An Effective Technique to Detect WIFI Unauthorized Access using Deep Belief Network

Original Scientific Paper

Rajakumar S.
Professor, Department of Electronics & Communication Engineering,
Panimalar Engineering College, Chennai, 600123 India
rajakumar109@outlook.com

Subraja Rajaretnam
Assistant professor, Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Jeppiaar Nagar,
Chennai 600 119 India
subraja654@gmail.com

William P.
Assistant Professor & Dean,
Research and Development,
Department of Information Technology,
Sanjivani College of Engineering, SPPU, Pune
william.wp09@gmail.com

Azhagu Jaisudhan Pazhani A.
Associate professor, Department of Electronics & Communication Engineering,
Ramco Institute of Technology, Rajapalayam,
Tamil Nadu 626117 India
pazhani876@gmail.com

Mabel Rose R. A.
Assistant Professor,
Computer Science and Engineering,
S.A. Engineering College, Poonamallee, Thiruverkadu,
Tamil Nadu 600077 India.
rose.RA87@gmail.com

Ahilan A
Associate Professor, Department of Electronics and Communication Engineering,
PSN College of Engineering and Technology,
India
listentoahil098@gmail.com

Abstract *– Network security has grown to be a major concern in recent years due to the popularity and development of Wi-Fi networks. However, the use of Wi-Fi networks is expanding quickly, and so is the number of attacks on Wi-Fi networks. In this paper, a novel WiFi Unauthorized Access Detection System (WUADS) technique has been proposed to detect unauthorized access in the WiFi network. Initially, the Wi-Fi frames are collected from the AWID dataset. The features of the Wi-Fi frame are extracted by using Principal Component Analysis (PCA). Finally, the Deep Belief Network (DBN) is employed for classification into authorized access and unauthorized access. The efficiency of the proposed WUADS technique was evaluated based on the parameters like accuracy, F1score, detection rate, precision, and recall. The performance analysis of the proposed WUADS technique achieves an overall accuracy range of 99.52%. The proposed WUADS method has a high success rate and the quickest attack detection time compared to deep learning techniques like CNN, RNN, and ANN. The proposed WUADS improves the overall accuracy better than 1.12%, 0.1%, and 14.22% comparative analysis of the SAE (Stacked AutoEncoder), WNIDS (wireless Network Intrusion Detection System), and 3D-ID (3 Dimensional-Identification) respectively.*

Keywords: *Wi-Fi networks, unauthorized access detection system, Principal Component Analysis, Deep Belief Network.*

1. INTRODUCTION

A Wi-Fi network comprises a wireless gateway facilitating internet access for various devices, with the router acting as a central hub connected to the internet modem [1]. Globally, wireless networks face increasing cyber threats, marked by sophisticated and persistent attacks that can bypass traditional security measures. The ubiquity of WiFi in diverse settings, such as businesses, coffee shops, and educational institutions, makes it challenging to verify users, leading to potential vulnerabilities [2, 3]. Wireless Local Area Networks (WLANs) utilize access points and wireless media, expanding rapidly as a wired technology alternative [4]. Found in numerous sectors like finance, telecommunications, healthcare, education, and public agencies, WLANs establish an invisible pathway between devices and the internet [5]. The growing popularity of WiFi can be attributed to its high data rate, flexibility, affordability, efficiency, mobility, and universal accessibility [6].

Data is transmitted and received by WiFi (sometimes referred to as a transceiver). A WLAN and fixed wire network can be connected by an access point, which also

creates links between users on the network [7]. WiFi data usage and communication are growing and are now considered necessities of an ever-expanding modern society; they are present in almost all homes, businesses, and public places [8, 9]. The Wi-Fi-Protected-Access/Preshared-Key (WPA2-PSK) does not guarantee 100% security and is still vulnerable to some types of attacks, including de-authentication, downgrade, and network security can be compromised by Denial-of-Service (DoS) attacks [10]. The challenge is coming up with a proactive and efficient method for quickly identifying illicit WiFi access. Current intrusion detection systems frequently fail to provide alerts in real time or may produce false positives, which negatively affects user experience and network performance. Furthermore, a solution that can detect unwanted access across a variety of devices and network configurations and react to developing threats is required due to the growth of IoT devices and diverse network designs. To overcome the above problem, a novel WUADS technique has been proposed to detect unauthorized access in the WiFi network. The main contributions are as follows:

