Intrusion Detection in Wireless Body Area Network using Attentive with Graphical Bidirectional Long-Short Term Memory

https://doi.org/10.3991/ijoe.v19i06.37593

Shaymaa Adnan Abdulrahman[1(✉)], Ehsan Qahtan Ahmed[2], Zahraa A. Jaaz[2,3],
Alya'a R. Ali[4]
[1]Business Information Technology Department, College of Business Informatics,
University of Information Technology & Communications, Baghdad, Iraq
[2]Computer Department, College of Science, AlNahrain University, Jadriya, Baghdad, Iraq
[3]College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN),
Kajang, Malaysia
[4]Department of Public Relations, College of Media, Al-Farahidi University, Baghdad, Iraq
dr.shaymaa.adnan@uoitc.edu.iq

Abstract—Recently developed low-power networked systems, wireless communications, and wireless sensors have all contributed to the rise of Wireless Sensor Networks (WSNs) as a potentially useful tool in the medical field. Securing Wireless Body Area Networks (WBANs) is essential for their widespread use in healthcare environments because the data they send frequently includes private and confidential patient health information. The study's goal is to create a system for detecting intrusions in WBAN. To best identify attacks in such systems, we present a novel "Attention-based Bi-directional Long Short-Term Memory with Graph Construction" (ABL-GC) here. The suggested approach ensures that the intrusion detection system uses only the features essential to detect a given attack, reducing the processing complexity.

Keywords—Wireless Body Area Network (WBAN), healthcare, intrusion detection, Attention-based Bi-directional Long Short-Term Memory with Graph Construction (ABL-GC)

1 Introduction

Over the past 20 years, research on wireless body area networks (WBAN) has received a lot of interest. The WBAN is a network made up of many medical sensor kinds, each with its function and debit. These sensors facilitate the monitoring of the patient's health and allow for quick emergency action. For conventional and carefully thought-out security solutions for encryption and authentication, the usage of computationally expensive cryptographic primitives is necessary. Due to their limited size, memory, and power capabilities, these security systems can often be challenging to convert to WBAN. In addition to resource limitations, insider attacks that compromise the medical device itself using cryptographic security techniques are ineffective for securing a network. "Intrusion detection systems" (IDS) are frequently used to monitor the node and network for any hostile activities as a second line of defense. The research community has not thoroughly investigated intrusion detection technologies that meet the requirements of WBAN [1].

IoT has increased the standard of patient care in the healthcare industry. People may live more pleasant lifestyles since continuous monitoring ensures their safety and well-being. Additionally, it enables a variety of applications, including Wireless Body Area Networks and implanted medical devices (WBAN). WBAN is made up of teeny, small gadgets that are thought to be the most innovative technology for enhancing healthcare. Due to these technologies' capacity to do remote monitoring, the overall standard of care given to patients in isolated locations or medical facilities has grown. WBANs have several advantages, but because sensor data is gathered from various sources, including persons and places, they are susceptible to outside assaults. People with bad intentions might manipulate the sensors and enter phony information that results in anomalous readings, which might lead to people receiving the incorrect diagnosis and treatments, resulting in enormous financial losses for any firms that change the healthcare system [2]. Any security issues, such as a change in the dosage of the prescription without authorization, might harm or even kill the patient. Patients don't want their private information to be misused or shared. Therefore, the WBAN must stop adjacent networks from listening in on patient conversations and leaking their private data. Any network's security must have authentication, which also aids in reducing unauthorized users and preventing many harmful security assaults on WBANs. To stop unauthorized users from accessing the system, WBAN uses authentication. This will be determined by the use of two factors and many levels of authentication; the first layer is related to sensors on the user's end and their device, while the second layer is internal to their device and an approved server [3–5].

These networks provide continuous, autonomous, real-time health monitoring for various medical uses by combining mobile devices, wireless wearable and implanted medical devices, and networks. Due to the delicate and often life-saving medical information that wireless body area networks handle, there are serious security and privacy concerns that prevent the widespread adoption of this technology. Implementing preventative security measures on wireless medical and mobile devices is difficult or impossible due to their low computational power. "Intrusion detection systems" (IDS), which can track and identify various security attempts, are necessary for these networks' full security [6–10].

