https://doi.org/ 10.33472/AFJBS.6.Si2.2024.211-225

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

ENHANCING WIRELESS SENSOR NETWORK SECURITY: SEQUENTIAL PATTERN ANALYSIS WITH BIOMETRIC AUTHENTICATION FOR PREDICTING ATTACKER TRANSACTIONS

Dr.K. Anuradha [1] , Dr. S. Nirmala Sugirtha Rajini [2]

1.Assistant Professor,
anu.navine@gmail.com
2.Professor,
sugirtharaja77@yahoo.com
Department of Computer Applications, Dr.MGR Educational and ResearchInstitute,
Maduravoyal, Chennai-95, India.

Article History

Volume 6,Issue Si2, 2024

Received:25 Feb 2024

Accepted : 30 Mar 2024

doi: 10.33472/AFJBS.6.Si2.2024.211-225

ABSTRACT

Nowadays, Wireless Sensor Networks (WSN) have created tremendous prominence because of their evident benefits compared to the conventional cable network, whichis simple in distribution, users' mobility over the area of network coverage and ease in new user connection. WSN security can be supported through the strategies of attack and defence using Machine Learning (ML). The ML technique assist in detecting the intruder based on their behavior but predicting accuracy of intruder is less because of exact behavior analysis of ML model. The dataset consists of 3,74,661 transmission of network and security attacks are classified as cyber ones, and these attacks are engaging in the system tentatively and spoil the data instead of stealing the data. Hence, this paper focuses on the Intrusion Detection System (IDS), which is done through a Stacked Autoencoder (SAE) with a sequential pattern of the Artificial Neural Network (ANN) method with biometric authentication that has generated better security from the DoS attack with accuracy 96.96%. Thus, the security methods in WSN majorly concentrateon finding intruders, eliminating malicious nodes, and securing transmission data. The integration of Artificial Neural Network (ANN) methods with biometric authentication offers a promising solution to enhance WSN security.

Keywords: Wireless Sensor Network, Denial of Service (DoS), Stacked Autoencoder, Intrusion Detection System, Artificial Neural Network, sequential

I INTRODUCTION

WSN has drawn more attention in recent years. They are extensively utilized in numerous applications, including observation of natural phenomena, underwater sensor networks and border surveillance. A WSN is a group of tiny sensor nodes that gather and send environmental data to a collecting node [1]. The nodes, also known as specks, are electronic components that include a sensor, radio interface, sensors, a processor, an analog-to-digital converter and a power source [2]. These tiny sensors are placed across a region to carry out their specified functions [3] effectively. The crucial properties of WSN are energy, great scalability, memory and power [4]. Real-time applications, monitoring of natural occurrences, military settings and healthcare facilities could all benefit from using these factors. These data must always be accessible, regardless of location or time. WSNs are highly susceptible and defenceless against internal and external attacks since node communications are created via wireless connections, which enable data to be altered and intercepted, disclosing critical data to the use of third parties who are not authorized.Important data of government, the military, business, and healthcare may be lost due to security lapses and attacks on WSNs [5]. Cybersecurity is a set of tools and procedures designed to protect against breaches and unauthorizedaccess, alterations, or loss of computer data, networks, programs, and other digital assets [6]. Misuse-based detection techniques aim to locate recognized hazards by their signatures [7].

On the other hand, malicious threats are constantly developing and proliferating, demanding an advanced network security system. Due to the extensive Internet usage, more computers are connected through networks. Efficient IDSs that distinguish between legal and stolen communications have been built using data science methodologies in recent years. IDSs are frequently used in communications networks to monitor and find malicious activity.IDSs can be differentiated into three groups: anomaly-based systems, hybrid systems and systems that utilize signatures to detect intrusions. While signature-based may identify known attacks with associated gathered signatures, it has a high false alarm rate [8].Anomaly-based can discover unknown hazardous acts by recognizing model deviation created based on typical behaviour. The accuracy presently used in anomaly intrusion detection techniques is lacking. Some datasets struggle to provide variation and volume of network traffic, while others lack information on a set of feature metadata [9]..

The notion behind detecting intrusions in a system is identifying an attempt to infiltrate and affect elements like accessibility, integrity, privacy, or the system's level of services. An essential part of Network Intrusion Detection Systems (NIDS) is addressing and solving security issues. NIDS keeps an eye on network traffic to look for any unusual activities. It also analyses data from network traffic to look for security breaches such as anomalies, invasions and abuse. A network with an NIDS installed may analyze traffic flows to find security concerns and

safeguard digital records.NIDS should address massive traffic and high dimensionality problems [10].

ML techniques are usually helpful in collecting substantial amounts of data and creating valuable insight [11]. NIDS can benefit from ML techniques, although these methods have limits when dealing with a lot of network data.Feature selection (FS) is a technique for reducing unwanted and repetitive features and selecting the most appropriate feature subset to improve the classification of attack pattern types. As a result, preprocessing, classifier algorithms and feature reduction are three essential factors in creating NIDS. The difficulties of NIDS include managing massive amounts of data, many false alerts, and data mismatches. These issues can be resolved by using different sequential patterns. As a result, the sequential pattern with ANN approach is the main emphasis of this study to improve accuracy and apply an efficient optimizer for predicting assaults of high accuracy using the IDS idea with ANN.

