Computer Communications 196 (2022) 195–206

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

# WOGRU-IDS — An intelligent intrusion detection system for IoT assisted Wireless Sensor Networks

Kadiyala Ramana [a],[*], A. Revathi [b], A. Gayathri [c], Rutvij H. Jhaveri [d], C.V. Lakshmi Narayana [e], B. Naveen Kumar [e]

[a] Department of Information Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, 500075, Telangana, India
[b] Department of Computational Intelligence, SRM Institute of Science and Technology, Chennai, 603203, Tamilnadu, India
[c] Department of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, 602105, Tamilnadu, India
[d] Department of Computer Science and Engineering, Pandit Deendayal Energy University, Gandhinagar, 382007, Gujarat, India
[e] Department of CSE, Annamacharya Institute of Technology and Sciences, Rajampet, 516126, Andhra Pradesh, India

ARTICLE INFO

*Keywords:*
Wireless Sensor Network
Intrusion detection systems
Gate recurrent unit
Whale optimization

ABSTRACT

One of the key mechanisms of the current electronic and wireless frameworks is the assistance of Wireless Sensor Networks (WSN) in Internet of Things (IoT) networks. A WSN typically consists of multipurpose sensor hubs for data sensing, processing, and communication. These networks are more suited to conveying medical data from various geographical regions and sending private medical data to the network owner. However, the worry about various attacks on health care data normally grows daily. These assaults could quickly have adverse impacts on the WSN-IoT (Internet of Things) nodes. Additionally, the low detection rate, significant processing overhead, and resource limitations of current intrusion detection systems all contribute to an increase in false alarm rates when trying to identify various attacks. The unique Whale Optimized Gate Recurrent Unit (WOGRU) Intrusion Detection System (IDS) for WSN-IoT networks is proposed in this research in light of the aforementioned issues in order to effectively identify various attacks. The whale algorithm was used in the proposed framework to tune the hyperparameters of the deep long short-term memory in order to achieve low computational overhead and great performance. Last but not least, validations are carried out using the WSN-DS dataset, and the performance of the suggested work is evaluated using the parameters accuracy, recall, precision, specificity, and F1-score. Additionally, the comparison study was conducted using the current frameworks. The data demonstrates that the suggested framework had an average performance of 99.85 percent for the detection of flooding, scheduling, black hole, and gray hole attacks.

## 1. Introduction

Applications based on WSN and IoT have revolutionized people's life since they can assist with daily duties. WSN and IoT have the potential to make the earth a smart planet. Several IoT network designs were influenced by WSNs. Confusion occurs from the similarity and distinction of the two terms. Despite having restricted processing, memory, and transmission capacities, both networks are effective for real-time applications like border area surveillance, which necessitates round-the-clock monitoring. Some sensors may fail or stop working in an unsafe situation where human aid is not possible. A network can be easily reconfigured using robust and energy-efficient routing techniques. WSN and IoT are prone to DoS, sinkhole, blackhole, gray-hole, wormhole, selective forwarding, Sybil and hello flood attacks, etc. because of these intricacies. Sensing nodes in IoT networks are smarter than those in WSNs, which essentially collect data from sensing devices and send it to the sink node. While WSNs use flat, hierarchical, and location-based routing, IoT networks use IP addressing.

Because of the internet of things (IoT), artificial intelligence (AI), cloud computing, and other technological advancements, the health-care industry has become a more digitalized sector. The fundamental purpose of this digitalized healthcare industry is to provide e-diagnosis and e-treatment to patients all over the world through a medical record that can be accessible via IoT [1–3]. However, accessing the patient's medical record through various communication modes such as (e.g., ZigBee, Bluetooth, WLANs) and through wearable devices such as sensors and actuators which is integrated with different networks (e.g., edge, cloud, mobile networks) causes many vulnerabilities in terms of security threats, authentication issues, privacy issues which leads to poor performance including in the healthcare industry [4,5]. Currently, many healthcare sectors utilizing the medical-cloud engines for patient's record storage, accessing purpose which enhances the

[*] Corresponding author.
*E-mail address:* ramana.it01@gmail.com (K. Ramana).

https://doi.org/10.1016/j.comcom.2022.10.001
Received 24 April 2022; Received in revised form 17 September 2022; Accepted 2 October 2022
Available online 13 October 2022

unauthorized access and hacking. Various hackers compromise the cloud engines through their unauthorized networks in order to manipulate the medical data (e.g., by inserting fake data or with unknown attacks) which will jeopardize the integrity or the availability of the healthcare services provided by these systems [6]. As a result, intelligent security solutions for the protection of healthcare data and threats prevention by compromised intrusion detection system (IDS) based IoT devices must be designed and developed. Many researchers have developed the IDS for general IoT devices which is not focused on the healthcare sectors [7]. The AI-based IDS systems plays a key role in security and privacy systems in recent days [8].

Applications for smart cities, transportation, homes, and healthcare are available through WSN and IoT-based communications. In this communication context, access to and processing of data must be done in real-time (for example, real-time monitoring of a patient, environmental condition in an industrial plant, and so on). Big data analytics can be used to find patterns in the large amount of data that IoT devices produce (for example, future health prediction of a patient). The internet offers such a communication setting. Other problems with it include privacy and security. The detection of intrusions in WSN and IoT is being researched by several scholars. The next section examines current research challenges and potential directions for intrusion detection research in WSN and IoT contexts.

Since most WSN and IoT intrusion detection systems do not offer complete protection against all threats, they are not secure. Some suggested tactics are attack-specific and ineffective against numerous attacks at once. We need to develop intrusion detection methods that can endure numerous attacks concurrently. Designing this technique can be challenging due to resource restrictions on sensors and IoT devices.

In WSN and IoT-based communication contexts, WSN sensors and smart IoT sensors have constrained computational power, storage capacity, and battery life. Therefore, these systems are unable to carry out computationally, communicationally, and storage-intensive operations. Use tiny messages for detecting intrusions. Large signals may use up other device resources during transmission and reception, rapidly depleting the sensors' batteries. To lower computing, communication, and storage costs without compromising security, we must develop intrusion detection systems.

A sizable heterogeneous network with its own capabilities and requirements is the WSN-integrated IoT. Intrusion detection is challenging in such a communication context. EHRs for some users may be stored and processed on a cloud server with IoT capabilities. Data is transmitted to the cloud via BAN devices. As a result, a network of various devices is established. All communication devices must be protected by an intrusion detection method. More study is required.

How to protect the privacy of data across resources. Applications that require secure data use WSN-based IoT connectivity (for example, smart healthcare). In order to sense health data and transmit it to cloud servers for storage and analysis, smart health sensors are implanted in or wrapped around the bodies of patients. Intruders may attack such a communication environment. This results in leaks and interruptions in data transfer. Data that is both stored and in transit must be protected. We require fresh, effective approaches to safeguard transmitted and stored data. IoT intrusion detection methods should respect user and/or device privacy.

There are many different sorts of devices in WSN and IoT-based communication systems, ranging from full-edged PCs to low-powered sensor devices and RFID tags. These gadgets employ a number of communication protocols. The range of communication, storage, processing power, and operating system of these devices varies. To safeguard all gadgets and technologies, we must develop an efficient intrusion detection approach.

Intrusion detection is made more difficult by WSN and IoT heterogeneity. Although heterogeneity enables the integration of several application domains, it also makes intrusion detection more difficult. The intrusion detection system needs to be strong and appropriate when a smart home application needs to access data from a healthcare sensing device. The majority of data is kept in the cloud, necessitating new intrusion techniques. To provide seamless communication across IoT platforms for such applications, we need strong intrusion detection algorithms.

The foundation of security devices is utilizing AI to develop multiple models that can assess network data instantaneously and forecast its nature [9]. Because of the huge volume and velocity of Sensor data, new Machine Learning (ML) difficulties in data science have arisen. Clustering, categorization, prediction, and analysis are some of the challenges that have been defined [10]. Almost every year, at least one or more assaults are launched, causing the failure of numerous cloud-based platforms and apps or posing a data leaking concern. Operating attacks are a fantastic illustration of stream data system applications because of their streaming nature [11]. ML provides powerful results for too vague problems especially for human formalization. The enactment of most Internet-based security frameworks in a smart healthcare system (as in other smart systems) is comparable to compiling a list of mischievous traits to block them. Intruders, on the other hand, are constantly refining and changing their techniques, making it incredibly difficult to predict when their negative features will be placed into the security black-list [12]. An intruder can inject undesirable data or get unobserved access to confidential data by making a minor alteration to the security protocol. To overcome this, we developed an intellectual IDS model which is combined with reinforcement learning approach to achieve better performance in healthcare sector in security perspective.

### 1.1. Contribution of the research

1. A Novel and Hybrid Learning Model based WSN-IOT-IDS (WOGRU-WSN-IDS) has been proposed in which GRU network hyperparameters are optimized by the whale algorithm which solves the classification problems and high-speed detection mechanism. It has higher accuracy, low complexity and low detection time.
2. This study uses the WSN-DS datasets to conduct the experimentations and comprehensive comparative analysis has been carried out using the existing learning model-based IDS system.
3. A scalable, high accurate, high speed WOGRU IDS System is introduced to handle the larger WSN datasets.