Due to the delicate and occasionally life-critical medical information they deal with as well as the major privacy and security issues they raise, WBANs are not commonly recognized. Traditional security through preventative measures cannot be implemented due to the limited measuring power capabilities present in wireless medical and mobile devices. Intrusion detection systems (IDS) examine and identify the various security gaps in these networks to give total security. To identify the agreed-upon sensors, some were added to the security components of WBANs, such as IDSs and fault-tolerant systems. The two aspects of security management in WBAN are interruption identification and avoidance. Interrupt avoidance is the first layer of a protection system, much as encryption and authentication procedures. These techniques use the time interval key to provide authentication and encryption [10–13]. The main contribution of this paper is to recognize a specific assault and simplify the processing.

The organization of this paper included as, section II represents related works, section III represents proposed work, section IV represents result and discussion and section V denotes the conclusion part.

2 Related works

Reference [14] provides applications and explains the basic idea and broad context of the core WBAN system, information-via-negation sensor approaches, sensor node features, and existing models for embedded and on-body WBANs. Reference [15] focuses on the two key components of the communication technology needs for WBAN. Several popular short-range wireless technologies are thoroughly described in the first part, which also introduces the short-range category. These are suggested as possible choices for intra-BAN communications, which cover both internal and external communications inside and between components of a body area network (BAN). Reference [16] examines the well-known forms of communication. Long and short-range waves are the two primary types of waves used in WBAN applications, with each having a different utility. Optimum circumstances for an effective transfer. Reference [17] addressed the issue of path loss in WBAN; a protocol was put out in this study. We use three sets of scenarios that have been implemented in the OMNET++ environment to achieve this purpose. Three delay and data rate parameters were chosen to compare the output of the suggested method with the RSS route loss factor. Reference [18] presents a method for enhancing a wireless body area network's intrusion detection system's (IDS) functionalities (WBAN). Artificial neural networks (ANN) and decision trees in the J48 format are two well-known machine-learning methods that are used in this method. One form of security worries that the new method decreases for a WBAN is denial-of-service (DoS) assaults. Controlling noise is crucial since it might impede the sensors' ability to obtain accurate data. Reference [19] examines the different WBAN assaults and safety issues. Several decision tree classifiers' accuracy was evaluated in this study utilizing a physiological dataset made up of ECG signals obtained from a 25-year-old male subject. The accuracy and detection rate findings of the original dataset were compared to a reduced dataset made consisting of fewer, more significant attributes using Weka. According to the findings, combining data mining and decision tree classifiers is an effective way to evaluate the improved accuracy of an actual dataset produced from a WBAN after modification. Reference [20] presents a simple, sink-node-aided intrusion detection technique for WBAN. By employing this technique; the sink node may regularly keep an eye on packet delivery and record any anomalies for additional examination. Our portable technology has very low false positive rates and a very high true positive rate. The validity and effectiveness of our suggested mechanism are confirmed by in-depth studies and simulations based on Castalia. Reference [21, 22] concentrates on the Wireless Body Area Network (WBAN), a kind of health technology composed of minuscule medical sensors. Based on network metrics, this research suggested a unique intrusion detection system (IDS) that can distinguish between normal and abnormal states as well as false alarms from jamming states. Additionally, our suggested method enables us to discriminate between three forms of jamming, which reduces the frequency of false alarms and speeds up detection. Finally, the Castalia platform, which is built on the OMNET++ emulator, is used to replicate this IDS mechanism.

Reference [23, 24] presents a hybrid attack detection framework that makes use of the "Proportional Coinciding Score" (PCS) and the "MK-Means" algorithm, two well-known machine learning techniques that may be utilized to address respiratory and heartburn issues while improving attack detection accuracy. The amount of features in the training data is first decreased by data pre-processing in the PCS. The MK-Means method is used to train the data and make categorization easier when the pre-processed features are supplied. Third, the MK-Means approach is employed to determine particular attack detection indications offered by the intrusion detection system, such as the number of data packages received. In [25, 26], described a few key security factors for WBAN communication. Researchers have also discussed several security breaches that might happen in WBAN while messages are being sent. Possible countermeasures to the aforementioned assaults are also discussed. Last but not least, this survey research thoroughly analyzes security characteristics, risks, and countermeasures while addressing the WBAN system. Finally, this study's findings support the creation of WBAN data transmission methods.