This paper proposes a novel approach that combines sequential pattern analysis using ANN with biometric authentication to predict and prevent attacker transactions in WSNs. The approach used to solve this challenge is explained in Section 2, which introduces associated literature for IDS models.Session 3 discusses the feature extraction method as SAE for encoding and decoding the transaction data with the ANN method by sequence pattern. Section 4 discusses the performance of the proposed SAE with the ANN sequence pattern with biometric authentication, which is evaluated with the existing ML model. Session 5 concluded that SAE with sequence pattern of ANN has high accuracy in detecting intruders as IDS.

II LITERATURE REVIEW

Cyber security is a critical aspect of the WSN for safely storing and transmitting data over the Internet. Numerous researchers have researched the WSN in terms of producing safe data and having the potential to identify and isolate cyberattacks ineffectually, notably in WSN. Accurately identifying the cyberattack is made possible by this literature's mastery of numerous ML techniques. These security risks are provided here, along with information on how ML techniques can help us conduct these assaults [12]. Anomaly detection is examined in IoT systems intrusion detection[13].The kNearestNeighbors (KNN) distances are thoroughly analyzed after fast and reliable anomaly detection using a Cumulative Sum Control (CUSUM)chart.The ML is currently utilized to accurately and quickly determine if a drone is in the air or on the ground [14]. To use NN classifiers and random forests, the attributes that dependon the communications packet size and inter-arrival time between the drone and its Remote Controller (RC) are fed into such systems.

One of the most well-known applications of AI is ML, in which algorithms create mathematical models from sample data for making predictions or judgments without being specifically trained in it [15]. Since they focus on connected hosts and connections like switches, IDSs are frequently installed afterthesecured network equipment [16]. Additionally, specific programs require an integration of data sets to operate correctly. The ML method doesn't need human involvement,

which is consistent with the nature of WSNs and has surprising patterns and behaviours [17]. The resources and computing capabilities of nodes and the requirement for sizable data sets for learning are the two critical obstacles to ML in WSNs. The challenging task of applying ML algorithms to maintain the confidentiality and integrity of security requirements is one of the most significant issues ML algorithms faceconcerning the security of WSN networks. Thereby, ML methods can improve wireless network security, decrease congestion issues, and assist with error detection and physical layer authentication processes [18].

Authors in [19] proposed a new model to improve DoS detection and lower power consumption in WSNs. ANN has no input restrictions, making it superior to other classification algorithms for categorizing complex and non-linear data sets [21]. Statistical analysis is provided as a possible way to detect online DoS.The authors employed binary logistic regression in the black-hole attacks and forward-selective. Logistic regression was utilized after a run-time monitoring tool had gathered the local WSN node performance and determined if the packets were malicious or benign. Their prediction was 96 to 100 percent accurate [22]. The authors have developed a flexible intrusion detection method utilizing a Deep Neural Network (DNN). The results accuracy for various forms of network traffic was also improved [23]. The authors also used Particle Swarm Optimization (PSO) and Backpropagation Neural Network (BNN) to develop a simple intrusion detection system for WSN networks [24]. The attack site visitors and non-attack traffic styles are analyzed after simulation depending upon unique parameters[25] .The author describes the Machine learning and Deep learning technology are used to avoid security issues in IOT Devices[26]

III RESEARCH METHODOLOGY

The major goal of SAE is initiating its parameter in the training data and associated with backpropagation functions. Once the SAE is done through AE, which performs as the pre-training model, assist ANN with a sequential pattern for generating a fine-tuned ANN model to detect attacktype.The sequence pattern helps identify the pre-trained model through the SAE algorithm and precisely see the attack type. The WSN-DS dataset is collected from open source Kagglein which CSV file shown with few transactions is illustrated in figure 1.

id	Time	Is_CH	who CH	Dist_To_CH	ADV_S	ADV_R	JOIN_S	JOIN_R	SCH_S	SCH_R	Rank	DATA_S	DATA_R	Data_Sent_To_BS	dist_CH_To_BS	send_code	Expaned Energy	Attack type
101000	50	1	101000	0	1	0	0	25	1	0	0	0	1200	48	130.08535	0	2.4694	Normal
101001	50	0	101044	75.32345	0	4	1	0	0	1	2	38	0	0	0	4	0.06957	Normal
101002	50	0	101010	46.95453	0	4	1	0	0	1	19	41	0	0	0	3	0.06898	Normal
101003	50	0	101044	64.85231	0	4	1	0	0	1	16	38	0	0	0	4	0.06673	Normal
101004	50	0	101010	4.83341	0	4	1	0	0	1	25	41	0	0	0	3	0.06534	Normal
101005	50	0	101010	31.91198	0	4	1	0	0	1	18	41	0	0	0	3	0.06717	Normal
101006	50	0	101044	24.34167	0	4	1	0	0	1	5	38	0	0	0	4	0.06214	Normal
101007	50	0	101010	26.75033	0	4	1	0	0	1	21	41	0	0	0	3	0.06662	Normal
101008	50	0	101044	63.66485	0	4	1	0	0	1	17	38	0	0	0	4	0.06649	Normal
101009	50	0	101000	32.90217	0	4	1	0	0	1	12	48	0	0	0	1	0.07903	Normal
101010	50	1	101010	0	1	0	0	30	1	0	0	0	1230	41	108.77162	0	2.3611	Normal
101011	50	0	101044	13.17446	0	4	1	0	0	1	10	38	0	0	0	4	0.0613	Normal
101012	50	0	101044	48.16567	0	4	1	0	0	1	13	38	0	0	0	4	0.06425	Normal
101013	50	0	101010	66.9102	0	4	1	0	0	1	16	41	0	0	0	3	0.07263	Normal
101014	50	0	101010	31.69105	0	4	1	0	0	1	17	41	0	0	0	3	0.06716	Normal
101015	50	0	101010	21.52629	0	4	1	0	0	1	8	41	0	0	0	3	0.06654	Normal
101016	50	0	101010	74.73928	0	4	1	0	0	1	4	41	0	0	0	3	0.0749	Normal
101017	50	0	101044	27.78157	0	4	1	0	0	1	29	38	0	0	0	4	0.06139	Normal
101018	50	0	101010	25.5197	0	4	1	0	0	1	26	41	0	0	0	3	0.06618	Normal
101019	50	0	101044	41.21473	0	4	1	0	0	1	28	38	0	0	0	4	0.0628	Normal
101020	50	0	101044	22.54714	0	4	1	0	0	1	15	38	0	0	0	4	0.06147	Normal
101021	50	0	101000	30.32029	0	4	1	0	0	1	4	48	0	0	0	1	0.07905	Normal
101022	50	0	101010	33.68188	0	4	1	0	0	1	14	41	0	0	0	3	0.06743	Normal