- Initially, all Wifi frames are collected from the network traffic and from that data, a dataset has been constructed.
- After that, the features of the WiFi frames are extracted using Principal Component Analysis (PCA) to reduce the dimensionality of Wi-Fi frames and capture the most significant variations in the data.
- Then , the extracted features are given as input to the Deep Belief Network (DBN) for the classification of Wi-Fi frames into authorized access and unauthorized access.
- If Wi-Fi frames signal unauthorized access, the subsequent steps may include generating alerts and blocking the unauthorized device.
- The criteria F1 score, recall, precision, specificity, and accuracy are used to analyse the proposed technique's performance.

The remainder of the analysis is divided into the following sections: The literature review is thoroughly described in Section II. The recommended WUADS method is described in Section III. Section IV presents the findings, while section V summarizes the results.

2. LITERATURE SURVEY

Wi-Fi attacks fall into two main groups: those targeting network security and those affecting network deployment strategies. Here's an overview of recent advancements in security management for Wi-Fi networks.

Ref. [11] had analysed various wireless network assaults and performed network attack classification using stacked autoencoder (SAE) and deep neural networks (DNN). The experimental result shows that the classification accuracies achieved a 98.4%, 98.3% and 73.12%, respectively. The paper lacks discussion on model interpretability, essential for practical deployment in real-world scenarios.

Ref. [12] had analysed various risks to users' personal activities in light of growing business interest in tracking openly broadcast wireless data. Additionally, it demonstrates how an utterly inert eavesdropper can identify the data being transferred over the network. The lack of workable remedies for dangers to user privacy that have been outlined in the study leaves users in the dark about how to reduce the risks.

A Wireless Network Intrusion Detection system (WNIDS) [13] was developed to effectively detect attacks. In order to order the network data as normal or belonging attack. With a smaller set of features, WNIDS gets a multi-class classification accuracy of 99.42%. Drawback of the proposed WNIDS is that it has identified some flooding assault events in the test dataset as regular records.

A 3D-ID, a WiFi vision-based person re-ID system [14] was proposed in three dimensions. WiFi can picture a person in their actual surroundings thanks to WiFi equipment and a 2D AoA (Angle of Arrival) assessment of the signal reflections. The precision of the 3D-ID system is 85.3%. A disadvantage is that it has trouble with limited user evaluation, sensing range, and crowded areas.

CSI-based localization [15] was proposed, using an active device in place of a jamming harmful signals and disrupting communications, which serves as a relay and passes the received frames with a random delay. Promising initial results and a prototype show efficient location obfuscatio. The drawback is that it faces limitations and complexities, particularly in MIMO systems and real-world deployment challenges.

An automatic feature selection system and two-phase hybrid ensemble learning NIDS based on machine learning [16] was proposed Using four distinct machine learning classifiers. With a detection rate of 0.9314 and a false alarm rate of 0.0144, the THE-AFS-RF model outperformed the others for the wireless application. Drawback is the Proposed NIDS struggles with data volume, lacks external validation.

A method for training artificial neurons to identify intrusions on WiFi networks using a bio-inspired optimization algorithm (BOA) [17] was proposed. The WiFi intrusion detection framework works better than any other method, therefore it might be considered a back-up plan for protecting WiFi networks. Proposed WiFi intrusion detection faces challenges handling complex features, potential convergence issues in real-world scenarios.

A high-performing, low-complexity machine learning-based WiFi intrusion detection system (WiFi IDS) [18] was proposed. According to the results, it performs

better than other classifiers and offers enhanced accuracy with 20% fewer test runs and 26 times shorter training times than XGBoost. One disadvantage of WiFi Intrusion Detection Systems (IDSs) is that they are susceptible to difficulties with outdated models and processing costs.

Although these techniques function better than those previously created, they have significant disadvantages, including data loss, privacy infringement, high service costs, hosting, and server issues. In this research, a unique proposed approach called WUADS has been offered to address the aforementioned shortcomings.