3 Problem statement

WBAN security concerns are crucial since they may be quite damaging to a person. Medical records or other sensitive information about a patient might be exposed if an attack is carried out successfully. WBANs are used to broadcast the very sensitive and important patient health information that is kept, making these networks which are extremely important in today's society vulnerable to any failure, vulnerability, or security concerns. Malware on medical equipment, for example, or security weaknesses in wireless communication channels shows false data, which frequently results in improper diagnosis and treatment. Objective problems with medical technology have grown significantly during the last ten years. Wireless broadcasting is prone to a variety of security challenges, including eavesdropping, data interception, and data manipulation since wireless media is open and shared, the centralized infrastructure is insufficient, channel and network dynamics, and other difficulties. Even though a security hole in a healthcare system won't result in a patient losing their privacy, it might nevertheless inflict bodily injury if it enables adversaries to submit phony data or modify/suppress actual data, which would result in improper diagnosis and treatment. Due to the sensitive and usually life-critical medical information they deal with, WBANs are not routinely recognized. Traditional security through preventative measures is not practicable nor sufficient since wireless medical and mobile devices have limited measurement power capabilities. To provide these networks with full protection, "intrusion detection systems" (IDS) assess and find several security weaknesses. To detect assaults in WBAN, we suggested the ABL-GC approach.

4 Proposed work

WBANs are not frequently used because of the delicate and occasionally life-critical nature of the medical information they deal with. The traditional security implementation through preventative measures is not acceptable nor adequate given the restricted measuring power resources contained in wireless medical and mobile devices. To fully secure these networks, intrusion detection systems (IDS) assess and spot a variety of security holes. To overcome this issue, we have proposed Attention-based BiLSTM with graph construction. Figure 1 represents the proposed methodology of this study:

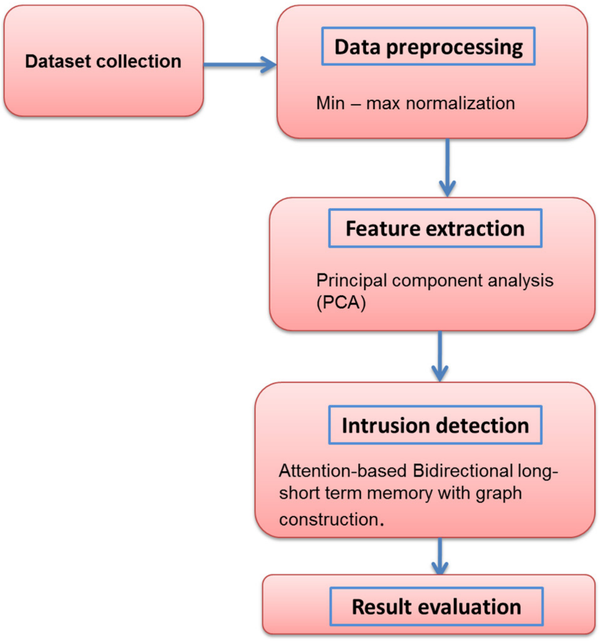

Fig. 1. Representation of our proposed methodology

4.1 Data collection

The Multiple Intelligent Monitoring in Intensive Care dataset was utilized in this investigation (MIMIC-I and II). From more than 90 ICU patients or participants, accurate physiological data records were collected for it. Moreover, the majority of researchers evaluated the feasibility of the suggested models using the MIMIC dataset as a benchmark. Four subjects were employed in this investigation to test the proposed model. There are seven characteristics in the dataset. These parameters, which also reflect the clinical condition of the patient, comprise the following: "Heart Rate" (HR), "Arterial Blood Pressure" (ABPsys, Dias, and Mean), Pulse, Temperature, "Respiration Rate" (RESP), and "Oxygen Saturation" (SPO2) with timesteps and date [2].

4.2 Data preprocessing using normalization

Several methods, including Min-Max normalization, z-score normalization, decimal scaling, standardized moment, and others, can be used to normalize datasets. Z-score normalization and min-max normalization are the two methods of normalization that are most well-liked and often employed. For our project, we employed the Min Max approach in (1).

$$w' = \frac{w - min_V}{max_V - min_V} \tag{1}$$

To normalize features in the range [0, 1], the following equation is used in min-max normalization. The lowest and maximum values of feature V are represented by min_V and max_V. The values w and w' represent the attribute's original and normalized values. As seen in the equation above, the maximum and minimum feature values are translated to 1 and 0, respectively.