Figure 1 WSN Dataset From Kaggle Source As An Input File

During data preprocessing, normalization is done todefine better the feature's information for accomplishing target as attack_type" in the binary format as "Normal" as 1 and "Intruder" as 0 is determined through labelEncoder(). The preprocessing assist in converting all independent variable into integer or float data types to maintain continuous variables and the ID number variable is dropped. The architecture of SAE with ANN sequence pattern model is explained in Figure 2.

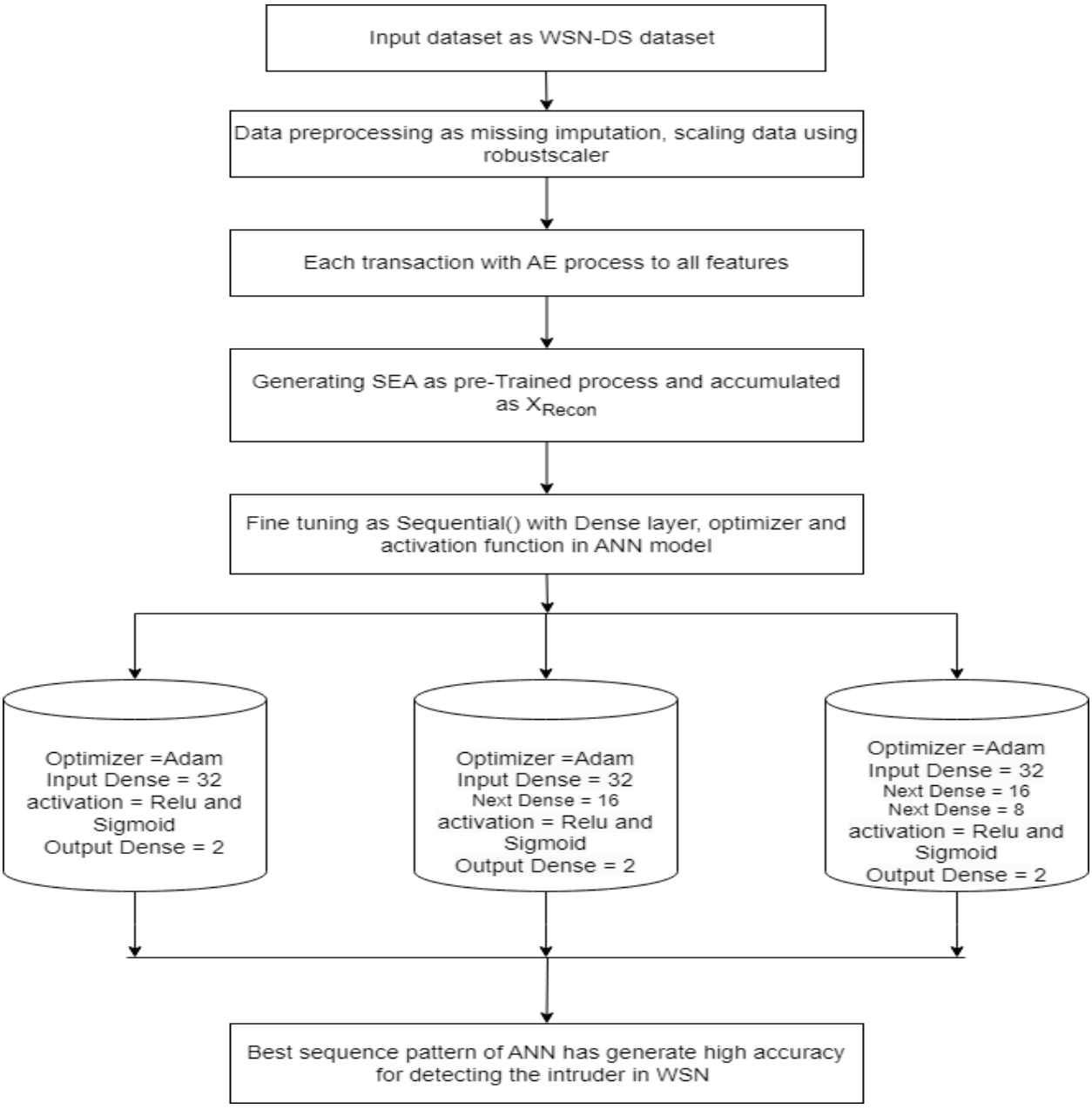

Figure 2 SAE with ANN sequence pattern architecture for IDS

The SAE algorithm has played an essential role in securing data transmission through encoder and decoder concept using hash key and reconstruction of encrypted code into input data, which act as a pre-trained network layer process shown in Figure 2.