3. PROPOSED SYSTEM

In this section, a novel WUADS technique has been proposed to detect unauthorized access in the WiFi network. Initially, the Wi-Fi frames are collected from the AWID (Aegean Wi-Fi Intrusion Dataset) dataset. The features of Wi-Fi frame are extracted by using Principal Component Analysis (PCA). Finally, the Deep Belief Network (DBN) is employed for classified into authorized access and unauthorized access. WUADS is an anomaly-based Wi-Fi network detection system. By searching for the state machine, which encapsulates the normal behavior of the protocol through its state transitions, one can keep an eye on state transitions in the Wi-Fi protocol. WUADS mimics the WiFi protocol's typical behavior. The results of network experiments can vary depending on the protocol that is utilized. Each protocol may have quite different communication protocols, and there is a chance that the experiment's channel and bandwidth will not work as intended. 802.11n is the most widely used wireless communication standard in the real world. Figure 1 shows the overview of proposed WUADS methodology.

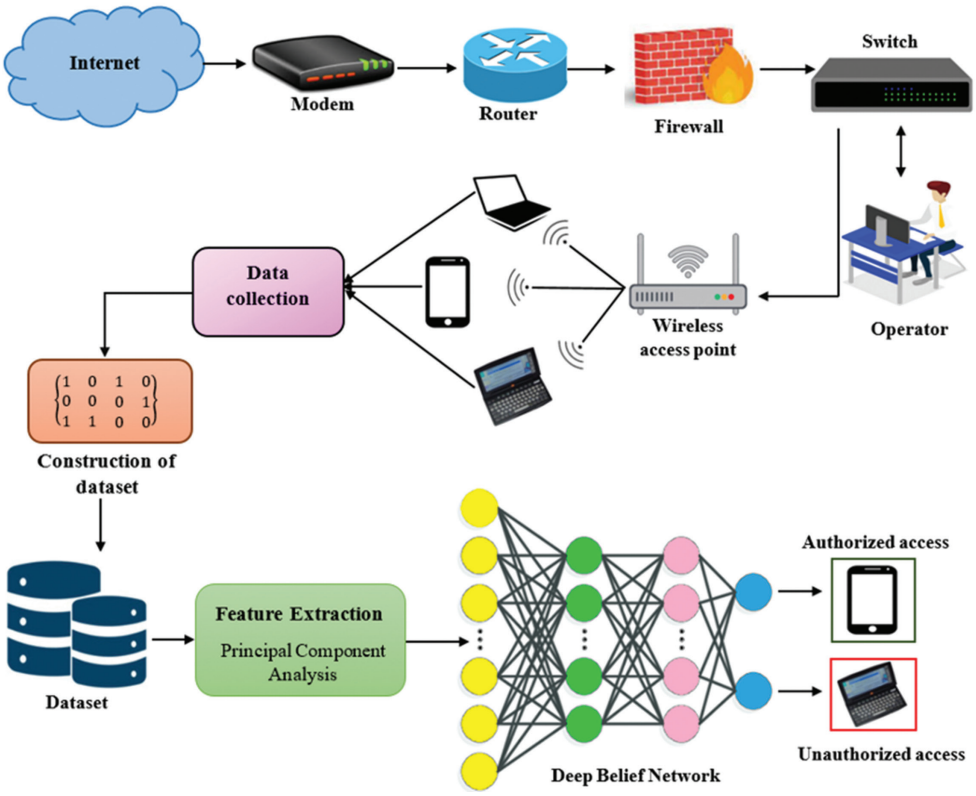

Fig. 1. An overview of proposed WUADS methodology

3.1. WORK FLOW OF WUADS METHODOLOGY

The proposed method's overview consists of a procedure for gathering and analyzing data. A variety of technologies, including computers, smartphones, tablets, the internet, modems, routers, firewalls, and switches, are used to gather data. After gathering the data, a dataset has been constructed. Principal component analysis is used to extract features from the dataset that the deep belief network can analyze. The authorization or unauthorizedness of data access is determined by the deep belief network. Either permitted or unauthorized access is the process's outcome.

