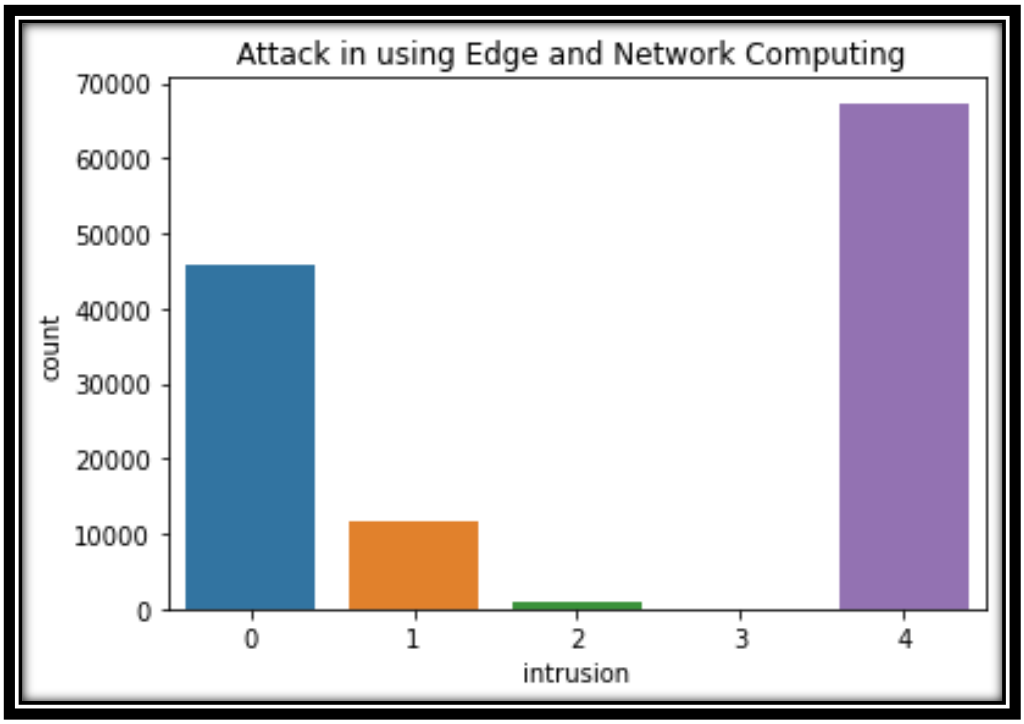

Figure.10 Graphical Representation of Attack in Edge and Network computing

Figure 10 depicts a study on interventions in edge and network computing, showing the distribution of different attack types on a scale from 0 to 4. It is worth noting that Attack 4 is the most prevalent threat, with nearly 65,000 occurrences. Conversely, Attack 0 also has a significant presence, with around 40,000 counts. Attacks 1, 2, and 3, on the other hand, have lower counts, indicating less frequent incidents. This distribution emphasises the need for strategic adjustments to address these attack categories. By prioritising interventions for the most common threats, specifically Attack 4, organisations can improve their system security and allocate resources more effectively to tackle vulnerabilities.