The paper structure is as follows as: Related work is introduced in Section 2. Section 3 discuss about the proposed framework, with background views on whale Optimization and GRU. The experimentation details, dataset description, result analysis along with comparisons are presented in Section 4. Finally, the paper is concluded in Section 5.

## 2. Related works

Since clients must exchange their raw data with third parties, such cloud or edge servers, to train a model, traditional centralized ML-based IDSs are susceptible to sensitive data privacy violations and attackers. To address this issue, a specific set of controls and methodologies defining the relative value of datasets, their sensitivity, compliance requirements, and the installation of suitable safeguards are needed. These methods are conceivable, but would necessitate more resources than the standard ML-based IDSs, in addition to higher computing costs.

Nadia [13] discussed real-time IoT devices and vulnerability scanning. The review article's design characterization, attack categorization, and outcomes for IoT systems inspired the suggested investigation. IoT's diversity and heterogeneity make attack detection and prevention difficult. Service stabbings, black holes, spoofing, IP attacks, denial, wormhole, and manipulation are frequent system-impacting attacks. ML and DL algorithms' impact on identifying and preventing cyber-attacks is discussed. Common intrusion detection algorithms include SVM, DT, and KNN.

Rohan Doshi et al. [14] proposed a supervised learning approach for NIDS router networks. Support vector, random forest, decision tree, KNN, and light weight deep neural networks are used. These algorithms extract stateless router properties including packets, bandwidth, source and destination ids, etc. DoS and DDoS are generated using real-time datasets between sender and receiver. Learning algorithms use real-time data to predict assaults. The proposed system has a single-attack limit.

Vaishali et al. [15] developed an ML system to identify harmful attacks in inclined structures. PUFs engineering is a lengthy procedure for cloning on the cloud and pursuing identification; avoidance is key due to its portability. The suggested system fits unique structures and includes a probabilistic, discriminator framework to clone attack potentials to strengthen CRP convention security. Plan and testing consider Referee, XOR, and Lightweight models. Different ML calculations, such as direct relapse and arbitrary woodlands.

[16] presents Content-based Filtering (CBF), information-based (KBF), collaborative separating (CF), and hybrid sifting (HF) for IoT frameworks. These cooperative frameworks recommend objects similar in essence or matching the usage and portion vector. AI-based CF model evaluations envisage dim information in a framework. The suggested models lack attack or recommender frameworks.

A recommender system or proposition structure filters information to anticipate a client's "rating" or "tendency" to like something. Brain network designs to beat lattice factorization cooperative separating models. This paper adjusts the multi-facet perceptron brain network for suggestion frameworks. MLP has different layers and concealed hubs have lighter weights. The proposed DL algorithm is not appropriate for large companies, and wounded difficulties are not accounted for [17].

Eclipse is used to adapt Apache Mahout's local area isolation. Gathering, batching, recommenders, etc. are computed. Math vectors, groups, Apache Hadoop, and Lucene vectorizer are in normal libraries. Finally, euclidean distance is measured [18].

This study presents a 3-layer IDS that employs a regulated technique to manage digital attacks on IoT enterprises. It has 3 stages: (1) Sort and profile the common lead of each IoT device associated to the framework. (2) Find hazardous packages on the framework when an attack occurs. The framework is tested with 8 well-known open-source devices. The viability of the proposed IDS configuration is evaluated using 12 assaults from 4 framework-based attack types, including DoS, MITM/spoofing, reconnaissance, and replay. The structure is additionally tested against 4 difficult multi-stage attacks [19].

The author offers a GP-based rule evolution approach for spotting new network attacks [20]. Reproduction, mutation, crossover, and dropping condition operators are used to develop new laws. New rules detect network risks automatically. Experiments show that rules generated by GPs utilizing KDD 1999 Cup data had a low "False Positive Rate", a low "False Negative Rate", and a high rate of recognizing unknown attacks.

Goeschel et al. [21] combined SVM, decision tree, and Nave Bayes calculations. Using SVM, they differentiated normal and aberrant data. They used a decision tree to identify explicit attack types. A tree-based technique can differentiate between known and unknown attacks. They used Nave Bayes to find unseen attacks.

Li et al. [22] suggested a K-closest neighbors' discovery strategy using equal figuring methods for faster estimate (GPU). They altered KNN's neighbor-selection rule. The standard KNN takes the top K nearest examples as neighbors, whereas the streamlining technique picks a fixed rate (for example, 50%). The continuing method incorporates discrepancies in information delivery and works effectively with poor data.

Moustafa et al. [23] used a GAN. The "KDD99" dataset lacks additional data, resulting in generalizable ML models. GAN was used to improve the dataset. GAN data resembled KDD99 flow data. Integrating this information into the training set reveals attack variations. They tested the accuracy of the entire dataset with the enlarged dataset using eight different assaults. According to experiments, adversarial learning improved 7 attack types.

**Table 1**
Data labeling for different attacks

| Sl.no | Type of attack | Labeling |
|---|---|---|
| 01 | Normal | 1 |
| 02 | Blackhole | 2 |
| 03 | GrayHole | 3 |
| 04 | Scheduling | 4 |
| 05 | Flooding | 5 |

Weak learners slightly outperform a random classifier. Ensemble classifiers are built by combining many weak learners to improve classifier performance. Majority vote, bagging, and boosting are common merging strategies [24]. Despite combining the weaknesses of part classifiers, the group classifier has produced excellent results in some mixes. Lightweight interruption recognition was proposed by Liu et al. [25]. They used SVM to classify attacks (target DDoS). Chang et al. [26] studied assault irregularity and location. They used LR, SVM, Decision Tree, RF, and ANN for ML calculations.

Modern smart healthcare security applications have significant disadvantages when employing standard machine learning-based intrusion detection systems. Encoding and transmission time are needed to transfer huge amounts of sensor data to a remote server. Low bandwidth might hinder data transfer. Cloud servers are far from sensors, therefore data must pass through numerous edge nodes. Long-distance data transport prohibits a VSN with multiple sensor nodes from providing real-time QoS. Traditional IDSs' cloud-based architecture is ineffective for achieving these goals. In conventional centralized model-training systems, users upload their datasets to the cloud server. Wireless communications and core network connections between clients and servers influence DL model training and judgments. The connection must be stable even when the network is down. Unpredictable wireless connections between client and server might degrade system performance and cause malfunctions. Model training and conclusions can be affected.

As data owners' privacy concerns develop, administrative procedures must be implemented to restrict data collection to those involved in processing and with express consent. Traditional centralized model-training architecture cannot assure privacy because clients send raw data to the server.

## 3. Proposed framework

### 3.1. System overview

The dataset collection unit, the data preparation model, and the intelligent detection model and response module are the primary divisions of the suggested Intrusion Detection Systems (IDS). The data collecting unit first gathers the data from various sensor locations before sending it to the data preparation unit. The suggested WOGRU-IDS module can find the intrusion if it occurs in the network once the preprocessing is finished. The module promptly informs the users of the existence of an attack if it is detected. The proposed WOGRUB structure is displayed in Fig. 1. The member node (MN) addresses a sensor hub, Cluster Head (CH) addresses a group head hub and sink addresses base station. The intrusion detection system is implemented in cloud nodes,with sacrificing the computational overhead and energy consumption of the network.

### 3.2. Data preprocessing

The dataset collected needs preprocessing mechanism since it consist of both letters and numerical. In preprocessing, letters are converted into numeric values. For the better identification of attacks, multi-class labeling is adopted in this paper. Below Table 1 presents the multi-class labeling for each attack.