3.2. DATASET COLLECTION

The dataset contains Wi-Fi activity that was captured over around five days and simulates a WUADS scenario. It has a desktop in monitor mode collecting frames, an access point, and Wi-Fi stations. One gadget invades the other. The dataset has four identified classes—three attack classes and one normal class—and provides multiple variations, including attack-specific and attack-class variants. The three types of assault are impersonation, flooding, and injection. 17 different Wi-Fi assaults are assigned to traffic records by the attack-specific version. We use the condensed attack-class form of the dataset,

which is available in both big and smaller variants to accommodate varying processing capacities.

3.3. PRINCIPAL COMPONENT ANALYSIS (PCA)

In this section, describe the WiFi frames can be feature extraction process by using PCA [19]. It is a widely used technique to reduce the dimensions of features. When the feature space is complex, conventional PCA cannot produce effective results since it linearly lowers the dimensions. To enhance the feature reduction process generalizes standard PCA to nonlinear dimension reduction. A useful feature dimension reduction approach is PCA, which is applied after the features have been normalised. To lower the dimensionality of huge datasets, eigenvectors of the covariance matrix with the greatest eigenvalues are identified using dimensionality reduction techniques like PCA. PCA algebraic definition is as follows:

Calculate the mean of B for data framework B as follows:

$$\mu = E(B) \tag{1}$$

Determine B's covariance as follows:

$$CU = C_{ov}(B) = E[(B-\mu)(B-\mu)^T \tag{2}$$

Count the eigenvalue λ_j, and eigenvector $a_1, a_2, \ldots a_N$, j= 1, 2…N of the covariance CV. The equation is solved for the Covariance CV;

$$W_k = \frac{\sum_{j=1}^{K} \lambda_n}{\sum_{j=1}^{M} \lambda_n} \tag{4}$$

The mutual range should be 83% greater than the size of the major segments, therefore choose the first K eigenvalue that did this, information about a more compact measurement subspace,

$$P = W^t - Y \tag{5}$$

Where Y is the original data that was knotted, and t denotes the transfer matrix. Operating the main K eigenvector independently from n to K ($K \ll n$).) increases the number of variables or measurements. The Wi-Fi network packets contain the attributes listed in Table 1.

$$|\lambda l - CV| = 0 \tag{6}$$

Whereas, l give the identity matrix credit for having dimensions that resembles CV. Decide on the λ_n Eigenvalues of the component K by counting the proportion of the data that the first component accounts for. The weight matrix W_k, whose columns are $B_T B$ eigenvalues, is established as follows:

Table 1. Initial feature set from dataset

Sl.No	Features	Description
1.	frame_epoch_time	Epoch time
2.	IP Add 1	Mac add 1
3.	IP Add 2	Mac add 2
4.	frame_type	Frame type
5.	frame_subtype	Framesubtype

To extract the frame epoch time from an unprocessed Wi-Fi frame, which represents the moment that the network device first noticed the frame, 1 and 2 addresses. The address frame type and frame variation can be found in two different places in a Wi-Fi frame. Using a set of frame source and frame destination addresses, we divide the Wi-Fi data into flows or sessions with a time interval of "t seconds". Depending on the type of Wi-Fi frame and how the Wi-Fi protocol is implemented, we can use the first four Wi-Fi addresses to determine the source and target Wi-Fi addresses.

3.4. DEEP BELIEF NETWORK (DBN)

WiFi frames may be divided between authorized and unauthorised access using the Deep Belief network. This network is referred from [20-22]. The DBN, which is able to extract the deep characteristics of the original data, is created by superimposing Boltzmann finite devices on a number of layers. The DBN's goal is to raise the likelihood of training data. Architecture of DBM shown in Fig. 2.