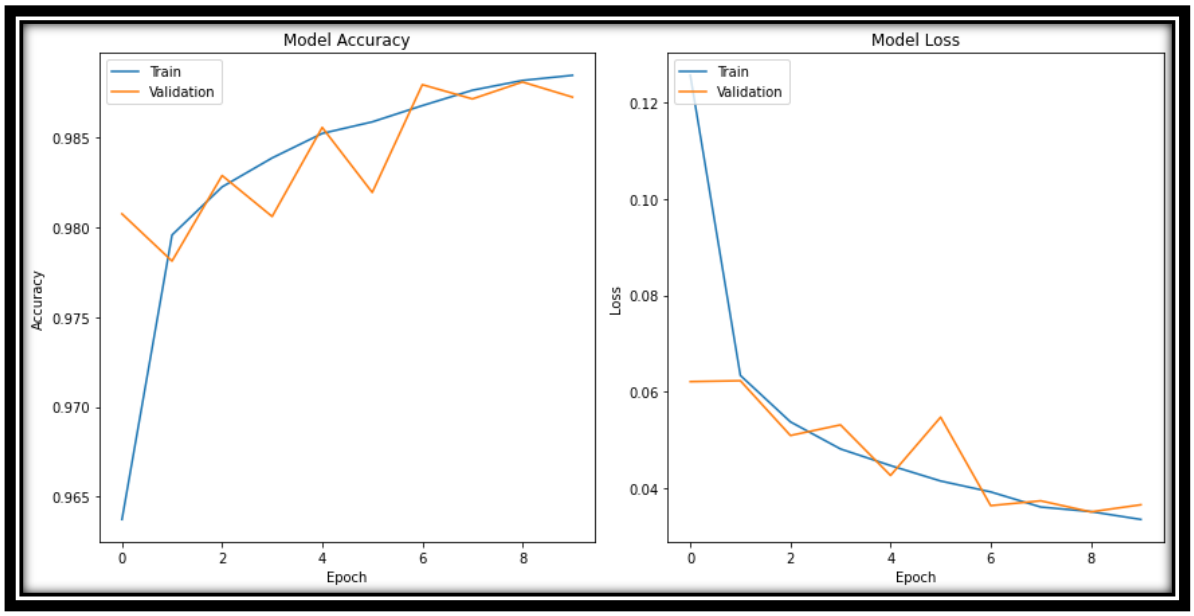

Figure.11 Performance of Accuracy and Loss

Figure 11 illustrates the accuracy and loss performance metrics for both the training and validation stages of the proposed model. The accuracy curve for training consistently improves, eventually reaching a stable point of 98.5%, demonstrating strong learning and model effectiveness. On the other hand, the validation accuracy curve follows a similar pattern but displays some fluctuations, indicating possible inconsistencies in the validation dataset that could impact performance reliability. As for the loss values, the training loss reduces to a minimum of 0.4, while the validation loss also shows a downward trajectory. This pattern suggests that the model has managed to minimize overfitting, as both training and validation losses decrease and approach optimal levels. In general, these findings highlight the model's efficiency and resilience in managing the data, showcasing its potential for dependable performance in real-world scenarios.

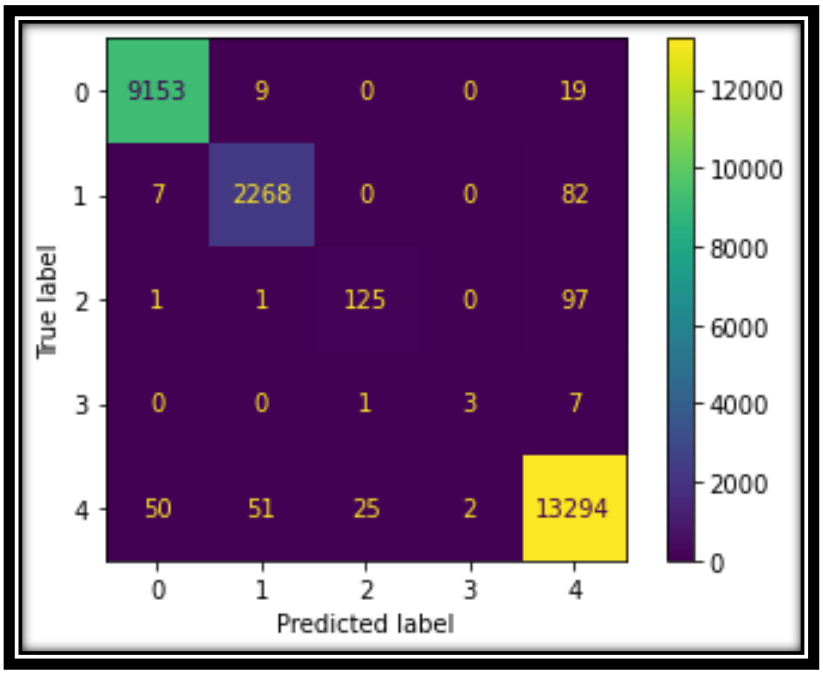

Figure.12 Confusion Matrix of Attacks

Figure 12 illustrates the confusion matrix for different attacks, emphasising how well the classification model performed. Attack 0 had 9,153 predicted labels, while Attack 1 had 2,268 correct predictions. Particularly noteworthy is Attack 4, which had a total of 13,294 accurate predictions, showing its importance in the dataset. On the other hand, Attack 3 was not accurately predicted, indicating difficulties in identifying this specific type of attack. Hence, the classification results show that Attack 4 achieved the most accurate predictions, highlighting its importance in the study.