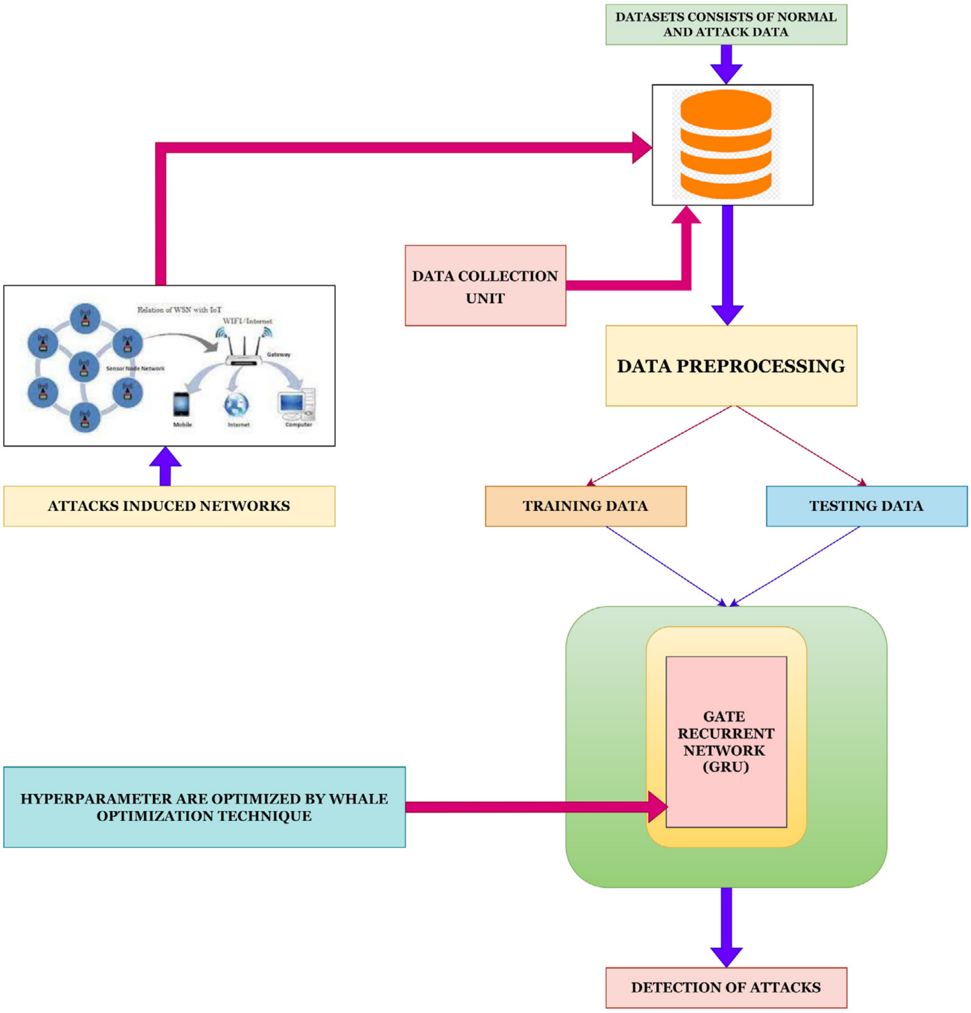


**Fig. 1.** Architectural diagram for the proposed framework.

**Table 2**
Types of attributes used for experimentation.

| Sl.no | Features used | Descriptions |
|---|---|---|
| 01 | Node ID | For every node, The IP address is allocated |
| 02 | Cluster ID | CH's IP address |
| 03 | Initial Energy of Nodes | It is the initial energy utilized to send the data to CH. |
| 04 | Energy Consumption(Ec). | Energy consumption used for the data transfer between nodes and sink for every iteration. |
| 05 | Residual Energy | This energy is the remaining energy once the data is transferred at each iteration. |
| 06 | Cluster Head distance | The distance between the CH and other nodes |
| 07 | Throughput | It is the ratio between the received bytes to the transmitted bytes (at CH Side) |
| 08 | Throughput-2(T) | It is the ratio between the received bytes to the transmitted bytes (at sink) |
| 09 | Delay(ms) | Measurement of data reaching time form node to CHs |
| 10 | Received Signal Strength Indicators (RSSI) | This parameter is predominantly used for the detection of signal strength which in turn used to calculate the distance. |

To have the better classification mechanism, normalization technique [27] is adopted. Some data features have minimum values of less than 1 and maximum values of hundreds of thousands, which affects classification algorithms. We must normalize the continuous data [28–31]. The attributes along with the descriptions is presented in Table 2.

### 3.3. WOGRU-IDS classification model

This section discusses about the working mechanism Gate Recurrent Unit and Whale optimization for the proposed architecture.

#### 3.3.1. GRU networks – Its working mechanism

Deep neural networks (DNN) have been used to overcome the constraints of classic neural networks in terms of high classification rate and better feature extraction. This is because DNN has strong non-linear fitting characteristics. However, because the temporal relationship between the training samples was not taken into consideration, these DNN have an erroneous classification ratio. Recurrent neural networks (RNN) can be used to overcome the aforementioned issue. For the most part, RNN models are explicitly intended for time series of information and large information examination in light of its quick recognition movement. Here the immediate charts are produced by the hubs with their particular groupings. With this assertion, this strategy shows dynamic synchronizations of groupings. For the information successions process inward memory is used. To foresee the future qualities, RNN for the most part utilizes the previous information. However, more applications struggle to remember the prior attributes and cause a disappearing gradient problem when there is a significant change in time between the past and the future information. As a result, this

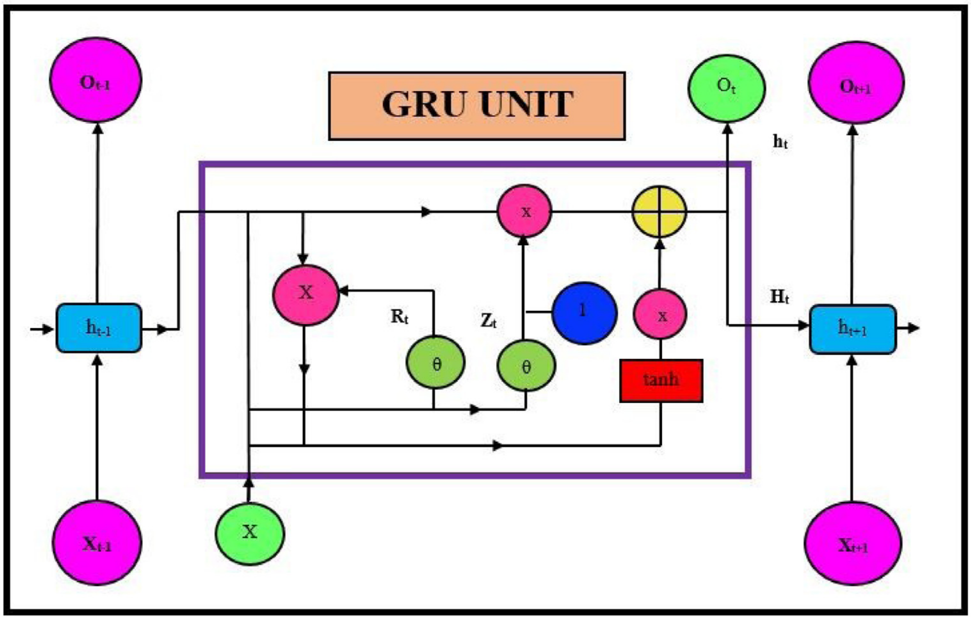


**Fig. 2.** GRU network architecture.

method needs to be updated to enable real-time applications. The RNN is modified as an LSTM structure to address these problems.

This study use Gated Recurrent Units since the detection/prediction time is crucial while constructing the IDS (GRUs) [32]. GRU is considered as the most fascinated variant of Long Short term memory (LSTM). The main aim is of this framework is to combine the forget gate and input vector as single vector. This network support the long term sequences and also long memories. The complexity is very much reduced when compared with the LSTM network. The GRU network architecture is illustrated in Fig. 2.

Following Eqs. (1)–(5) are coined by Chung to represent the characteristics of GRU:

$$h_t = (1 - x_t) \odot h_{t-1} \ + \ x_t \odot h_t \tag{1}$$

$$h_t = g(W_h x_t \ + \ U_h(r_t \odot h_{t-1}) \ + \ b_h) \tag{2}$$

$$z_t = \sigma(W_h x_t \ + \ U_z h_{t-1} \ + \ b_z) \tag{3}$$

$$r_t = \sigma(W_h x_t \ + \ U_r h_{t-1} \ + \ b_r) \tag{4}$$

The overall GRU characteristic equation is represented by

$$P = GRU \sum_{t=1}^{n} [x_t, h_t, z_t, r_t(W(t), B(t), \eta(\tan nh))] \tag{5}$$

where $x_t$ is the input feature in the current state, $y_t$ is the output state, $h_t$ is the module's output at the current instant, $Z_t$ and $r_t$ are update and reset gates, $W(t)$ is weights $(t)$ is bias weights at current instant. These GRU network are used to extract the temporal features from the pre-processed ECG data. The GRU model learns the R-R interval peaks with larger changes and uses the Cuttle fish method to optimize the weights to the GRU in order to suppress over-fitting problems. To overcome the complexity problem, modified GRU is used in this research in which the hyperparameters of the dense layers are optimized by the whale algorithms.

### 3.3.2. *Whale algorithm*

One of the most fascinating and enormous animals on Earth is the whale. The adult whale can reach lengths of over 30 m and weights of almost 180 tonnes. There are seven different species of whales: the Killer, Minke, Right, Sei, Humpback, and Blue Whale. The fact that a whale does not actually sleep is what makes its life the most intriguing. This is due to the fact that its brain is constantly just partially asleep so that it can breathe from the water's surface. Whales are very intelligent, emotional creatures. It is because some areas of their brains have spindle cells, which are also present in our brains. Whales are cleverer and more intelligent because they have nearly twice as many cells as humans. When hunting, they also speak in their own language. Whales have the ability to live alone, in groups, or in families that last their entire lives. The humpback whale obtains its food by using the bubble-net feeding technique. Whales use this method to catch krill or tiny fish that are nearby. The whale creates bubbles in the shape of the number 9 while on the hunt for food. The bubbles rise using this technique in spirals and double loops. The whale makes bubbles in a spiral around the prey as it swims up to the surface of the water during the upward spiral formation, diving to a depth of 12 m. A metaheuristic optimization algorithm based on biological principles is developed using models of this spiral bubble approach as shown in Fig. 3. The steps that make up the mathematical model are listed below. Whale Optimization Algorithm (WOA), which first proposed in [33], increased interest in the recent years. The following simulation of humpback whale behavior and movements during their search for food and supplies is used to calculate this stochastic search technique.