4.3 Feature extraction using Principal component analysis (PCA)

If the features are chosen incorrectly, the overall performance of detection models would suffer greatly. The method of feature extraction used a variety of data mining approaches to identify some of the key traits for the detection of unusual connections. The characteristics, as we will see later employed can serve as the foundation for further feature extraction. Here, we shall quickly discuss some of the features of the information and features. There are a total of 22 separate data sets in the data collection. Each connection record has 41 characteristics that can have either discrete or continuous values. There are three types of 41-dimensional features. The first category of attributes is known as a product's basic or inherent features. Network connection, including duration, prototype, and service, several bytes derived from source IP addresses, or TCP connections use the destination IP addresses and certain flags. The dataset's feature selection approach has been extensively adopted as a standard way for network-based computing detection of intrusions However, in later works by others, it was discovered by researchers that the 41-dimensional characteristics are not the most effective in terms of intrusion detection and performance IDSs may be enhanced further by researching new features. PCA is a technique used in neural network and statistics research. The most basic methods of dimensionality reduction for big dimensional vectors' input data effectively feature extraction. We will then look into the application after that. The dimension of network connection data is reduced using PCA which described in (2) and (3).

$$y^e = \Phi^S y \tag{2}$$

$$\sum_{j=1}^{n} \lambda_j / \sum_{j=1}^{m} \lambda_j \geq R \tag{3}$$

The data vectors' covariance matrix is then calculated in (4).

$$D\Phi = \Phi \Lambda \tag{4}$$

Solving the equation yields the primary components. The covariance matrix eigenvalue problem C:

$$\Phi = [r_1, r_2, \ldots, r_n]\, \Lambda = [\lambda_1, \lambda_2, \ldots, \lambda_n] \tag{5}$$

Here, $\lambda_i (i = 1, 2, \ldots, n)$ are the eigenvalues and $v_i (i = 1, 2, \ldots, n)$ are the corresponding eigenvectors. Only the top m eigenvectors for each vector that corresponds to the m greatest eigenvalues must be calculated in equation (6) to represent network data records in a low-dimensional manner.

$$D_r = \lambda_j \lambda_j \tag{6}$$

Then, in equation (7)

$$D = \frac{1}{M} \sum_{s=1}^{M} (y_1 - \mu)(y_1 - \mu)^S \tag{7}$$

For the following connection to hold, a parameter *v* that represents inthe precision of approximation of the *m* largest eigenvectors can be included in PCA.

$$\mu = \frac{1}{M} \sum_{s=1}^{M} y_1 \tag{8}$$

We may choose the number given a precision parameter *v*. For a fresh input data set *y*, we may select the low-dimensional feature vector and the number of eigenvectors based on (8) and (9) as follows:

$$y_s = \left[y_{s1}, y_{s2}, \ldots, y_n \right]^s (s = 1,\, 2,\, \ldots,\, M),\;\; m = 41 \tag{9}$$

To demonstrate the use of the PCA-based dimension reduction, the proposed approach was used in conjunction with the SVMs with several classes for classifier development. The issue may be that because the training set contains so little data, some information may be lost during dimension reduction using PCA. In terms of SVM detection accuracy, SVMs without PCA are only marginally superior to SVMs with PCA. However, faster training and testing will be advantageous for SVMs with PCA, which is crucial for growing system applications.

4.4 Attention-based bidirectional long-short term memory with graph construction

Attention neural networks have demonstrated effectiveness on a range of current tasks, including question answering, machine translation, speech recognition, and picture captioning. For relation classification problems, we suggest the attention-based bidirectional LSTM with a graph creation mechanism in this section.

Let G should be a matrix made up of output vectors $[g_1, g_2, \ldots, g_S]$ and S is the length of the phrase that the BiLSTM layer generated. The output vectors are used in a weighted total to provide the representation *r* of the sentence in (10), (11), and (12):

$$j_s = \sigma(U_{Yj} + U_{gj}\, g_{s-1} + U_{dj^{d_{s-1}}} + a_j) \tag{10}$$

$$e_t = \sigma(U_{Ye}^{ys} + U_{me}\, g_{t-1} + U_{de^{d_{s-1}}} + a_e) \tag{11}$$

$$h_t = tang(U_{yd}^{ys} + U_{gd}\, g_{s-1} + U_{dd^{d_{s-1}}} + a_d) \tag{12}$$

Where, $H \in \mathbb{R}^{d^{\omega} \times T}$, d^{ω} is the word vectors' dimension, and *w* is a learned parameter vector. ω^T is a transpose. The dimension of $\omega, \alpha, \mathit{and}\, r$ is $d^{\omega}, T, \mathit{and}\, d^{\omega}$ separately.