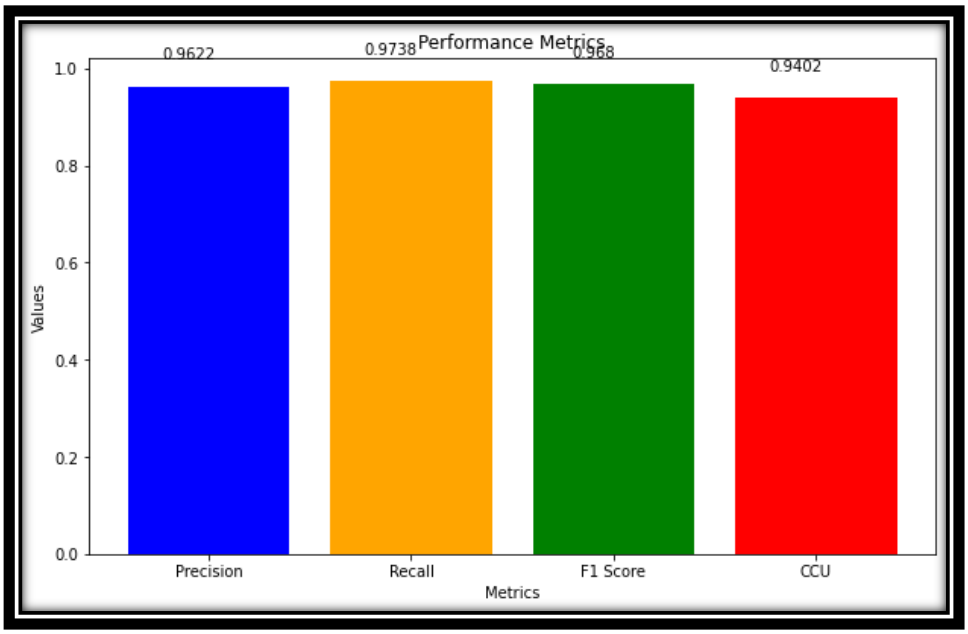

Figure.13 Illustration of Performance Metrics of Proposed Model

Figure 13 illustrates the performance measures of the new model, demonstrating excellent outcomes with a precision of 0.9622, a recall of 0.9738, an F1 score of 0.958, and a Correct Classification Rate (CCU) of 0.9402. These measures suggest that the model shows a high degree of precision and efficiency in its forecasts, indicating its strength and dependability in the specified context. The amalgamation of these performance metrics underscores the model's ability to accurately recognize and categorize pertinent data points in the dataset.

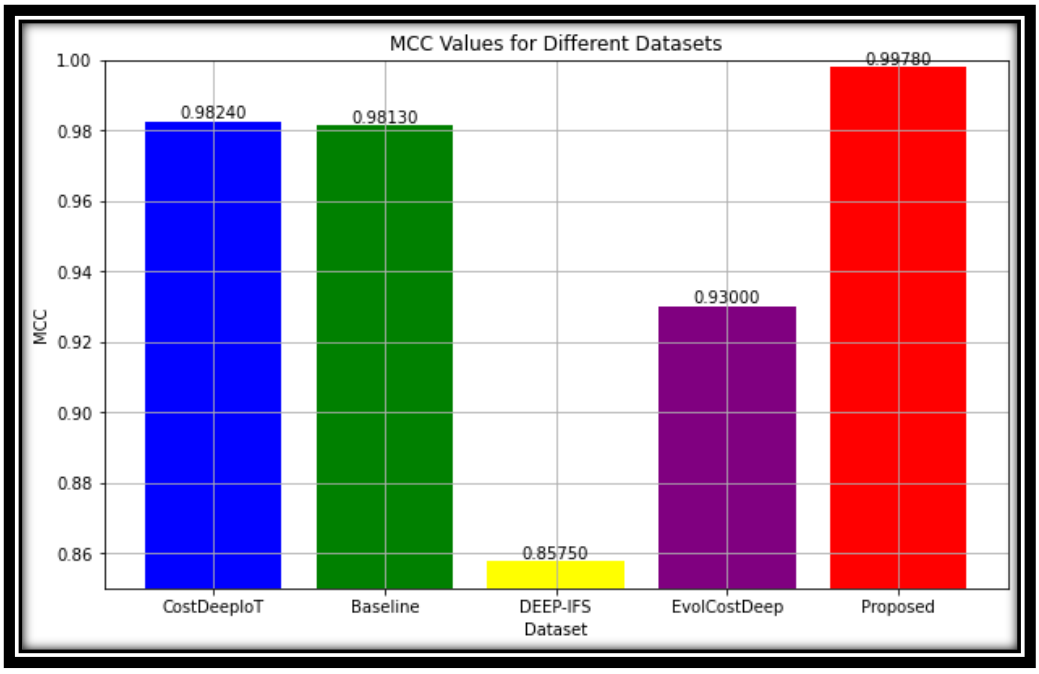

Figure.14 MCC values of Different Datasets

Figure 14 shows the Matthews Correlation Coefficient (MCC) values for various datasets, offering insights into the performance of different models in classification. The new method achieves an impressive MCC of 0.98780, indicating excellent predictive precision. In contrast, CostDeepIot and Baseline models have similar MCC values of 0.98, while EvolCostDeep performs lower at 0.93. DEEP-IFS is notably the weakest performer among the models evaluated. These results clearly demonstrate that the proposed model surpasses its competitors significantly, showing its efficiency in accurately categorising data and suggesting its potential for wider application in classification tasks.