WOA differs from other optimization algorithms in that it just needs to alter two parameters, in addition to its intriguing behavior. These factors enable a seamless changeover between the exploration and exploitation stages.

**Encircling prey:** In order to update their process to the best goal, the search process starts at the beginning and circles the meals in the immediate area. As observed in Eqs. (6) and (7), the working process is described in statistical formulations.

$$If \ (c \ < \ 0.5 \ and \ mod(k) \ < \ 1)$$

$$V \ = \ modu\{(k.V \ - \ V.q)\} \tag{6}$$

$$V(q+1) \ = \ [V(s) \ - \ \{c.q\}] \tag{7}$$

Where, $c = 0.1$ (constant), "$V(q+1)$" represent the best solution and other attributes are estimated as per the below formulations in Eqs. (8) and (9).

$$M \ = \ mod\{2 * c * k - c\} \tag{8}$$

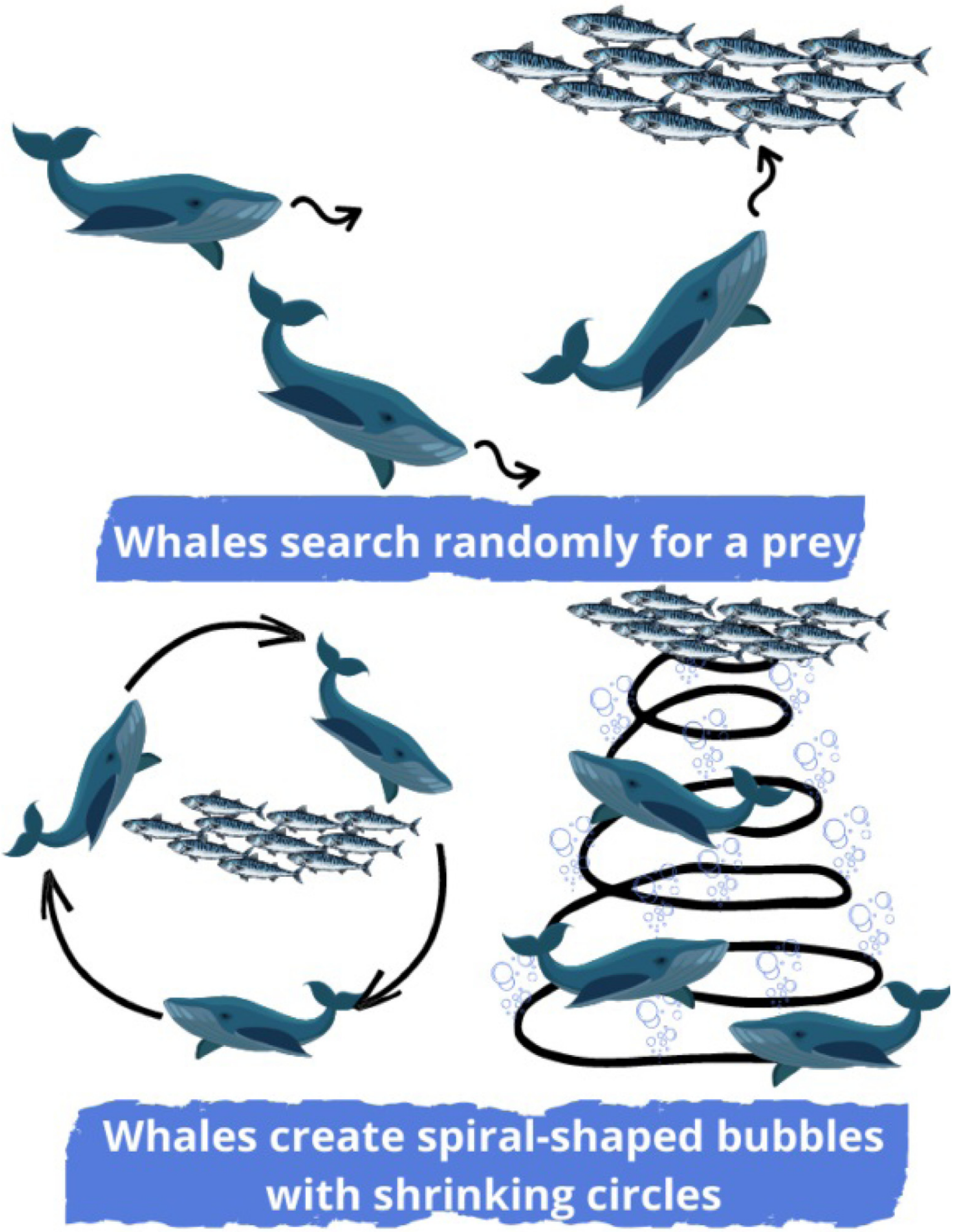

Whales search randomly for a prey
Whales create spiral-shaped bubbles with shrinking circles

**Fig. 3.** Whale optimization algorithm basic structure.

$$X_p = 2 * k \tag{9}$$

Where, $k$ denote the arbitrary value within the range of 0–2.

**Prey Searching:** In food searching process, the input “$V$” is denoted with “$V_{rand}$” which is estimated using the below Eqs. (10) and (11).

$$V = mod\{(O.V_{rand}) \; - \; V(q)\} \tag{10}$$

$$V(q+1) = [V_{rand}(q) \; - \{P.R\}] \tag{11}$$

The target was circled and a spiral upgrade was done during the search phase of the WOA approach. The mathematical expression for updating a new position is shown in Eq. (12).

$$V(q+1) \; = \; R^1 * ex^{s1} * \cos(2\pi p) + V(q) \tag{12}$$

“$s1$” stands for the constant “0–1”, and “$R$” stands for the distance between the starting location and the updated position after each iteration.

### 3.4. WOGRU -IDS-Its working mechanism

The weights of GRU networks are optimized using the straightforward whale techniques, as was covered in the preceding Section. In this instance, the primary phrase for optimizing the hyperparameters of GRU networks is the whale prey hunting process. Any training network’s hyperparameters include learning rates, hidden layers, input weights, hidden layers, and epochs. These hyperparameters are initially chosen at random and sent to the GRU training network. Equation provides the proposed network’s Fitness Function (FF) (9). Hyperparameters are computed for each iteration using Eqs. (11) and (12). When the FF matches the equation, iteration ends (9). The entire operating mechanism was displayed in Fig. 3 and algorithm 1.

$$FF = Max\,(Accuracy,\ Precision,\ Recall,\ \&\ F1 - Score) \tag{13}$$

**Algorithm 1** Pseudo Code for the Proposed WOGRU-IDS

```
Input = Hyperparameters of the GRU training network
Output = Categorization of the attacks
Begin
Randomly assigned hyperparameters
Random initialize whale population
while true do
    Calculate GRU output using equation(5)
    Calculate the FF using the equation(13)
    for t=1 to Max_iteration do
        Assign the bias weights and input layers by equation (11)and (12)
        Calculate the FF from the GRU network using equation(5)
        if (FF = = Maximum Accuracy) then
            Go to Step 16
        else
            Go to Step 10
        end if
    end for
    if (output measurement $\leq$ 1) then
        / Normal Data traces / /* No traces found
    else if (output measurement $\leq$ 2 && output measurement > 1) then
        / Detection of Blackhole attack
    else if (output measurement $\leq$ 3 && output measurement > 2) then
        Detection of Grayhole attack
    else if (output measurement $\leq$ 4 && output measurement > 3) then
        Detection of Scheduling attack
    else if (output measurement $\leq$ 4 && output measurement > 3) then
        Detection of flooding attack
        Go to step 1
    end if
end while
End
```

## 4. Experimentation and results

### 4.1. Simulation experiments

The proposed algorithm was implemented using opensource Tensorflow v1.18 with Keras API Environment, and performed on a computer configured with Intel Quad Core i5-10th generation CPU, 8 GB RAM, and 8 GB NVIDIA titan GPU enabled Windows10 Operation Systems.

### 4.2. Dataset descriptions

The proposed architecture was evaluated by the WSN-DS public datasets [34]. This is an intrusion detection dataset developed using LEACH (Low Energy Adaptive Clustering hierarchy) based Wireless Sensor Networks (WSN) in Network Simulator (NS-2) environment. WSN-DS contains four types of Denial Service attacks: blackhole, grayhole, flooding and scheduling. Below Table 3 depicts the complete statistical information of WSN-DS public datasets used for evaluating the performance of the proposed algorithm.