The final representation of a sentence pair used for categorization is derived from (13):

$$d_s = j_s h_s + e_s d_{s-1} \tag{13}$$

First, BiLSTM with graph construction units is suggested to address the gradient disappearing issue. The fundamental concept is to add an adaptive gating mechanism that controls how much BiLSTM with graph construction units retain their prior state and retain the characteristics that were retrieved from the most recent data input. Then, several BiLSTM with graph construction variations has been suggested. The peephole connections enable all gates to investigate into the cell even while the output gate is closed by directly using the current cell state to create the gate degrees. Typically, attention-based BiLSTM recurrent neural networks are composed of four components. The network has two sub-networks for the left and right sequence contexts, which are respectively forward passing and backward pass, as illustrated in Figure 2.

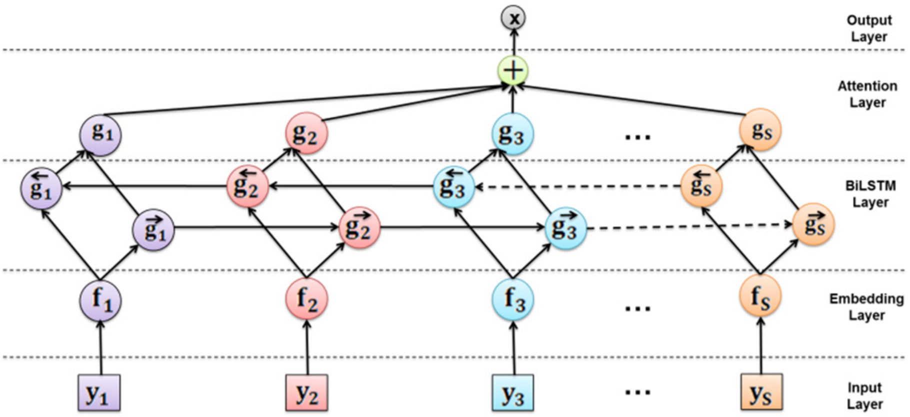

Fig. 2. Attention-based BiLSTM with graph construction

One input gate i_t with an associated weight matrix $W_{xi}, W_{hi}, W_{ci}, b_i$; one forget gate f_t with an associated weight matrix $W_{xf}, W_{hf}, W_{cf}, b_f$; one output gate O_t with an accompanying weight matrix $W_{xo}, W_{ho}, W_{co}, b_o$ all of these gates are programmed to produce a certain degree utilizing the input at hand x_i, the state h_{i-1} shows the result of the preceding step, the current condition of this cell c_{i-1}. For the sake of deciding whether to accept inputs, disregard previously stored memory and output the state created afterward. For example, as the following (14), (15), (16), (17), (18), (19) show:

$$p_s = \sigma(U_{Yp}^{ys} + U_{gp}\, g_{s-1} + U_{dp^{d_{s-1}}} + a_j) \tag{14}$$

$$g_s = p_s \mathrm{tang}(d_s) \tag{15}$$

$$g_j = [g_j \oplus g_j] \tag{16}$$

$$\mathrm{N} = \mathrm{tang}\ (\mathrm{G}) \tag{17}$$

$$\propto = softmax(U^S N) \tag{18}$$

$$v = G \propto^S \tag{19}$$

As a result, the weighted sum will be calculated utilizing the prior cell state as well as the most recent data produced by the cell to produce the current cell state. Having access to both past and future context is helpful for many sequence modeling tasks. Standard attention-based BiLSTMnetworks, however, only analyze sequences in temporal order and neglect context from the future. The hidden-to-hidden connection in the second layer of bidirectional LSTM networks flows in the opposite temporal order from those in the first layer, thus extending the capabilities of unidirectional LSTM networks. As a result, the model may make use of data from the past and the future. Attention-based BiLSTM with graph construction is employed in this paper. The following (20) shows the result of the ith word:

$$\mathrm{g}^* = \mathrm{tang}(\mathrm{v}) \tag{20}$$

Here, we aggregate the results of the forward and backward passes using an element-wise sum.

5 Result and discussion

To analyze the node and network for any hostile activity, "intrusion detection systems" (IDS) are frequently utilized as a second line of defense. The research community hasn't examined intrusion detection systems that are suitable for WBAN demands in great detail. We have analyzed the previous research techniques like Ensemble attention based BiLSTM [EA-BILSTM [27]], "Attention-based bidirectional long-short term memory network" [AT-BILSTM [28]], Multi-head attention based BiLSTM [MHA-BiLSTM [29]], Self-attention based BiLSTM auto encoder [SABiAE [30]] and our proposed method is attention based BiLSTM with graph construction [ABL-GC [Proposed]].