Working of Stacked Autoencoder

One unsupervised Neural Network (NN) is Autoencoder (AE),which helps to learn to reduce the difference between input and output data. Encoders and decoders are the two types of AE. The original data gets mapped with encoder code, which deals with code dimensions less than the original data. In the decoder case, the code has tried to map an original input. The dimensionality reduction is an AE application that considers input as/; the AE goal is represented as y = z, expressed in equation 1 for learning AE function.

$$F_{w.ib}(x) \approx y \tag{1}$$

Where,

W = Weight of the entire neural network

ib = Image bias

The primary reconstruction loss in AE loss function for L_p distance in which Stochastic Gradient Descent (SGD) has been utilized to fine-tune the weight and bias in AE module shown in equation 2.

$$L(w,ib) = \min \left\| x - F_{w,ib}(x) \right\|_P \tag{2}$$

However, better results are obtained through a Stacked Autoencoder (SAE) that involves various AE in which the output of each AE is assigned to the input of the succeeded AE. The steps given below are essential steps for SAE training.

Step 1 - Encoder transformation

The SAE with M number of AE is represented as m^{th} AE's encoder and decoder functions transformation.In SEA, the encoder transformation function has been examined using function of encoder transformation for each AE in forward order gets, illustrated in equation 3.

$$x_{encoded} = x^m = \alpha^m, \alpha^{m-1}, \ldots, \alpha^2, \alpha^1(x) \tag{3}$$

Step 2 - Decoder transformation

In the case of SAE, the decoder transformation function has been evaluated by function of decoder transformation for each AE in reverse order, illustrated in equation 4.

$$x_{Decoded} = x_{reconstrct} = \alpha^{1}, \alpha^{2}, \ldots, \alpha^{2}, \alpha^{1}\left(x^{w}\right) \tag{4}$$

When one layer is trained, the other layer's parameters get fixed, whereas the output of the preceding layer has been utilized as an input for the subsequent layer. Thus, it will continue till the training is completed. The backpropagation algorithm has been used to reduce the reconstruction error once all the layers are trained and the weights are modified. To accomplish high-level features, SAE code is essential for encoding the statistical features. Hence, this research concentrated on SAE code for performing statistical features from network traffic.

Figure 3 explains the heat map based on correlation on the 16 available variablesintheWSN-DS dataset that have been analyzed to understand the significance of the attributes present.

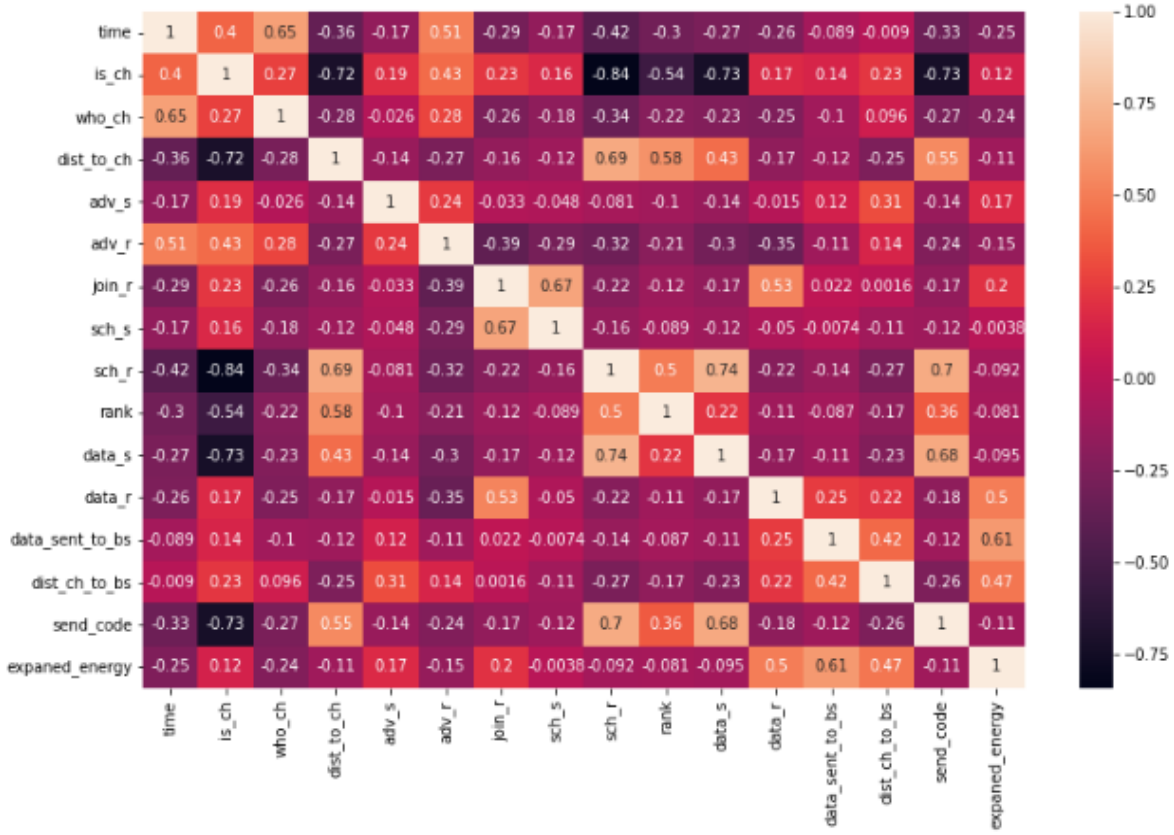

Figure 3 WSN-DS dataset correlation on their 16 variables

ANN model working principle

To acquire ANN model with sequence patterns and made by accomplishing an apparent with accurate prediction.TheX dataset pairs contain variables that are assumed as well as the outcome (m^1, t^1), (m^2, t^2), (m^3, t^3), ….(m^X, t^X). The NN structure is generally created using the basic formula mentioned in Equation 5.