Above table depicts the statistical details of the training data used for the network. Nearly 2,62,177(70%) samples are used for training and 1,12,384 (30%) samples are used for testing. Nearly 22 attributes are present in the datasets and all parameters are used for the training and testing . the description of attacks are tabulated in Table 4.

**Table 3**
Number of traces utilized for testing and training the proposed network.

| Sl.no | Attack details | No of traces |
|---|---|---|
| 01 | Normal | 340006 |
| 02 | Black Hole attack | 14596 |
| 03 | Gray hole attack | 10049 |
| 04 | Scheduling attack | 3312 |
| 05 | Flooding attack | 6638 |
| | **Total Traces** | **374661** |

**Table 4**
Descriptions of Attacks in the Datasets.

| Sl.no | Attacks details | Description of attacks |
|---|---|---|
| 01 | Normal | Normal type records |
| 02 | Black Hole Attack | It is category of DoS attack which is injected during the initial phase of CH formation |
| 03 | Gray hole Attack | It is category of DoS attack which is injected during the CH announcements to other nodes |
| 04 | Scheduling Attack | It is DoS attack which occurs at the initial phase of routing |
| 05 | Flooding Attack | It is category of injecting users based attacks in routing |

**Table 5**
Formulae for the performance metrics' calculation.

| Sl.no | Performance metrics | Mathematical expression |
|---|---|---|
| 01 | Accuracy | $\frac{TP+TN}{TP+TN+FP+FN}$ |
| 02 | Sensitivity or recall | $\frac{TP}{TP+FN} * 100$ |
| 03 | Specificity | $\frac{TN}{TN+FP}$ |
| 04 | Precision | $\frac{TN}{TP+FP}$ |
| 05 | F1-Score | $2 * \frac{Precision\ *\ Recall}{Precision\ +\ Recall}$ |

### 4.3. Performance metrics and evaluation

To evaluate the proposed methodology on the datasets, performance metrics such as Accuracy, Precision, Recall, Specificity and F1-score were used. Table 5 presents mathematical expressions of the performance metrics. Accuracy is used to measure the performance of the proposed detection model. The parameters such as precision, recall, specificity and F1-score are used for identifying the attacks correctly and also rate of non-attacks and normal cases identified as attack data respectively.

TP — True Positive Values
TN — True Negative Values
FP — False Positive Values
FN — False Negative Values

### 4.4. Results and findings

We experimented the proposed framework in the following aspects : (1) Analyzing the performance of the proposed framework against four attacks, in order to meet the networks' safety criteria against attacks and integrate into the networks' intrusion detection system. (2) Using the state-of art ML and other existing learning classification models to compare with proposed architecture (3) Performing the time consumption experimentations to prove the proposed system's excellence.

Generally the Receiver Operating Curve (ROC) is utilized to measure the classifier performance by plotting the actual positive rate against the false positive rate. The ROC area gives the best performance of the classifier. If the ROC is very high then the classifier performance is also very high and vice versa. Figs. 4 to 8 shows the proposed model ROC characteristics in detecting the different attacks. From the Figs. 4 to 8, it is found that the maximum area covered by proposed model is 0.95 I and maximum accuracy is 99% in detecting the different category of

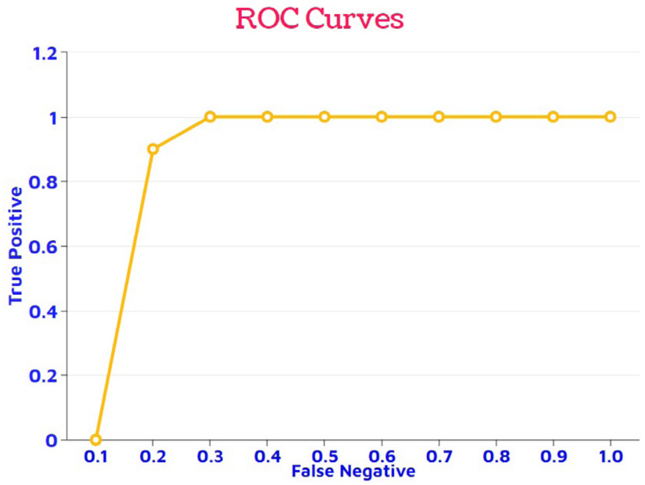


**Fig. 4.** ROC curves for the proposed architecture in blackhole attacks.

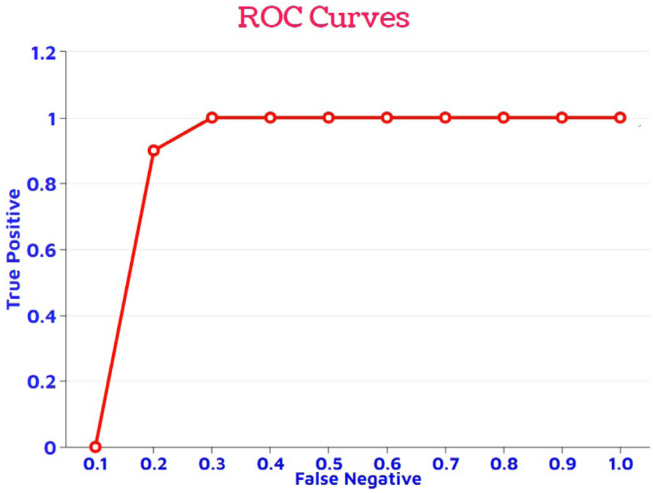


**Fig. 5.** ROC curves for the proposed architecture in grayhole attacks.

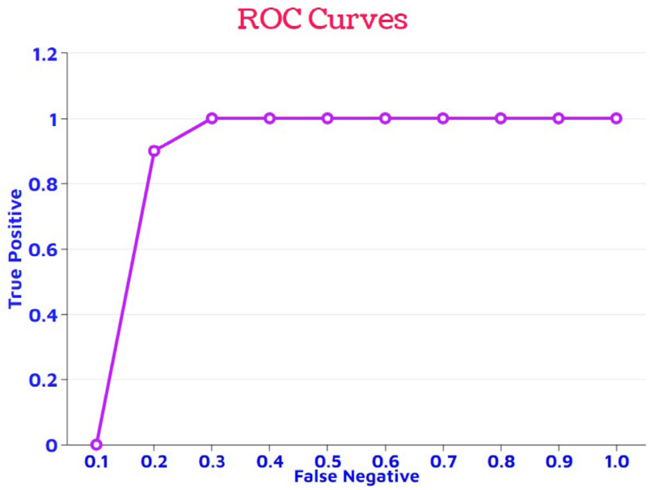


**Fig. 6.** ROC curves for the proposed architecture in flooding attacks.

attacks. Fig. 9 shows the proposed model confusion Matrix in detecting the multiple category of attacks.