4.4 Comparative Analysis

In this section the outcome of the proposed model is compared with other existing model and it is discussed in detail.

Table.1 Comparison of Existing Dataset with Proposed SDNDDOS during MCC [42]

Dataset	Test MCC
NSL-KDD	0.9724
CICIDS201	0.9965
CIRA-CIC-DoHBrw-2020	0.9975
ICS-SCADA	0.8864
Proposed SDNDDOS	0.9979

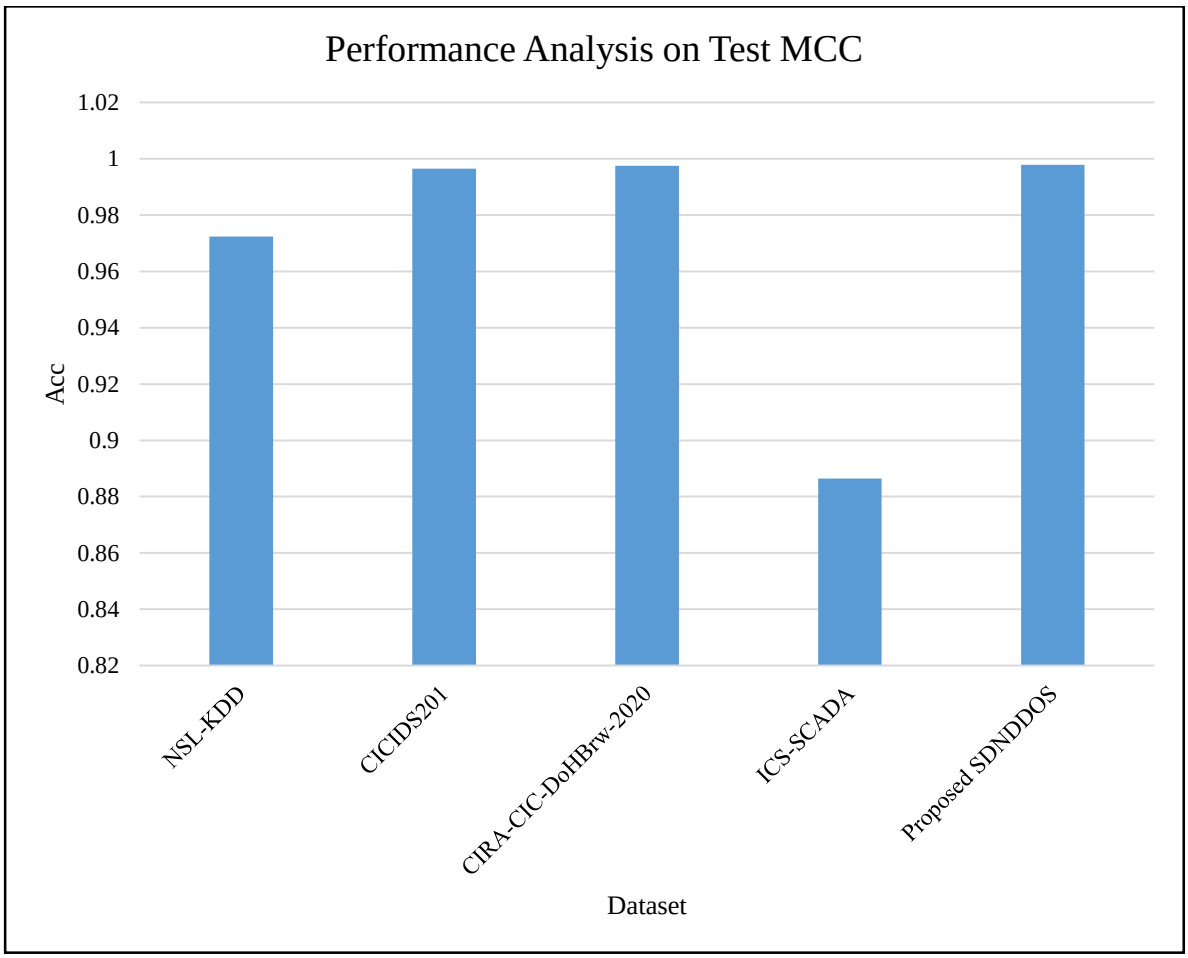

Figure .15 Performance Analysis of MCC Test [42]

The Table.1 and figure.15 has shown the performance metrics for the dataset and it is evaluated by MCC, which determines the efficiency of the different dataset in classification task. It is observed that NSL-KDD dataset has achieved 0.9724 and it shows good prediction. Further, CICID201 dataset has attained 0.9965, whereas the CIRA-CIC-DoHBrw-2020 has scored 0.9975 and ICS-SCADA has recorded a least MCC value of 0.8864. From the results, it is inferred that proposed model has attained high results for different dataset and also in detection tasks.