$$F\left(m^{i}\right)=t^{i} \tag{5}$$

Where,

m^i= Input value for i= 1, 2, 3, …, X.

t^i= Target value

Moreover, it allows for error $\in^i$typically, n indicates the ANN output expressed in equations6 and 7.

$$n^{i}=F\left(m^{i}\right) \tag{6}$$

and

$$t^{i}=n^{i}+\in^{i} \tag{7}$$

Then^ihas indicated weight and bias associated with parameters generated as an optimizer influence. The setup of ANN in F has reduced the error function illustrated in Equation 8.

$$E=\frac{1}{N}\sum_{i=1}^{X}\left\|t^{i}-n^{i}\right\|^{2} \tag{8}$$

Where,

N = Training patterns numbers

The N=2 has represented that ANN model is a two-way classification method

E = Parameter function for F

It is essential to determine the weight values which minimize the error by differentiating E.This research has discussed one term of the sum illustrated in equation 9.

$$\left\|t-n\right\|^{2}=\left(t_1-n_1\right)^{2}+\left(t_2-n_2\right)^{2}+\ldots+\left(t_x-t_x\right)^{2} \tag{9}$$

The input and output value is fixed, but only the parameter is estimated by weights and differentiated from both sides, as illustrated in equation 10.

$$\frac{\partial}{\partial w_{ij}} = \left(\left\| t - n \right\|^2 \right) = -2(t-n).\frac{\partial n}{\partial w} \quad (10)$$

ANN is more precise and even checks the fitness in the NN context and the output is defined as$n^i = W_{ij}m^i + b.$

Thus, the output entirely relies upon weights, but the differentiation on both sides is based on$W_{ij}$by chain rule is shown in equation 11.

$$\frac{\partial}{\partial w_{ij}} = \left(\left\| t - n \right\|^2 \right) = 2(t_i - n_i)m_i \quad (11)$$

Where,

$m_j$is the ith coordinate position. The derivative provided direction in the reverse direction of this gradient after giving the maximum guidance for achieving the least point. Additionally, this derivative should be as near to 0 as feasible to ensure the least error rate.Thus, the ANN method is a layer-based network involving one or more artificial neurons, which usually influences the input, hidden, and output layers.

The significant advantage of the input activation function Reluis that it doesn't stimulate all neurons simultaneously in which a neuron influences negative value is converted into zero anddeactivated.This makes the network with required neurons computationally effective in an outcome. In the case of backpropagation, the graph for gradient value at the negative side is said to be zero, determining that neuron elimination. The sigmoid function has assisted in maintaining the multi-class criteriathatmap the output value from 0 to 1 and is executed with better performance in the output layer of a classifier.Moreover, it doesn't have any guidelines for selectingthe activation function. The issue property may assist in the selection of a quickconverging network. There are specific properties under research, such as the Relu and sigmoid as an activation function.

IV RESULTS AND DISCUSSION

Figure 4 illustrates the sequence pattern epochs with loss function as binary cross entropy in which optimal results are obtained in the SAE-ANN sequence model 2 shows better accuracy compared to another sequence pattern of SAE-ANN model. Thus, the trained sequence pattern results in classifying the IDS performance of SAE with sequence pattern of ANN in WSN can be evaluated through confusion matrix metrics.

```
model_3 = Sequential()
model_3.add(Dense(32, input_dim=in_dim, activation='relu'))
model_3.add(Dense(16, activation='relu'))
model_3.add(Dense(5, activation='sigmoid'))
# Model Compilation
model_3.compile(loss='binary_crossentropy', optimizer='adam', metrics=['accuracy'])
```

```
model_3.fit(X_train, y_train, validation_data=(X_test, y_test), batch_size=5, epochs=10)

Epoch 1/10
7168/7168 [==============================] - 34s 5ms/step - loss: 0.2604 - accuracy: 0.7285 - val_loss: 0.1748 - val_accuracy: 0.7643
Epoch 2/10
7168/7168 [==============================] - 38s 5ms/step - loss: 0.1657 - accuracy: 0.7945 - val_loss: 0.1540 - val_accuracy: 0.8362
Epoch 3/10
7168/7168 [==============================] - 33s 5ms/step - loss: 0.1284 - accuracy: 0.8682 - val_loss: 0.1117 - val_accuracy: 0.8809
Epoch 4/10
7168/7168 [==============================] - 38s 5ms/step - loss: 0.1055 - accuracy: 0.8879 - val_loss: 0.0993 - val_accuracy: 0.8921
Epoch 5/10
7168/7168 [==============================] - 39s 5ms/step - loss: 0.0901 - accuracy: 0.9173 - val_loss: 0.0798 - val_accuracy: 0.9381
Epoch 6/10
7168/7168 [==============================] - 34s 5ms/step - loss: 0.0695 - accuracy: 0.9511 - val_loss: 0.0597 - val_accuracy: 0.9575
Epoch 7/10
7168/7168 [==============================] - 30s 4ms/step - loss: 0.0536 - accuracy: 0.9649 - val_loss: 0.0558 - val_accuracy: 0.9628
Epoch 8/10
7168/7168 [==============================] - 21s 3ms/step - loss: 0.0482 - accuracy: 0.9664 - val_loss: 0.0473 - val_accuracy: 0.9699
Epoch 9/10
7168/7168 [==============================] - 22s 3ms/step - loss: 0.0453 - accuracy: 0.9685 - val_loss: 0.0476 - val_accuracy: 0.9702
Epoch 10/10
7168/7168 [==============================] - 21s 3ms/step - loss: 0.0473 - accuracy: 0.9688 - val_loss: 0.0443 - val_accuracy: 0.9696
<keras.callbacks.History at 0x195819d3f70>
```