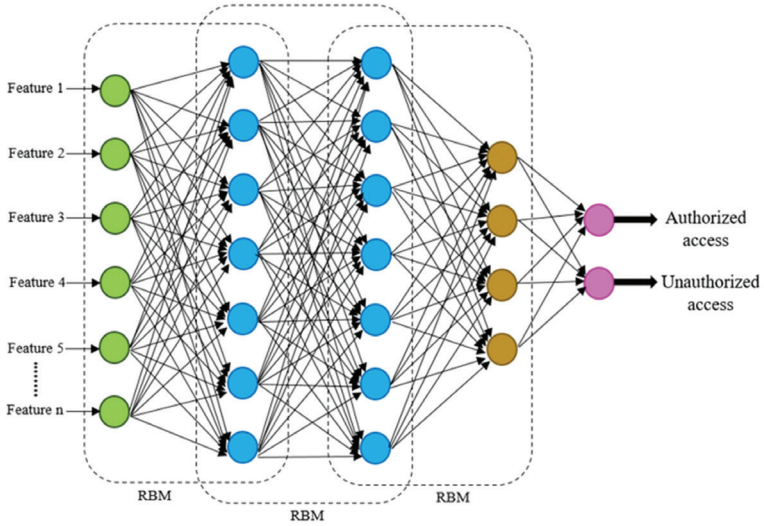

Fig. 2. Architecture of DBN

The DBN inputs are first sent to a low-level Restricted Boltzmann machine (RBM), which then begins the training process. After training the DBN outputs-containing top level RBM, the training process proceeds gradually up the hierarchy. Application of the energy function comprises:

$$\rho(L_x, L_y) = F_p^{-1} * e^{-F(L_x, L_y)} \quad (6)$$

Where L_{xj} and L_{xk} stand for the binary states of the hidden unit k and the visible unit j, respectively, and F_p designates the partition function created by combining probable pairings of exposed and hidden units,

$$F_p = \sum_{L_x, L_y} e^{-F(L_x, L_y)} \quad (7)$$

The following formula is used to get the energy of the entire hidden and visible unit configuration.

$$F(L_x, L_y) = -\sum_{j=1} b_j L_{xj} - \sum_{k=1} c_k L_{yk} - \sum_{j,k} L_{xj} L_{yk} Z_{jk} \quad (8)$$

Where Z_{jk} stands for the ratio of visible to hidden units, and b_j and c_k refer to the overt and covert unit biases, respectively. Updating the RBM weight requires:

$$\Delta Z_{j,k} = F_t (L_{xj} L_{yk}) - F_m (L_{xj} L_{yk}) \quad (9)$$

Where $F_t (L_{xj} L_{yk})$ and $F_m = (L_{xj} L_{yk})$ represent the expectations of the model and the training set, respectively. Ultimately, WiFi frames are categorized into allowed and unauthorized access using a DBN.

4. RESULT AND DISCUSSION

In this section, the experimental arrangement of the suggested WUADS was implemented using MATLAB to detect authorized and unauthorized access. Accuracy, precision, recall and specificity, are the different metrics used to evaluate it.

4.1. PERFORMANCE ANALYSIS

The following statistical metrics, including precision, specificity, F1 score, recall, and accuracy, are used to evaluate the success of the classification technique.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

$$Precision = \frac{TP}{TP+FP} \quad (11)$$

$$Recall = \frac{TP}{TP+TN} \quad (12)$$

$$Specificity = \frac{TN}{TN+FP} \quad (13)$$

$$F1\ score = 2\left(\frac{Precision*Recall}{Precision+Recall}\right) \quad (14)$$

Where *TP, FP* stands for the true and false of the sample and *TN, FN* stands for the true and false negatives.

Table 2 displays the classification of various WiFi security classes in relation to specific factors. the suggested WUADS's average accuracy, F1score, precision, recall, and specificity with the given parameters. The suggested WUADS have an average accuracy of 99.49% and 99.56%, respectively. Presentation scrutiny of the proposed model shown in Fig. 3.

Table 2. Performance Analysis of the proposed model

Class	Accuracy	Specificity	Precision	Recall	F1 Score
Authorized	99.49	95.56	89.25	85.97	88.89
Unauthorize	99.56	96.25	90.31	86.69	88.75