Accuracy is defined as the proportion of accurately anticipated instances positive or negative to all cases. The IDS must also be lightweight to have little impact on the

WSN's infrastructure and have high accuracy in identifying an intruder, even unknown assaults. According to what they discover and the accuracy they achieve, algorithms keep getting better. They are now more adept at anticipating and recognizing system dangers. This application provides several classification methods and visualization options to evaluate the accuracy of a dataset where data was gathered via a WBAN. When compared to other existing methods, our proposed method ABL-GC provides a high level of accuracy. Figure 3 represents a comparison of accuracy with current techniques.

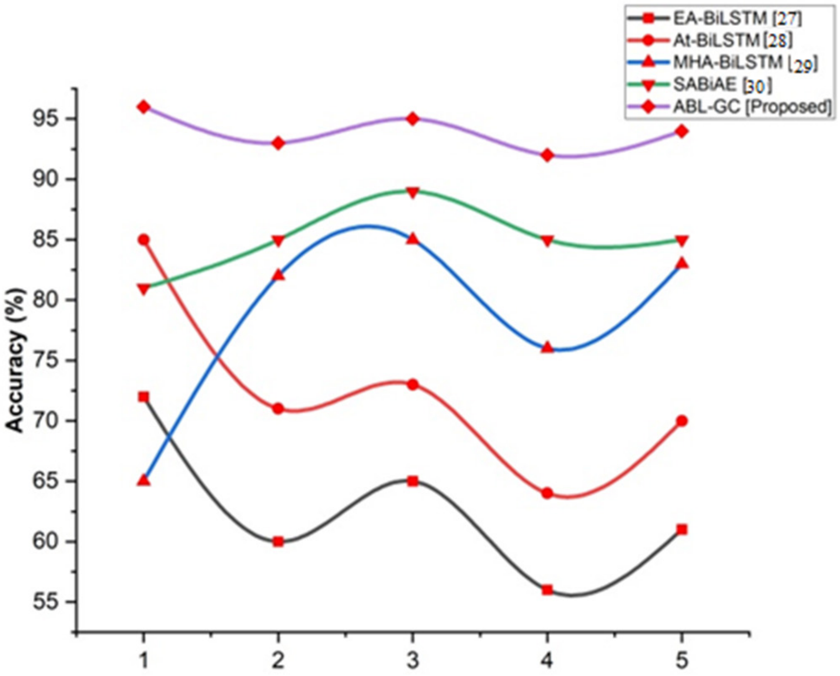

Fig. 3. Comparison of accuracy with current techniques

Accuracy is defined as the degree to which a measurement closely resembles its true value. Precision is the degree to which repeated measurements under the same circumstances provide the same results. It measures the proportion of positive data occurrences that occur. The proportion of pertinent samples among the recovered samples in pattern identification, data retrieval, and analysis is known as precision or the positive predictive value. Precision is the amount of data that a number conveys about its digits. The degree of precision demonstrates how closely two or more measures adhere to one another. Certainly not the same as accuracy. When compared to other existing methods, our proposed method ABL-GC provides a high level of Precision. Figure 4 represents a comparison of precision with current techniques.