Figure 4 Epochs for SAE-ANN sequence model 2

Table 1 Confusion matrix for various SAE-ANN model

Classification of SAE-ANN model	**Confusion matrix class values for IDS in WSN-DS test sample**			
	True Positive (TP)	**True Negative (TN)**	**False Positive (FP)**	**False Negative (FN)**
SAE-ANN sequence model 1	56348	46983	5556	3476
SAE-ANN sequence model 2	59135	49867	2073	1324
SAE-ANN sequence model 3	57388	47915	4620	2476

Table 1 illustrates the 30% test sample from the WSN-DS dataset in which the overall test sample is 1,12,399 transaction records involved. The TP represent the normal in attack type, TN represents the intruder in attack type, FP representsthe wrongly predicted normal type from actual by the respective model, and FN representsthe wrongly predicted intruder type from actual by the respective model. This research involves three different sequence patterns of SAE-ANN model. Table 2 illustrate the confusion matrix for various SAE-ANN model.

Table 2 Confusion matrix metrics for various SAE-ANN model

Classification of SAE-ANN model	Confusion matrix class values for IDS in WSN-DS test sample					
	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Sensitivity	Specificity
SAE-ANN sequence model 1	91.96	91.03	94.19	92.58	0.942	0.894
SAE-ANN sequence model 2	96.96	96.61	97.81	97.20	0.978	0.960
SAE-ANN sequence model 3	93.69	92.55	95.86	94.18	0.959	0.912

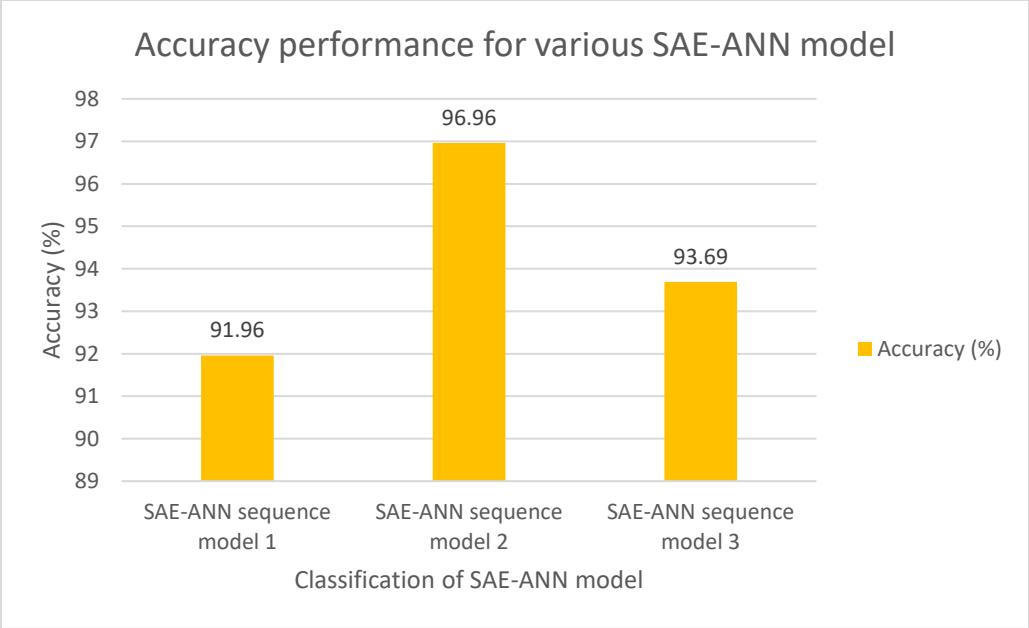

Figure 5 Micro and weighted value for various ANN models

Figure 5 illustrates the accuracy of three different SAE-ANN sequence models with Adam optimizer. The accuracy of SAE-ANN sequence model 2 is 96.96%, which is comparatively higher than other SAE-ANN sequential models. The proposed sequential pattern of SAE-ANNhasa better prediction in classifying IDS from the transaction node in WSN.