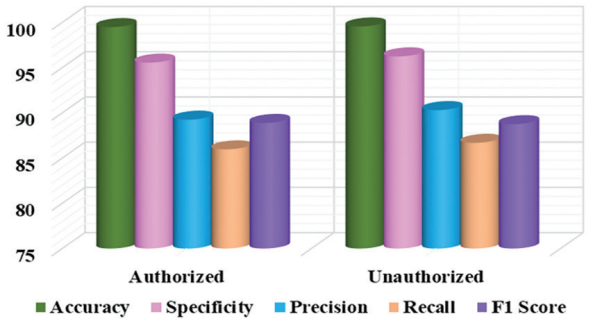

Fig. 3. Performance analysis of the proposed model

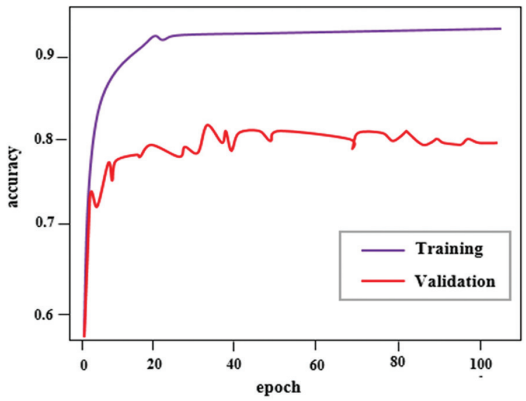

Fig. 4. Accuracy of proposed approach training and testing

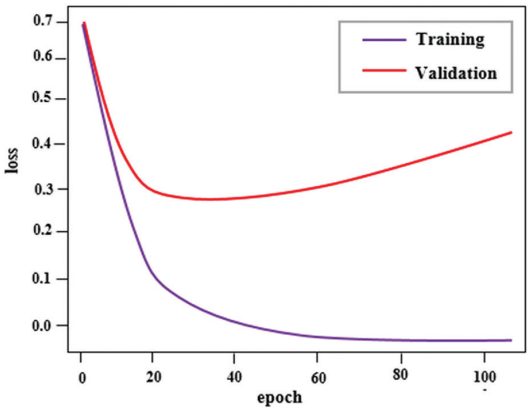

Fig. 5. Loss of proposed approach in training and testing

Figures 4 and 5 show how the recommended method has produced excellent accuracy throughout both training and testing. Performance is determined by accuracy, specificity, precision, recall, and the F1 score, and the proposed model's accuracy is 99.52%.

4.2. COMPARISON ANALYSIS

The proposed model and the current deep learning models are compared and analysed in this section. Precision, specificity, recall, accuracy, and F1 score were castoff to assess the presentation of current approaches in order to prove that the recommended strategy's outcome is more successful. Table. 3 compares the proposed model to CNN, RNN, ANN, and DBN, four types of machines learning neural networks.

Table 3. comparison between the suggested model to current deep learning networks.

Network	Success Rate (%)	Detection Time (sn)
CNN	70.5	710
RNN	74.8	736
ANN	85.4	787
Proposed(DBN)	92.9	863

From Table 3 compares the various algorithms such as CNN, RNN, ANN, DBN and it determined the unauthorized access at the highest rate and in the shortest time. It would be instructive to also list in Table 4 the corresponding optimal scores by the other deep learning algorithms. And it clearly indicates that the proposed DBN achieved better result than other algorithms. Successive rate of prevailing deep learning networks and the proposed model shown in Fig. 6.

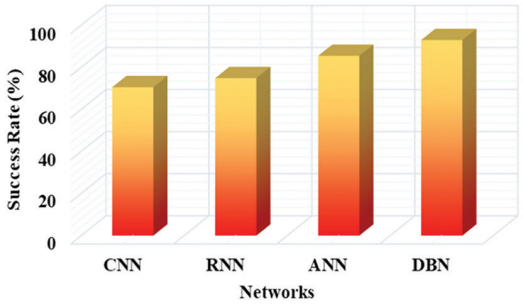

Fig. 6. Successive rate of existing deep learning networks and the proposed model

Fig. 6 illustrate, the successive rate of existing deep learning networks and the suggested technique. It clearly shows the proposed WUADS method has high success rate compare to deep learning techniques like CNN, RNN, and ANN.

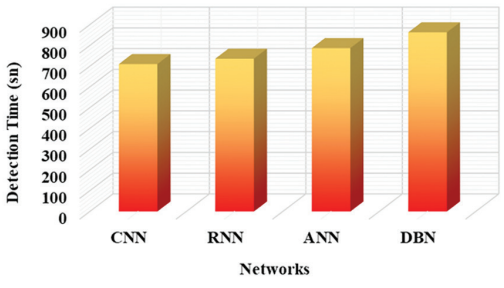

Fig. 7. Detection time of existing deep learning networks and the proposed model

The typical time required to spot one assault is shown in Fig. 7. The proposed WUADS outperforms CNN, RNN, and ANN by roughly 75% and has the shortest attack detection time when compared to existing methods.