Table.2 Comparison of Performance Analysis of Prevailing Dataset with Proposed SDNDDOS [43]

Dataset	Accuracy	Precision	Recall	FI-Score	False positive
CICIDS2019	98.70%	99.78%	98.81%	98,78%	18.50%
InSDN	98.20%	97.51%	97.93%	98.27%	18%

Slow-read-98.88%	98.88%	96.80%	95.90%	96.27%	3.65%
DDoS-attack	99.26%	99.10%	99.60%	98.17%	2.25%
Proposed SDNDDOS	99.79%	99.50%	99.80%	98.47%	1.25%

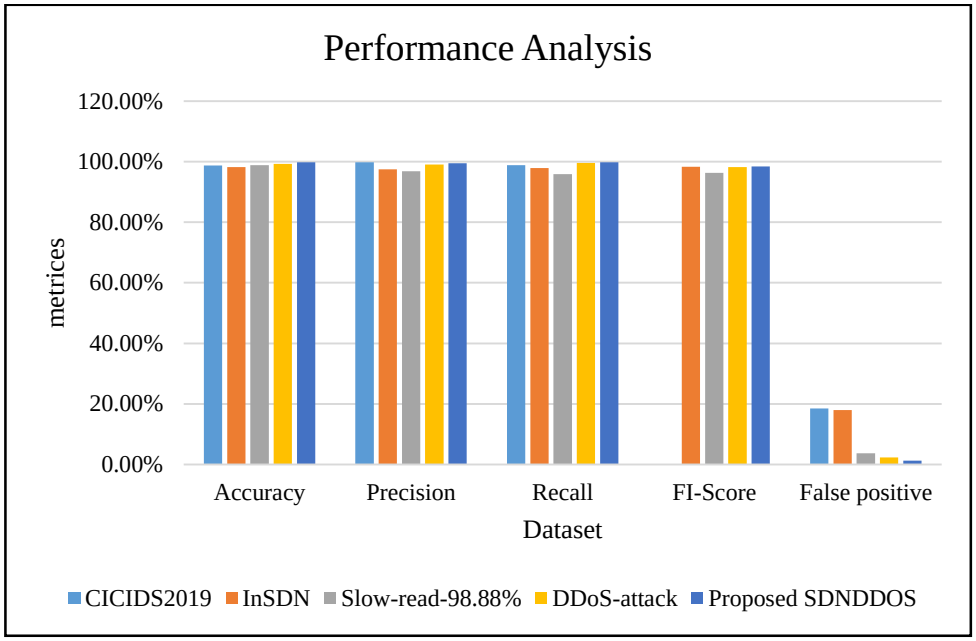

Figure.16 Illustration of Comparison of Performance Analysis of Proposed Dataset with Existing Dataset [43]

The table.2 and figure.16 has illustrated that the CICIDS2019 dataset has attained 98.70 accuracy, precision of 99.78, recall is 98.81, ensuing F1-score of 98.78 and 18.50 of false positive. The dataset InSDN has scored accuracy (98.20), precision (97.51), recall (97.93) and F1-score (98.27) along with false positive (18). Similarly, slow-read dataset has recorded 98.20 of accuracy, 97.51 of precision, 97.93 of recall and 98.27 of F1 score and attained 3.65 of false positive. The DDoS-attack dataset has shown an accuracy (99.26), precision (99.10), recall (99.60) and F1-score is 98.47, then false positive rate is 2.25. From these results it is found that proposed SDNDDOS has reached the highest value of 99.79 of accuracy, 99.50 of precision, 99.98 of recall and 98.47 of F1-score and least false positive rate of 1.25. Hence, it is inferred the proposed SNDDoS dataset has shown an effective performance when it is compared with the other dataset.

Table.3 Comparison of Performance Metrics of Proposed Dataset with Existing Dataset [44]

Dataset	Accuracy	Precision	Recall	FI-Score
Logistic regression	81	83	81	81
Decision Treee	99.57	100	100	100
KNN	99.02	99	99	99
SVM	81.23	84	81	81
Proposed HDBNCNN	99.23	99.72	99.72	99.72