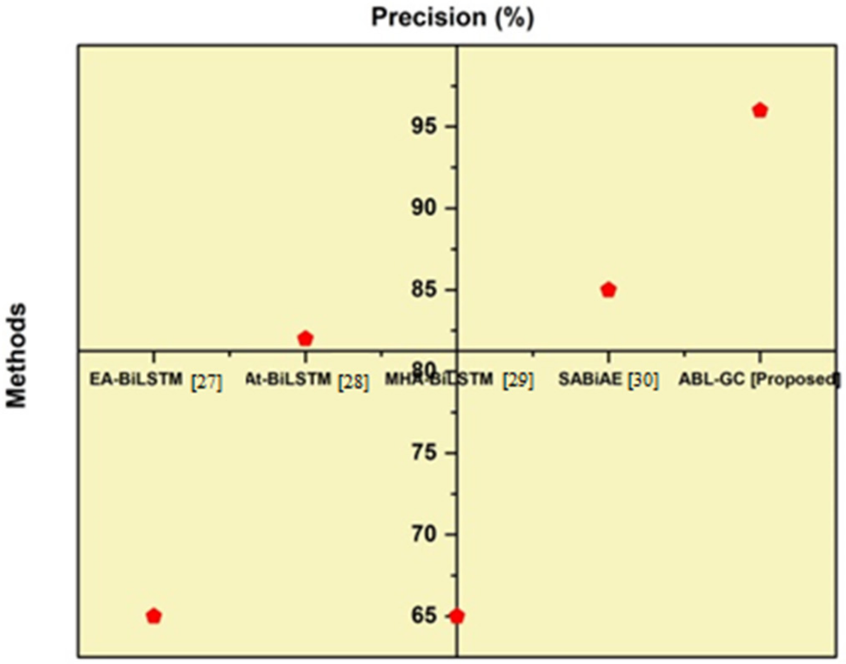

Fig. 4. Comparison of precision with current techniques

Recall indicates the statistic reflects the Precision's missing component or the proportion of actual attack cases that the classifier covered. Consequently, a classifier's high recall value is preferred. This measurement is comparable to the detection rate. Recall or sensitivity, on the other hand, refers to the portion of all relevant models that were successfully retrieved. However, knowledge and the level of relevance both affect memory and accuracy. When compared to other existing methods, our proposed method ABL-GC provides a high level of Recall. Figure 5 represents a comparison of recall with current techniques.

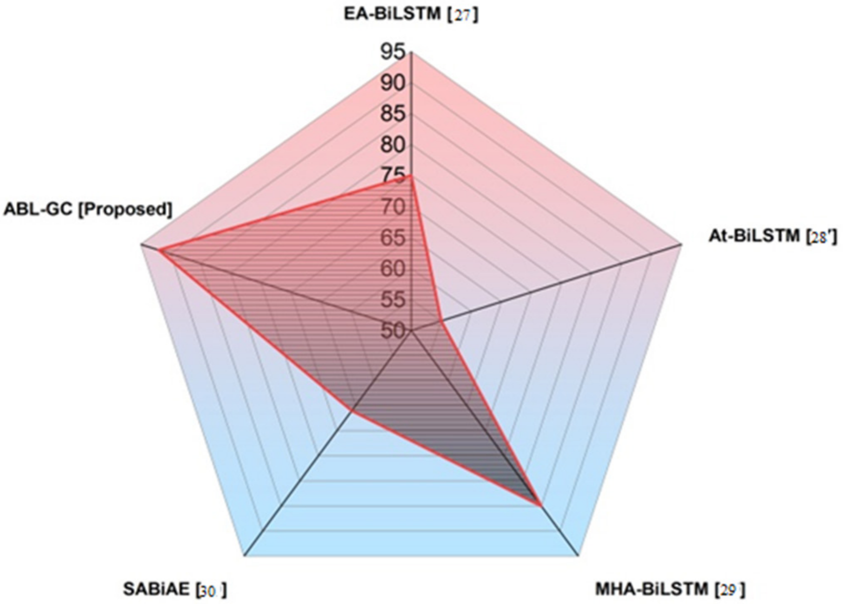

Fig. 5. Comparison of recall with current techniques

The precision and recall at a specific threshold are combined to form the harmonic mean of the F1 score. The F1-score, which combines both metrics into a single value, is produced by taking the harmonic mean of the accuracy and recall of a classifier. This approach is typically used to compare the performance of two classifiers. When just one accuracy measure is required as an assessment criterion, the F1 score is recommended. Figure 6 represents a comparison of the f1score with current techniques.