Table 4. Comparison of the current and suggested models

Authors	Methods	Accuracy
Wang et al. [11]	SAE	98.4%
Reyes et al. [13]	WNIDS	99.42%
Ren et al. [14]	3D-ID	85.3%
Proposed	WUADS	99.52%

From Table 4 the proposed WUADS progresses the inclusive accurateness better than 1.12%, 0.1%, 14.22% Wang et al. [11], Reyes et al. [13], and Ren et al. [14]. The various recommended techniques are contrasted in Table 4. The data clearly demonstrates that the average accuracy value is 99.52%, meaning that the classifier used in the feature extraction and classification approach provides a higher accuracy number.

An extensive comparison of accuracy amongst extensive approaches is shown in Fig. 8, Sharp differences demonstrate proposed WUADS better performance and demonstrate how well it works to produce accurate results when compared to other models. The proposed WUADS improves the overall accuracy of 1.12%, 0.1%, 14.22% than existing SAE, WNIDS, 3D-ID correspondingly.

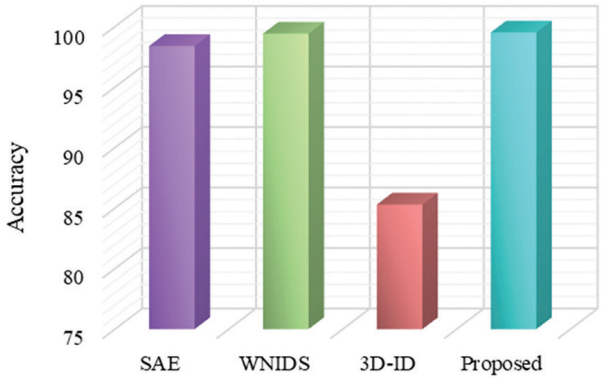

Fig. 8. Comparison in terms of Accuracy

5. CONCLUSION

In this paper, a novel WiFi Unauthorized Access Detection System (WUADS) technique has been proposed to detect unauthorized access in the WiFi network.The AWID dataset is where the Wi-Fi frames are first gathered. PCA is used to extract the Wi-Fi frame's features. Lastly, approved and illegal access are classified using the DBN. The efficacy of the suggested WUADS technique was evaluated based on variables such as detection rate, F1score, precision, accuracy, and recall. The suggested WUADS technique's performance analysis yields an overall accuracy range of 99.52%. Comparing the suggested WUADS method against deep learning techniques such as CNN, RNN, and ANN, it has the fastest attack detection time and a high success rate.

Comparative examination of the SAE, WNIDS, and 3D-ID shows that the proposed WUADS improves overall accuracy by 1.12%, 0.1%, and 14.22%, respectively. Although proposed WUADS provides a solid solution, it has several drawbacks, such as dataset dependence and possible noise in the feature extraction process the future work will be to integrate user authentication procedures to DBN-based detection, resulting in a multi-layered security strategy that blends machine learning and conventional techniques.

6. REFERENCES

[1] W. A. Jabbar, T. K. Kian, R. M. Ramli, S. N. Zubir, N. S. Zamrizaman, M. Balfaqih, V. Shepelev, S. Alharbi, "Design and fabrication of smart home with internet of things enabled automation system", IEEE Access, Vol. 7, 2019, pp. 144059-144074.

[2] J. B. Sequeiros, F. T. Chimuco, M. G. Samaila, M. M. Freire, P. R. Inácio, "Attack and system modeling applied to IoT, cloud, and mobile ecosystems: Embedding security by design," ACM Computing Surveys, Vol. 53, No. 2, 2020, pp.1-32.

[3] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, H. Arshad, "The internet of things security: A survey encompassing unexplored areas and new insights", Computers & Security, Vol. 112, 2022, p. 102494.

[4] S. Das, E. Mao, "The global energy footprint of information and communication technology electronics in connected Internet-of-Things devices", Sustainable Energy, Grids and Networks, Vol. 24, 2020, p. 100408.