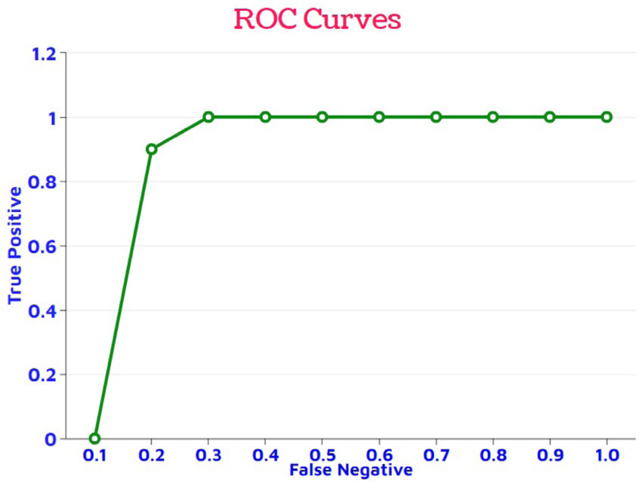


**Fig. 7.** ROC curves for the proposed architecture in scheduling attacks.

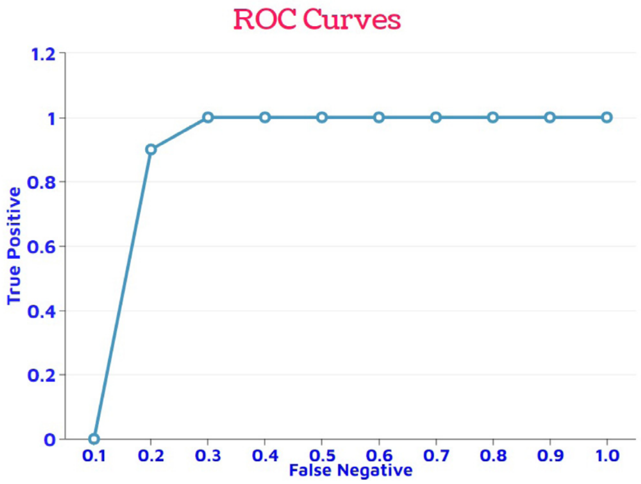


**Fig. 8.** ROC curves for the proposed architecture in normal attacks.

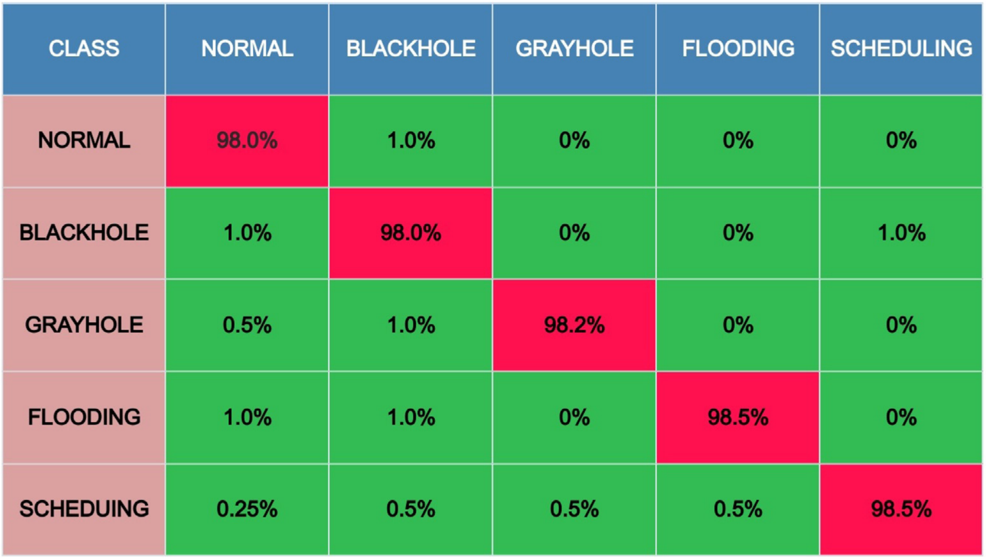
**Table 6**
Performance metrics of the proposed algorithm in different attacks.

| Type of attack | Performance metrics | | | | |
|---|---|---|---|---|---|
| | Accuracy (%) | Recall (%) | Specificity (%) | Precision (%) | F1-Score (%) |
| Black Hole | 99.8 | 99.85 | 99.84 | 99.87 | 99.88 |
| Gray hole | 99.79 | 99.82 | 99.82 | 99.86 | 99.86 |
| Flooding | 99.81 | 99.82 | 99.83 | 99.85 | 99.87 |
| Scheduling | 99.81 | 99.83 | 99.82 | 99.88 | 99.86 |
| Normal | 99.81 | 99.83 | 99.82 | 99.88 | 99.86 |

Table 6 gives the validation metrics by utilizing WSN-DS datasets. From the table it is clear that performance metrics such as "accuracy, precision, recall, specificity and F1-score" has exhibited the stable performance which ranges from 99% to 100% in detecting the different attack catagories. The inclusion of optimized hyperparameters in the DL model has produced the constant performance in detecting the attacks such as blackhole, Grayhole, flooding, scheduling and even the normal conditions

### 4.5. *Comparative analysis*

To prove the efficiency of the proposed model, we have compared with the other state of art learning models such as support vector



| CLASS | NORMAL | BLACKHOLE | GRAYHOLE | FLOODING | SCHEDULING |
|---|---|---|---|---|---|
| NORMAL | 98.0% | 1.0% | 0% | 0% | 0% |
| BLACKHOLE | 1.0% | 98.0% | 0% | 0% | 1.0% |
| GRAYHOLE | 0.5% | 1.0% | 98.2% | 0% | 0% |
| FLOODING | 1.0% | 1.0% | 0% | 98.5% | 0% |
| SCHEDUING | 0.25% | 0.5% | 0.5% | 0.5% | 98.5% |

**Fig. 9.** Confusion matrix for the proposed architecture for detection of different attacks.

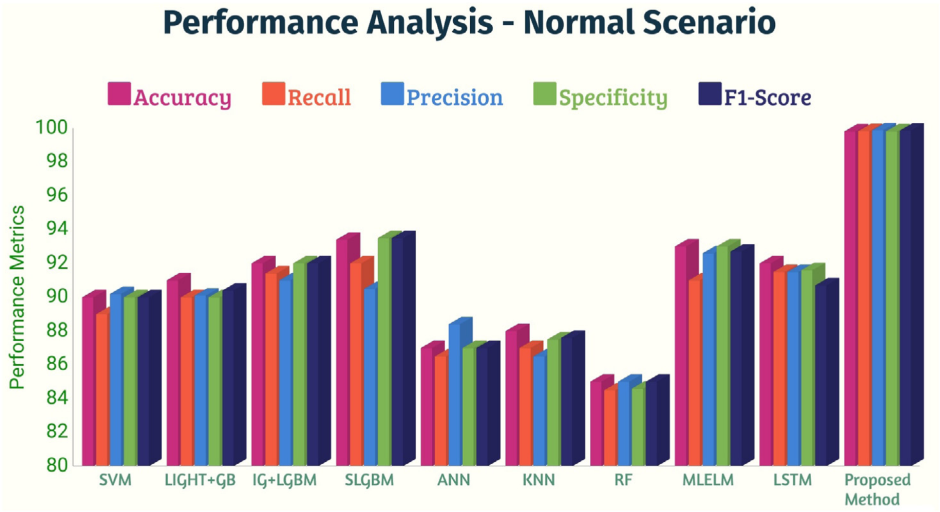


**Fig. 10.** Comparative analysis of performances of different learning models in detecting the normal scenario.

machine (SVM) [35], Artificial Neural Networks (ANN) [36], K-nearest Neighborhood (KNN) [37], Random Forest(RF) [38], Light+GB [39], IGLGBM [40], SLGBM [41], Multi -layer Extreme Learning Machines (MLELM) [28] and Long Short Term Memory (LSTM) [42].

Different hybrid learning models performances has been compared with WSN-DS datasets and analysis are shown from Figs. 10 to 14. In Fig. 10, various models performance has been compared for detecting the normal scenario. In this case, the proposed model has produced 99.81% accuracy,99.88% precision,99.83% recall and even high F1-score of 99.86%. In Fig. 11, various models performance has been compared for detecting the Blackhole attacks. In this case, the proposed model has produced 99.8% accuracy,99.87% precision,99.85% recall and even high F1-score of 99.88%. In Fig. 12, various models performance has been compared for detecting the Grayhole attacks. In this case, the proposed model has produced 99.79% accuracy,99.86% precision,99.82% recall and even high F1-score of 99.86%. In Fig. 13, various models performance has been compared for detecting the Scheduling attacks. In this case, the proposed model has produced 99.81% accuracy,99.88% precision,99.83% recall and even high F1-score of 99.86%. In Fig. 14, various models performance has been compared for detecting the Flooding attacks. In this case, the proposed model has produced 99.81% accuracy,99.85% precision,99.82% recall and even high F1-score of 99.87%. The LSTM and MLELM has produced the good detection performance but lesser than the proposed model. Moreover, the proposed model has produced the better detection than ANN, KNN, SVM, LIGHT+GB, IGLGBM and SLGBM respectively. This is because of integration of whale optimization over the GRU training network in the proposed framework. This improves the classification model for different attack detection. Further, the similar fashion of performances in found in Figs. 10, 11, 12 and 13 also.

The detection times of each learning model for the data presented in the section were calculated during the subsequent experimental phase. The findings shown in Fig. 15 show that the proposed model performs better than other existing models in handling larger datasets and producing a shorter detection time. Furthermore, the suggested model has resulted in high-speed detection and shows that the WOGRU model has demonstrated greater scalability than the other current methods in handling the bigger multi-class data.

It is found that the proposed framework has exhibited the superior performances than the other existing algorithms in detection of other attacks such as Grayhole, Blackhole, scheduling and flooding attacks.