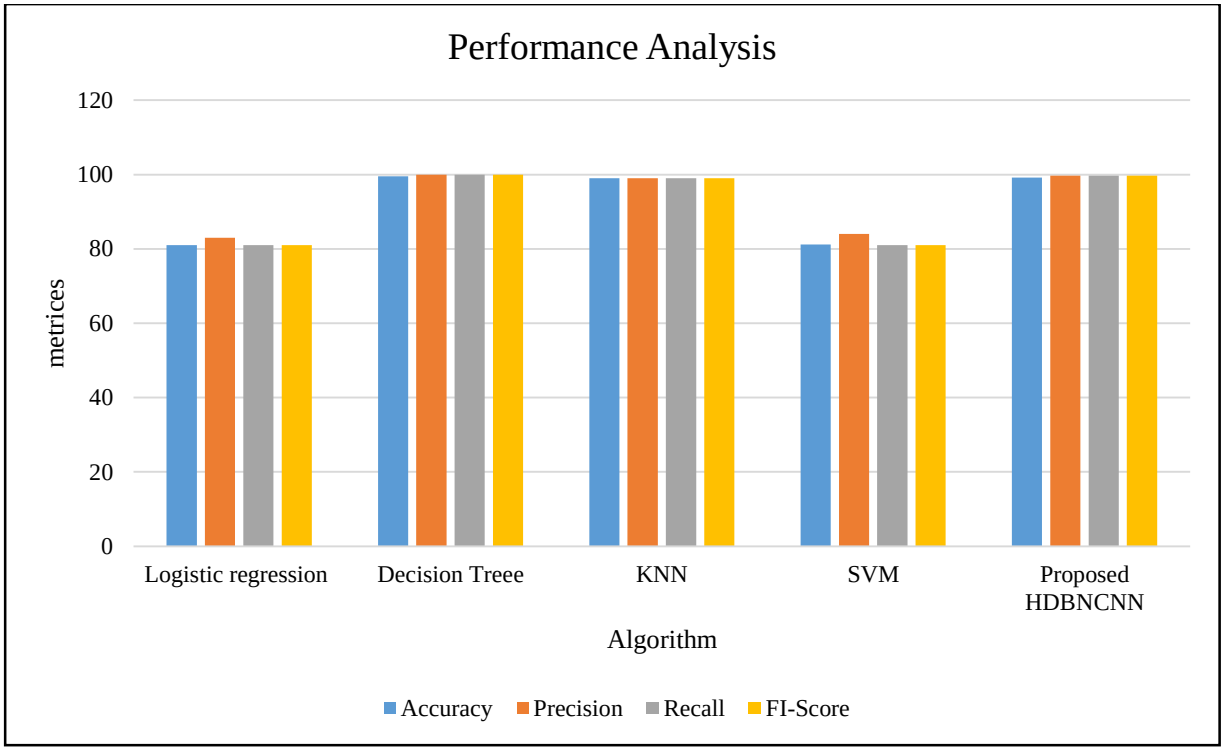

Figure.17 Illustration of Performance Metrics of Proposed Dataset [44]

The Table.3 and figure.17 shows the performance metrics of different ML models on the dataset. It is observed that Logistic regression has attained 81 of accuracy, recall and F1-score along with 83 of precision. Similarly, DT has recorded cent percent in recall, precision and F1-score, then 99.51 of accuracy. The KNN model has scored 99 in precision, recall and F1-score along with 99.02 of accuracy. Moreover, the SVM has achieved accuracy (81.23), precision (84) and recall and F1-score with 81%. Hence, the proposed HCNNABILSTM model has attained 99.23 of accuracy, precision, recall and F1-score with 99.72. These outcomes shows that proposed model has achieved a greater efficiency than other models.

5. Conclusion

The proposed study emphasized the openness in the sinkhole attacks, while malicious nodes deceived the routing traffic by unreliable information in routing. The study presented a proposed methodo for detecting sinkhole attacks through the utilization of a Hierarchical Deep Belief Network Convolutional Neural Network (HDBNCNN) combined with Federated Learning. This incorporation improved the effectiveness of detection but also preserved data confidentiality by enabling training on various nodes without divulging sensitive data. In order to enhance the identification of sinkhole attacks, the study integrated the seagull Adaptive Elephant Grey Wolf Optimization (GWO) algorithm for feature selection. This algorithm guaranteed that only the most pertinent characteristics were employed during the detection stage, thereby enhancing the precision of the detection mechanism. This study provided a valued understanding in secure communication in the decentralized network and obtained an accuracy of 99.23, precision, recall and F1-score with 99.72 in detecting sinkhole attacks compared with the traditional methods, significantly increasing the resilience of MANET routing protocols from vulnerabilities. In future, it will provide a robust protection for different types of attacks in MANETs. Hence, the outcomes emphasized the significance of various methods in directing the security issues in dynamic and exposed network settings.

References

[1] R. Agrawal *et al.*, "Classification and comparison of ad hoc networks: A review," *Egyptian Informatics Journal*, vol. 24, no. 1, pp. 1-25, 2023.