[5] N. Sidek, N. A. Ali, G. Alkawsi, "An Integrated Success Model of Internet of Things (IoT)-Based Services in Facilities Management for Public Sector", Sensors, Vol. 22, No. 9, 2022, p. 3207.

[6] X. Fu, G. Fortino, W. Li, P. Pace, Y. Yang, "WSNs-assisted opportunistic network for low-latency message forwarding in sparse settings", Future Generation Computer Systems, Vol. 91, 2019, pp. 223-237.

[7] J. Hua, N. Shunwuritu, "Research on term extraction technology in computer field based on wireless network technology", Microprocessors and Microsystems, Vol. 80, 2021, p. 103336.

[8] T. De Schepper, J. Famaey, S. Latré, "Multi-technology management of heterogeneous wireless networks", Proceedings of the IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 20-24 April 2020, pp. 1-6.

[9] M. Tao, Z. A. Bhuiyan, A. Rahman, G. Wang, T. Wang, M. Ahmed, J. Li, "Economic perspective analysis of protecting big data security and privacy", Future Generation Computer Systems, Vol. 98, 2019, pp. 660-671.

[10] Q. Jiang, X. Huang, N. Zhang, K. Zhang, X. Ma, J. Ma, "Shake to communicate: Secure handshake acceleration-based pairing mechanism for wrist worn devices", IEEE Internet of Things Journal, Vol. 6, No. 3, 2019, pp. 5618-5630.

[11] S. Wang, B. Li, M. Yang, Z. Yan, "Intrusion detection for WiFi network: A deep learning approach", Proceedings of Wireless Internet: 11th EAI International Conference, Taipei, Taiwan, 15-16 October 2018, pp. 95-104.

[12] P. Shrivastava, P. Agarwal, "WiFi Data Leakage Detection", IOP Conference Series: Materials Science and Engineering, Vol. 804, No. 1, 2020, p. 12042.

[13] A. Reyes, D. F. Vaca, G. A. Castro Aguayo, Q. Niyaz, V. Devabhaktuni, "A machine learning based two-stage Wi-Fi network intrusion detection system," Electronics, Vol. 9, No. 10, 2020, p. 1689.

[14] Y. Ren, J. Yang, "Robust Person Identification: A WiFi Vision-based Approach", arXiv:2210.00127, 2022.

[15] M. Cominelli, F. Gringoli, R. L. Cigno, "AntiSense: Standard-compliant CSI obfuscation against unauthorized Wi-Fi sensing", Computer Communications, Vol. 185, 2022, pp. 92-103.

[16] A. K. Mananayaka, S. S. Chung, "Network Intrusion Detection with Two-Phased Hybrid Ensemble Learning and Automatic Feature Selection", IEEE Access, Vol. 11, 2023, pp. 45154-45167.

[17] L. Narengbam, S. Dey, "WiFi Intrusion Detection using Artificial Neurons with Bio-inspired Optimization Algorithm", Procedia Computer Science, Vol. 218, 2023, pp. 1238-1246.

[18] A. A. Bhutta, A. N. Mian, "Lightweight real-time WiFi-based intrusion detection system using LightGBM", Wireless Networks, 2023, pp. 1-13.

[19] S. Ayesha, M. K. Hanif, R. Talib, "Overview and comparative study of dimensionality reduction techniques for high dimensional data", Information Fusion, Vol. 59, 2020, pp. 44-58.

[20] Agasthian, R. Pamula, Kumaraswamidhas, "Integration of monitoring and security based deep learning network for wind turbine system", International Journal of System Design and Computing, Vol. 1, No. 1, 2023, pp. 11-17.

[21] X. Sun, G. Wang, L. Xu, H. Yuan, N. Yousefi, "Optimal estimation of the PEM fuel cells applying deep belief network optimized by improved archimedes optimization algorithm", Energy, Vol. 237, 2021, p. 121532.

[22] P. G. Sreelekshmi, M. B. Priya, V. Vishu, "Deep Forgery Detect: Enhancing Social Media Security Through Deep Learning-based Forgery Detection", International Journal of Data Science and Artificial Intelligence, Vol. 1, No. 1, 2023, pp. 9-19.