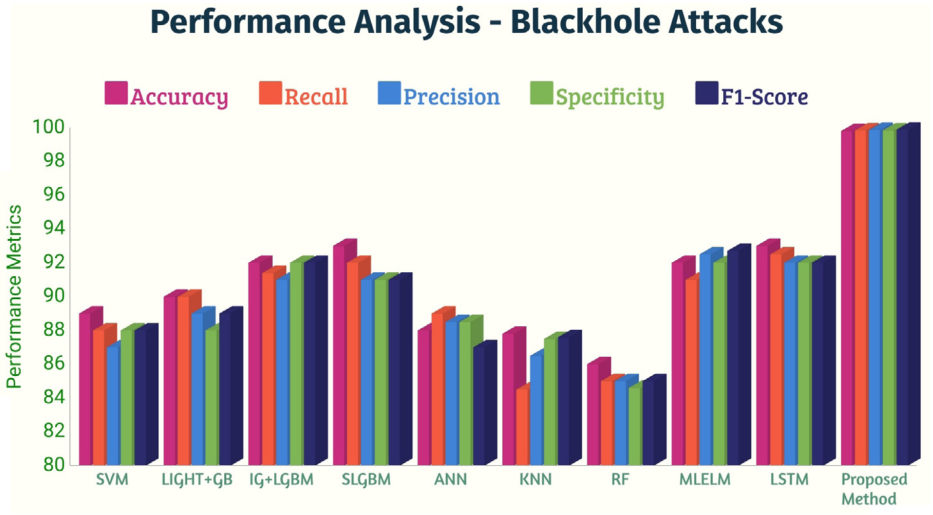


**Fig. 11.** Comparative analysis of performances of different learning models in detecting the blackhole attacks.

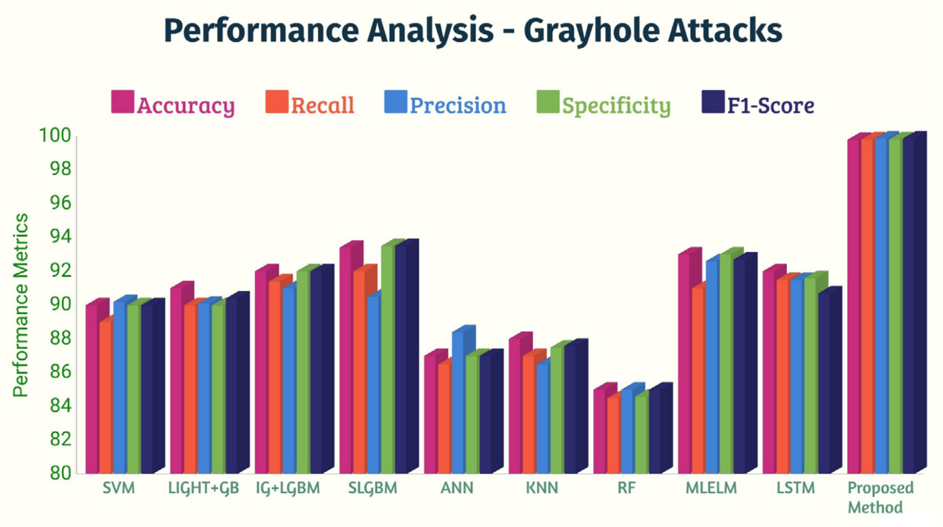


**Fig. 12.** Comparative analysis of performances of different learning models in detecting the grayhole attacks.

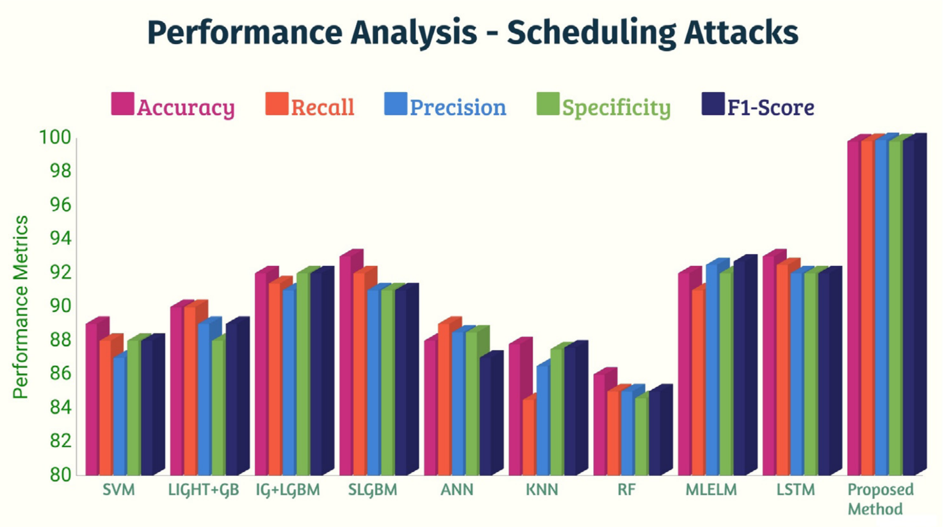


**Fig. 13.** Comparative analysis of performances of different learning models in detecting the scheduling attacks.

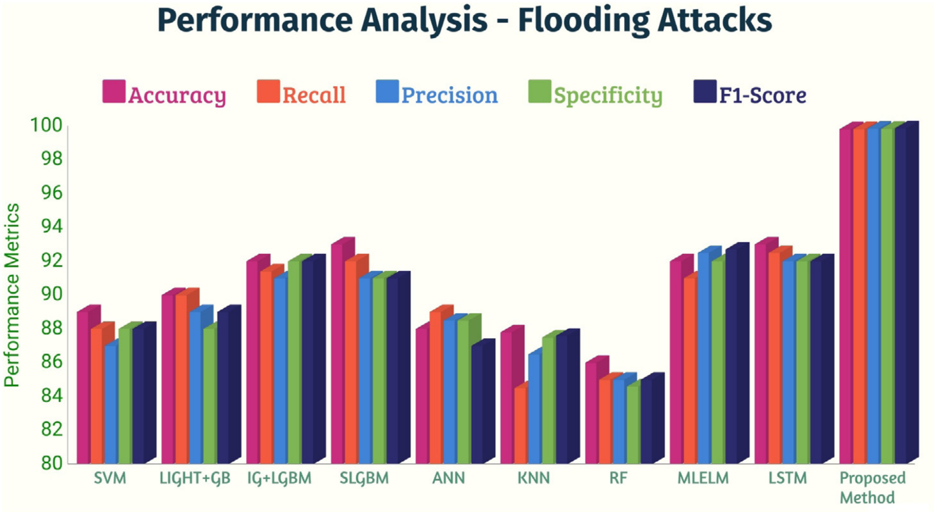


**Fig. 14.** Performance comparison of different learning models in detecting the flooding attacks.

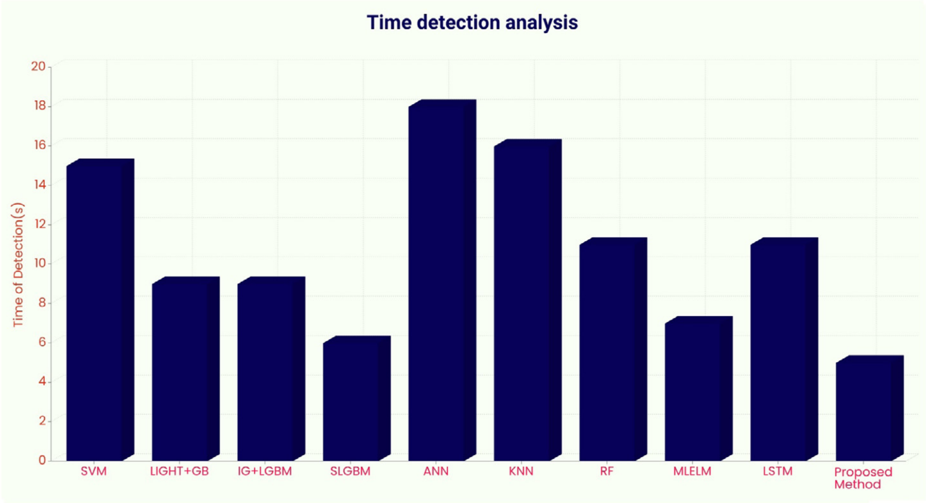


**Fig. 15.** Time detection analysis of different learning models in detecting the attacks.

## 5. Conclusion and future enhancement

Based on the whale optimization and principles of GRU training network, we architected the novel and intelligent intrusion detection model- WOGRU IDS targeted for the clustered WSN environments. The proposed models has been compared with the other existing learning frameworks. The extensive experimentation is carried out using WSN-DS intrusion datasets and compared with the other existing learning models. Simulation results shows that this proposed framework has shown the better performances than the other existing learning models in terms of classification and detection time. The proposed model provides the new dimension in intrusion detection system in WSN-IoT environment. Even though this model solved the multiple classification attacks with high classification rate countermeasure defensive measure with strong encryption scheme needs to be incorporated to defend against the attacks.

We intend to further minimize the detecting system's device-specific energy consumption in our upcoming research. As an alternative to regression, which only considers samples of actual sensor data, we also intend to investigate alternative techniques, such as state graphs, for assessing changes in sensor data trends.

## CRediT authorship contribution statement

**Kadiyala Ramana:** Conceptualization, Methodology, Writing – original draft, Software. **A. Revathi:** Data curation, Writing – original draft, Visualization. **A. Gayathri:** Data curation, Visualization, Investigation. **Rutvij H. Jhaveri:** Supervision, Writing – review & editing. **C.V. Lakshmi Narayana:** Formal analysis, Software, Validation. **B. Naveen Kumar:** Formal analysis, Software, Validation.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

Data will be made available on request.

## References

[1] Chun-Wei Tsai, Chin-Feng Lai, Athanasios V. Vasilakos, Future internet of things open issues and challenges, Wirel. Netw. 20 (8) (2014) 2201–2217.