[2] G. Kirubasri, S. Sankar, D. Pandey, B. K. Pandey, V. K. Nassa, and P. Dadheech, "Software-defined networking-based Ad hoc networks routing protocols," in *Software defined networking for Ad Hoc networks*: Springer, 2022, pp. 95-123.

[3] M. Poyyamozhi, B. Murugesan, N. Rajamanickam, M. Shorfuzzaman, and Y. Aboelmagd, "IoT—A Promising Solution to Energy Management in Smart Buildings: A Systematic Review, Applications, Barriers, and Future Scope," *Buildings*, vol. 14, no. 11, p. 3446, 2024.

[4] M. A. Al-Absi, A. A. Al-Absi, M. Sain, and H. Lee, "Moving ad hoc networks—A comparative study," *Sustainability*, vol. 13, no. 11, p. 6187, 2021.

[5] A. H. Wheeb, R. Nordin, A. A. Samah, M. H. Alsharif, and M. A. Khan, "Topology-based routing protocols and mobility models for flying ad hoc networks: A contemporary review and future research directions," *Drones*, vol. 6, no. 1, p. 9, 2021.
[6] B. M. Esiefarienrhe, T. Phakathi, and F. Lugayizi, "Node-based QoS-aware security framework for sinkhole attacks in mobile ad-hoc networks," in *Telecom*, 2022, vol. 3, no. 3: MDPI, pp. 407-432.
[7] Z. A. Zardari, K. A. Memon, R. A. Shah, S. Dehraj, and I. Ahmed, "A lightweight technique for detection and prevention of wormhole attack in MANET," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 8, no. 29, pp. e2-e2, 2021.
[8] F. Safari, I. Savić, H. Kunze, and D. Gillis, "The diverse technology of MANETs: a survey of applications and challenges," *Int. J. Future Comput. Commun*, vol. 12, no. 2, 2023.
[9] S. Yaqoob and E. J. Singh, "A Study of Developments in the Routing Protocols in the Wireless Ad Hoc Networks (WANET)," *International Journal for Research in Applied Science Engineering Technology (IJRASET)*, 2022.
[10] S. Swain, B. R. Senapati, and P. M. Khilar, "Evolution of vehicular ad hoc network and flying ad hoc network for real-life applications: Role of vanet and fanet," in *Modelling and Simulation of Fast-Moving Ad-Hoc Networks (FANETs and VANETs)*: IGI global, 2023, pp. 43-73.
[11] A. Förster *et al.*, "A beginner's guide to infrastructure-less networking concepts," *IET Networks*, vol. 13, no. 1, pp. 66-110, 2024.
[12] J. Lin *et al.*, "Packet Reordering in the Era of 6G: Techniques, Challenges, and Applications," *Electronics*, vol. 12, no. 14, p. 3023, 2023.
[13] R. Uddin, S. A. Kumar, and V. Chamola, "Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions," *Ad Hoc Networks*, vol. 152, p. 103322, 2024.
[14] M. Arif *et al.*, "Sdn-based vanets, security attacks, applications, and challenges," *Applied Sciences*, vol. 10, no. 9, p. 3217, 2020.
[15] M. Matracia, N. Saeed, M. A. Kishk, and M.-S. Alouini, "Post-disaster communications: Enabling technologies, architectures, and open challenges," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1177-1205, 2022.
[16] D. Kafetzis, S. Vassilaras, G. Vardoulias, and I. Koutsopoulos, "Software-defined networking meets software-defined radio in mobile ad hoc networks: state of the art and future directions," *IEEE Access*, vol. 10, pp. 9989-10014, 2022.
[17] S. Khoeurt, C. So-In, P. Musikawan, and P. Aimtongkham, "Multidirectional Trust-Based Security Mechanisms for Sinkhole Attack Detection in the RPL Routing Protocol for Internet of Things."
[18] M. Abdan and S. A. H. Seno, "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 2375702, 2022.
[19] C. Gowdham and S. Nithyanandam, "A Rule-Based Approach for Grey Hole Attack Prediction in Wireless Sensor Networks," *Intelligent Automation & Soft Computing*, vol. 35, no. 3, 2023.
[20] A. Kumar *et al.*, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors and Microsystems*, vol. 80, p. 103352, 2021.
[21] S. S. M. Vincent and N. Duraipandian, "Detection and prevention of sinkhole attacks in MANETS based routing protocol using hybrid AdaBoost-Random forest algorithm," *Expert Systems with Applications*, vol. 249, p. 123765, 2024.
[22] A. K. Sangaiah, A. Javadpour, F. Ja'fari, P. Pinto, H. Ahmadi, and W. Zhang, "CL-MLSP: The design of a detection mechanism for sinkhole attacks in smart cities," *Microprocessors and Microsystems*, vol. 90, p. 104504, 2022.
[23] L. D. R. Popli, "Sinkhole attack detection in manet using swarm intelligence techniques," *International Journal of Engineering Applied Sciences and Technology*, vol. 5, no. 4, pp. 155-160, 2020.
[24] M. Shukla, B. K. Joshi, and U. Singh, "Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET," *Wireless Personal Communications*, vol. 121, pp. 503-526, 2021.
[25] A. Kumari, S. Dutta, and S. Chakraborty, "A fuzzy based Q–learning approach to prevent sinkhole attacks in MANET (FQ–SPM)," *Journal of Intelligent & Fuzzy Systems*, no. Preprint, pp. 1-12, 2024.
[26] H. A. Babaeer and S. A. Al-Ahmadi, "Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking," *IEEE Access*, vol. 8, pp. 92098-92109, 2020.
[27] A. Kaur, A. Oberoi, and J. Singh, "IMPLEMENTATION PAPER ON COUNTERING OF BLACKHOLE AND SINK HOLE ATTACK ON MANET WITH DSR PROTOCOL," *International Journal of Advanced Research in Computer Science*, vol. 12, no. 2, 2021.
[28] S. Kaushik, K. Tripathi, R. Gupta, and P. Mahajan, "Enhancing reliability in mobile ad hoc networks (MANETs) through the K-AOMDV routing protocol to mitigate black hole attacks," *SN Computer Science*, vol. 5, no. 2, p. 263, 2024.
[29] P. Shanmugaraja, M. Bhardwaj, A. Mehbodniya, S. VALI, and P. C. S. Reddy, "An Efficient Clustered M-path Sinkhole Attack Detection (MSAD) Algorithm for Wireless Sensor Networks," *Adhoc & Sensor Wireless Networks*, vol. 55, 2023.
[30] R. K. Dhanaraj, L. Krishnasamy, O. Geman, and D. R. Izdrui, "Black hole and sink hole attack detection in wireless body area networks," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 1949-1965, 2021.