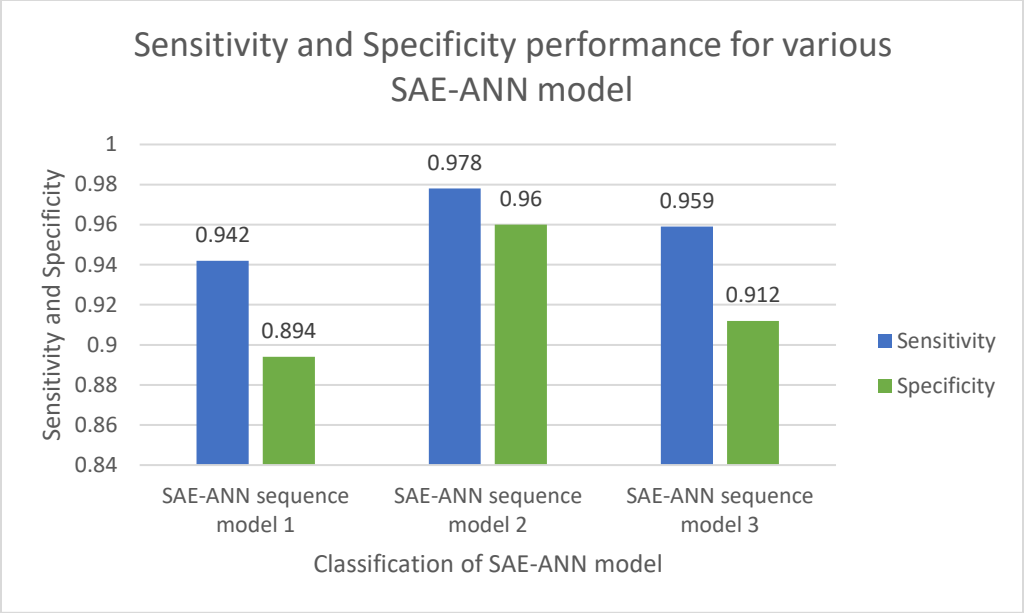

Figure 6 Sensitivity and specificity score for various ANN models

Figure 6 illustrates the sensitivity and specificity of differentSAE-ANN models.SAE-ANN sequence model 2 hasbetter sensitivity of 0.978 and specificity of 0.960, which is higher than other SAE-ANN models. Hence, it determines that a high true positive rate is better in SAE-ANN sequence model 2.

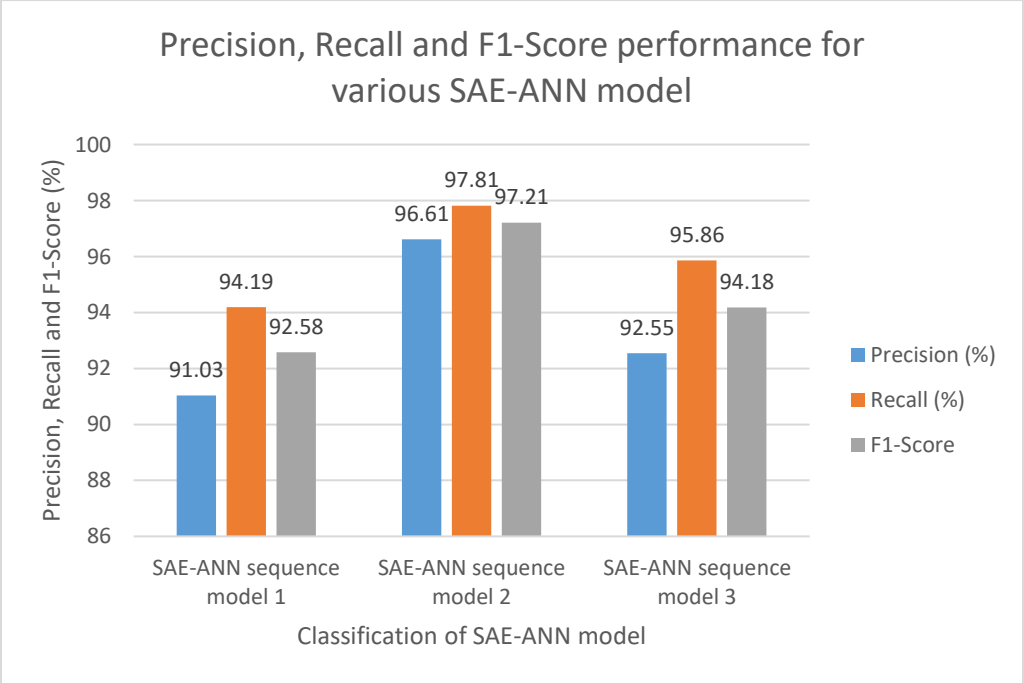

Figure 7 Accuracy for different optimizer ANN models

Figure 7 illustrates the precision, recall and F1-Score with different SAE-ANN models. In contrast, the precision, recall and F1-Score for SAE-ANN sequence 2 is 96.61%, 97.81%, and 97.21%,respectively,andhas a better TP rate and TN rate than other SAE-ANN sequence models. Hence, SAE-ANN sequence model 2 performs betterin predicting IDS classification through SAE in WSN.

V CONCLUSION AND FUTURE WORK

The SAE-ANN technique with different sequential patterns as the classifier in recognizing IDS and identifying network shields from DoSattacksis developed to address the issues above. The pre-trained SAE algorithm plays an essential role in this research for securing the transmission data by encryption and decryption through hash key and fine-tuned through various sequence patterns of the ANN model. Thus, evaluating the proposed SAE-ANN model produces high IDS recognition and securely transmits WSN data. Biometric verification offers several benefits over conventional authentication techniques, including increased safety, convenience, and accessibility. However, it also poses certain challenges, such as privacy concerns, potential vulnerabilities to spoofing attacks, and the need for specialized hardware or software infrastructure. The integration of sequential pattern analysis using ANN methods with biometric authentication presents a promising approach for enhancing the security of WSNs.