[2] M.L. Oliveira Luís, Joel J.P.C. Rodrigues, Wireless sensor networks a survey on environmental monitoring, J. Commun. 6 (2) (2011) 143–151.
[3] Kalpna Guleria, Anil Kumar Verma, Comprehensive review for energy efficient hierarchical routing protocols on wireless sensor networks, Wirel. Netw. 25 (3) (2019) 1159–1183.
[4] Lingwei Xu, Xinpeng Zhou, Xingwang Li, Rutvij H. Jhaveri, Thippa Reddy Gadekallu, Yuan Ding, Mobile collaborative secrecy performance prediction for artificial IoT networks, IEEE Trans. Ind. Inf. (2021).
[5] Anna L. Buczak, Erhan Guven, A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Commun. Surv. Tutor. 18 (2) (2015) 1153–1176.
[6] R. Durga, E. Poovammal, Kadiyala Ramana, Rutvij H. Jhaveri, Saurabh Singh, Byungun Yoon, CES blocks—A novel chaotic encryption schemes-based blockchain system for an IoT environment, IEEE Access 10 (2022) 11354–11371.
[7] B. Ida Seraphim, E. Poovammal, Kadiyala Ramana, Natalia Kryvinska, N. Penchalaiah, A hybrid network intrusion detection using darwinian particle swarm optimization and stacked autoencoder hoeffding tree, Math. Biosci. Eng. 18 (6) (2021) 8024–8044.
[8] Md Jalil Piran, Sandeep Verma, Varun G. Menon, Doug Young Suh, Energy-efficient transmission range optimization model for wsn-based internet of things, Comput. Mater. Contin. 67 (3) (2021) 2989–3007.
[9] Tayyab Khan, Karan Singh, Mohd Hilmi Hasan, Khaleel Ahmad, G. Thippa Reddy, Senthilkumar Mohan, Ali Ahmadian, ETERS a comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs, Future Gener. Comput. Syst. 125 (2021) 921–943.
[10] Amna Mubashar, Kalsoom Asghar, Abdul Rehman Javed, Muhammad Rizwan, Gautam Srivastava, Thippa Reddy Gadekallu, Dong Wang, Maryam Shabbir, Storage and proximity management for centralized personal health records using an ipfs-based optimization algorithm, J. Circuits Syst. Comput. 31 (01) (2022) 2250010.
[11] Sudarshan Nandy, Mainak Adhikari, Mohammad Ayoub Khan, Varun G. Menon, Sandeep Verma, An intrusion detection mechanism for secured IoMT framework based on swarm-neural network, IEEE J. Biomed. Health Inf. 26 (5) (2021) 1969–1976.
[12] Daniel S. Berman, Anna L. Buczak, Jeffrey S. Chavis, Cherita L. Corbett, A survey of deep learning methods for cyber security, Information 10 (4) (2019) 122.
[13] Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, Parvez Faruki, Network intrusion detection for IoT security based on learning techniques, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2671–2701.
[14] Rohan Doshi, Noah Apthorpe, Nick Feamster, Machine learning ddos detection for consumer internet of things devices, in: 2018 IEEE Security and Privacy Workshops, SPW, IEEE, 2018, pp. 29–35.
[15] Vishalini Laguduva, Sheikh Ariful Islam, Sathyanarayanan Aakur, Srinivas Katkoori, Robert Karam, Machine learning based iot edge node security attack and countermeasures, in: 2019 IEEE Computer Society Annual Symposium on VLSI, ISVLSI, IEEE, 2019, pp. 670–675.
[16] Najdt Mustafa, Ashraf Osman Ibrahim, Ali Ahmed, Afnizanfaizal Abdullah, Collaborative filtering techniques and applications, in: 2017 International Conference on Communication, Control, Computing and Electronics Engineering, ICCCCEE, IEEE, 2017, pp. 1–6.
[17] Nishanth Reddy Pinnapareddy, Deep Learning Based Recommendation Systems, 2018.
[18] A.V. Singh Ruchika, Mayank Sharma, Building an effective recommender system using machine learning based framework, in: International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ictus), 2017.
[19] Eirini Anthi, Lowri Williams, Małgorzata Słowińska, George Theodorakopoulos, Pete Burnap, A supervised intrusion detection system for smart home IoT devices, IEEE Internet Things J. 6 (5) (2019) 9042–9053.
[20] E. Baraneetharan, Role of machine learning algorithms intrusion detection in WSNs a survey, J. Inf. Technol. 2 (03) (2020) 161–173.
[21] Kathleen Goeschel, Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis, in: SoutheastCon 2016, IEEE, 2016, pp. 1–6.
[22] Lixiang Li, Hao Zhang, Haipeng Peng, Yixian Yang, Nearest neighbors based density peaks approach to intrusion detection, Chaos Solitons Fractals 110 (2018) 33–40.
[23] Nour Moustafa, Benjamin Turnbull, Kim-Kwang Raymond Choo, An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things, IEEE Internet Things J. 6 (3) (2018) 4815–4830.
[24] Samir Ifzarne, Hiba Tabbaa, Imad Hafidi, Nidal Lamghari, Anomaly detection using machine learning techniques in wireless sensor networks, in: Journal of Physics Conference Series, Vol. 1743, (1) IOP Publishing, 2021, 012021.
[25] Yufei Liu, Dechang Pi, A novel kernel SVM algorithm with game theory for network intrusion detection, KSII Trans. Internet Inf. Syst. (TIIS) 11 (8) (2017) 4043–4060.
[26] Yaping Chang, Wei Li, Zhongming Yang, Network intrusion detection based on random forest and support vector machine, in: 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing, EUC, Vol. 1, IEEE, 2017, pp. 635–638.
[27] Sarunya Kanjanawattana, A novel outlier detection applied to an adaptive k-means, Int. J. Mach. Learn. Comput. 9 (5) (2019) 569–574.
[28] Wenjie Zhang, Dezhi Han, Kuan-Ching Li, Francisco Isidro Massetto, Wireless sensor network intrusion detection system based on MK-ELM, Soft Comput. 24 (16) (2020) 12361–12374.
[29] Ismail Butun, Salvatore D. Morgera, Ravi Sankar, A survey of intrusion detection systems in wireless sensor networks, IEEE Commun. Surv. Tutor. 16 (1) (2013) 266–282.
[30] Koffka Khan, Ashok Sahai, A comparison of BA, GA, PSO, BP and LM for training feed forward neural networks in e-learning context, Int. J. Intell. Syst. Appl. 4 (7) (2012) 23.
[31] B. Sowmiya, E. Poovammal, Kadiyala Ramana, Saurabh Singh, Byungun Yoon, Linear elliptical curve digital signature (LECDS) with blockchain approach for enhanced security on cloud server, IEEE Access 9 (2021) 138245-138253.
[32] Zhiwei Guo, Lianggui Tang, Tan Guo, Keping Yu, Mamoun Alazab, Andrii Shalaginov, Deep graph neural network-based spammer detection under the perspective of heterogeneous cyberspace, Future Gener. Comput. Syst. 117 (2021) 205–218.
[33] Nidhi Lakhera, A.R. Verma, Surjeet Singh Patel, Bhumika Gupta, A novel approach of ECG signal enhancement using adaptive filter based on whale optimization algorithm, Biomed. Pharmacol. J. 14 (4) (2021) 1895–1903.
[34] Gautam M. Borkar, Leena H. Patil, Dilip Dalgade, Ankush Hutke, A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN a data mining concept, Sustain. Comput. Inform. Syst. 23 (2019) 120–135.
[35] Ravi Vinayakumar, Mamoun Alazab, K.P. Soman, Prabaharan Poornachandran, Ameer Al-Nemrat, Sitalakshmi Venkatraman, Deep learning approach for intelligent intrusion detection system, IEEE Access 7 (2019) 41525–41550.
[36] Chien-Chung Su, Ko-Ming Chang, Yau-Hwang Kuo, Mong-Fong Horng, The new intrusion prevention and detection approaches for clustering-based sensor networks [wireless sensor networks], in: IEEE Wireless Communications and Networking Conference, Vol. 4, IEEE, 2005, pp. 1927–1932.
[37] Feng Ding, Guopu Zhu, Mamoun Alazab, Xiangjun Li, Keping Yu, Deep-learning-empowered digital forensics for edge consumer electronics in 5G HetNets, IEEE Consumer Electron. Mag. (2020).
[38] Yassine Maleh, Abdellah Ezzati, Youssef Qasmaoui, Mohamed Mbida, A global hybrid intrusion detection system for wireless sensor networks, Procedia Comput. Sci. 52 (2015) 1047–1052.
[39] T.P. Rani, C. Jayakumar, Unique identity and localization based replica node detection in hierarchical wireless sensor networks, Comput. Electr. Eng. 64 (2017) 148–162.
[40] Jian Su, Zhengguo Sheng, Alex X. Liu, Yu Han, Yongrui Chen, A group-based binary splitting algorithm for UHF RFID anti-collision systems, IEEE Trans. Commun. 68 (2) (2019) 998–1012.
[41] Shuai Jiang, Juan Zhao, Xiaolong Xu, SLGBM an intrusion detection mechanism for wireless sensor networks in smart environments, IEEE Access 8 (2020) 169548-169558.
[42] Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, Qi Shi, A deep learning approach to network intrusion detection, IEEE Trans. Emerg. Top. Comput. Intell. 2 (1) (2018) 41–50.