[31] M. Zaminkar and R. Fotohi, "SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism," *Wireless Personal Communications,* vol. 114, no. 2, pp. 1287-1312, 2020.

[32] J. L. Webber *et al.*, "An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks," *Computers and Electrical Engineering,* vol. 111, p. 108964, 2023.

[33] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest–RFTRUST," *Computer Networks,* vol. 198, p. 108413, 2021.

[34] A. V. Jatti and V. Sonti, "Sinkhole Attack Detection and Prevention Using Agent Based Algorithm," *Journal of University of Shanghai for Science and Technology,* vol. 23, no. 5, pp. 526-544, 2021.

[35] B. Esiefarienrhe, T. Phakathi, and F. Lugayizi, "Node-Based QoS-Aware Security Framework for Sinkhole Attacks in Mobile Ad-Hoc Networks. Telecom 2022, 3, 407–432," ed: s Note: MDPI stays neutral with regard to jurisdictional claims in published …, 2022.

[36] *Predicting the Rate of Progression of the ALS Disease in Patients*. (2015).

[37] V. Mankotia, R. K. Sunkaria, and S. Gurung, "DT-AODV: A dynamic threshold protocol against black-hole attack in MANET," *Sādhanā,* vol. 48, no. 4, p. 190, 2023.

[38] H. Khosravi and M. GhasemiGol, "A mobile agent-based method to counter sinkhole attacks in wireless sensor networks," *Jordanian Journal of Computers and Information Technology,* vol. 7, no. 4, 2021.

[39] S. Alsharifi and M. Alanezi, "Detection of Security Attacks in Wireless Sensor Networks," *JMCER,* vol. 2022, pp. 84-93, 2022.

[40] G. G. Gebremariam, J. Panda, and S. Indu, "Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models," *Alexandria Engineering Journal,* vol. 82, pp. 82-100, 2023.

[41] P. Deepa1, M. A. , and S. M. S. , "An Efficient Lung Tumor Detection Using Improved Energy Based Gaussian Mixture Markov Random Field With Distribution Based Long Short-Term Memory Network," *International Journal of All Research Education and Scientific Methods (IJARESM),* vol. Volume 12, no. Issue 4, , 2024.

[42] L. A. C. Ahakonye, G. C. Amaizu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Classification and characterization of encoded traffic in SCADA network using hybrid deep learning scheme," *Journal of Communications and Networks,* vol. 26, no. 1, pp. 65-79, 2024.

[43] A. A. Alashhab *et al.*, "Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model," *IEEE Access,* 2024.

[44] U. H. Garba, A. N. Toosi, M. F. Pasha, and S. Khan, "SDN-based detection and mitigation of DDoS attacks on smart homes," *Computer Communications,* vol. 221, pp. 29-41, 2024.