REFERENCES

1. R. H. Padyal and S. V. Kadam, "Continuous neighbour discovery approach for improvement of routing performance in WSN," 2017 2nd Int. Conf. Converg. Technol. I2CT 2017, vol. 2017-Janua, pp. 675-679, 2017, doi: 10.1109/I2CT.2017.8226215.
2. X. Zhao, S. Ren, H. Quan, and Q. Gao, "Routing protocol for heterogeneous wireless sensor networks based on a modified grey wolf optimizer," Sensors (Switzerland), vol. 20, no. 3, pp. 1-18, 2020.
3. P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," Proc. IEEE Int. Conf. Signal Process. Commun. ICSPC 2017, vol. 2018-Janua, no. July, pp. 288-293, 2018.
4. G. S. Dhunna and I. Al-Anbagi, "A low power cybersecurity mechanism for WSNs in a smart grid environment," 2017 IEEE Electr. Power Energy Conf. EPEC 2017, vol. 2017-Octob, pp. 1-6, 2018.
5. S. Qaboos, A. Khoudh, S. Qaboos, and A. Khoudh, "Improving the resilience of wireless sensor networks against security threats: A survey and open research issues," Int. J. Technol. , vol. 9, no. 4, pp. 828-839, 2018.
6. S. Aftergood, "Cybersecurity: The cold war online," Nature, vol. 547, no. 7661, p. 30, 2017.
7. C. N. Modi and K. Acha, "Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review," J. Supercomput., vol. 73, no. 3, pp. 1–43, 2016.

8. M. Al-Imran and S. H. Ripon, "Network intrusion detection: an analytical assessment using deep learning and state-of-the-art machine learning models," International Journal of Computational Intelligence Systems, vol. 14, no. 1, p. 200, Dec. 2021, doi: 10.1007/s44196-021-00047-4.
9. W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," Expert Systems with Applications, vol. 67, pp. 296–303, Jan. 2017.
10. N. Kaja, A. Shaout, and D. Ma, "An intelligent intrusion detection system," Applied Intelligence, vol. 49, no. 9, pp. 3235–3247, Sep. 2019.
11. Wang J, Gao Y, Yin X, Li F, Kim HJ. An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks. Wireless Communications and Mobile Computing. 2018 Dec 2;2018.
12. Rahul Reddy Nadikattu, "FUNDAMENTAL APPLICATIONS OF MACHINE LEARNING ACROSS THE GLOBE", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320- 2882, Volume.6, Issue 1, pp.31-40, January 2018.
13. K. Doshi, M. Mozaffari, and Y. Yilmaz, "RAPID: Real-time Anomalybased Preventive Intrusion Detection," ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML), 2019.
14. S. Sciancalepore, O. A.Ibrahim, G. Oligeri, and R. Di Pietro, "Detecting Drones Status via Encrypted Traffic Analysis," ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML), 2019.
15. Schwendemann, S.; Amjad, Z.; Sikora, A. A survey of machine-learning techniques for condition monitoring and predictive maintenance of bearings in grinding machines. Comput. Ind. 2021, 125, 103380. [CrossRef]
16. Liu, H.; Lang, B. Machine learning and deep learning methods for intrusion detection systems: A survey. Appl. Sci. 2019, 9, 4396. [CrossRef]
17. Cui, L.; Yang, S.; Chen, F.; Ming, Z.; Lu, N.; Qin, J. A survey on application of machine learning for Internet of Things. Int. J. Mach. Learn. Cybern. 2018, 9, 1399–1417. [CrossRef]
18. Rezaee, A.A.; Pasandideh, F. A Fuzzy Congestion Control Protocol Based on Active Queue Management in Wireless Sensor Networks with Medical Applications. Wirel. Pers. Commun. 2018, 98, 815–842.
19. Ahmad, R.; Wazirali, R.; Bsoul, Q.; Abu-Ain, T.; Abu-Ain, W. Feature-Selection and Mutual-Clustering Approaches to Improve DoS Detection and Maintain WSNs' Lifetime. Sensors 2021, 21, 4821.
20. Wazirali, R.; Ahmad, R. Machine Learning Approaches to Detect DoS and Their Effect on WSNs Lifetime. Comput. Mater. Contin. 2022, 70, 4922–4946.
21. Yaghini, M.; Khoshraftar, M.M.; Fallahi, M. A hybrid algorithm for artificial neural network training. Eng. Appl. Artif. Intell. 2013, 26, 293–301.

22. . Ioannou, C.; Vassiliou, V. An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression. In Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Montreal, QC, Canada, Oct 28–Nov 2 2018; pp. 259–263.
23. Vinayakumar, R.; Alazab, M.; Soman, K.P.; Poornachandran, P.; Al-Nemrat, A.; Venkatraman, S. Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access 2019, 7, 41525–41550.
24. Lu, X.; Han, D.; Duan, L.; Tian, Q. Intrusion detection of wireless sensor networks based on IPSO algorithm and BP neural network. Int. J. Comput. Sci. Eng. 2020, 22, 221–232.
25. Dr.K. Anuradha,Dr.S. Nirmala SugirthaRajini,T.Bhuvaneswari,Viji Vinod TCP /SYN Flood of Denial of Service (DOS) Attack UsingSimulation,ISSN: 0193 - 4120 Page No. 14553 – 14558,2020.
26. Dr.K. Anuradha,Dr.S. Nirmala SugirthaRajini, Analysis of Machine Learning Algorithm in IOT Security Issues and Challenges, Jour of Adv Research in Dynamical & Control Systems, Vol. 11, 09-, 2019.