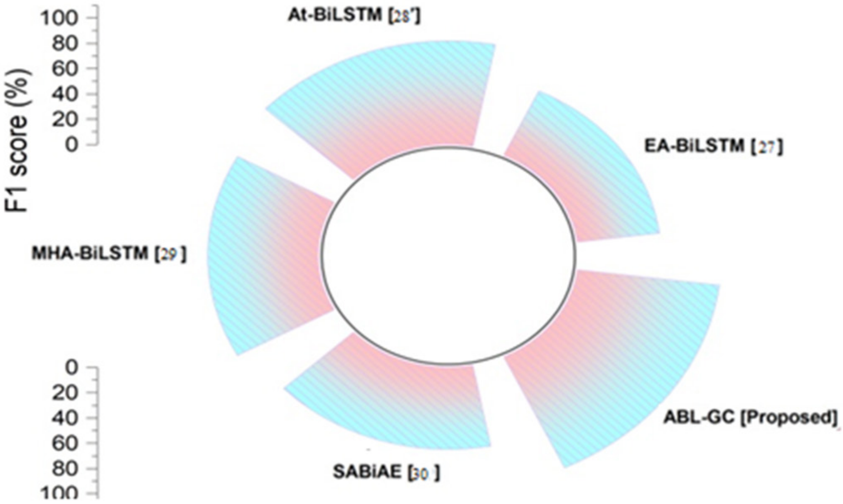

Fig. 6. Comparison of f1score with current techniques

The true positive rate, often referred to as sensitivity or recall in machine learning, is an indicator that counts the proportion of real positives that are correctly detected. True positives are the number of instances of abnormality that were identified as abnormal in the submitted vector data set. False negatives are the count of those anomalous sequences that the detector set categorized as normal, whereas true negatives are the number of normal sequences (normal cases) in the whole sequence that were correctly identified as normal. False positives are the number of instances where normal cases were incorrectly classified as abnormal. Weuses these measures, respectively, whenever and anywhere we talk about positive detection and misclassifications. When compared to other existing methods, our proposed ABL-GC provides a high true positive rate. Figure 7 represents a comparison of the true positive rate with current techniques.

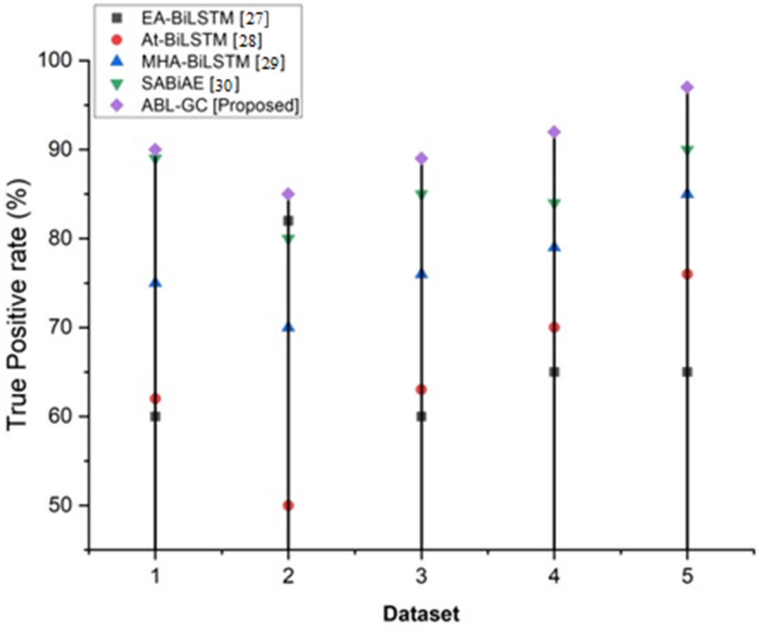

Fig. 7. Comparison of true positive rate with current techniques

6 Conclusion

The information gathered by these sensors is remotely transferred by medical experts via a WLAN or PDA, which is then utilized to treat patients accordingly. WBANs have some benefits, including decreased hospital costs, increased patient quality of life, longer-term data collecting, etc. Despite these advantages, WBANs present several security issues. We presented the "attention-based bidirectional long-short term memory with graph construction" (ABL-GC) technique to address this issue.

These factors include safeguarding data privacy and secrecy, validating data authenticity, and guaranteeing data availability when shared wirelessly. Using a real physiological dataset obtained from a WBAN, classifiers were assessed for accuracy and detection rate in this study. IDS was the deployment of an intrusion detection system. A future proposal will investigate the effect of adversarial assaults on the recommended model to show the resilience of deep learning methodologies against such attacks.

7 References

[1] G. Thamilarasu, "Genetic algorithm based intrusion detection system for wireless body area networks," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015: IEEE, pp. 160–165. https://doi.org/10.1109/ISCC.2015.7405510

[2] A. Albattah and M. A. Rassam, "A Correlation-Based Anomaly Detection Model for Wireless Body Area Networks Using Convolutional Long Short-Term Memory Neural Network," *Sensors,* vol. 22, no. 5, p. 1951, 2022. https://doi.org/10.3390/s22051951

[3] A. J. Aldarwish, A. A. Yassin, A. M. Rashid, H. A. A. Alasadi, A. A. Yaseen, and E. T. Khalid, "Design a Sturdy and Secure Authentication Scheme Capable of Early Detection of COVID-19 Patients using WBANs," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 27, no. 2, pp. 900–910, 2022. https://doi.org/10.11591/ijeecs.v27.i2.pp900-910

[4] J. Q. Kadhim and H. Salim, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," *International Journal of Emerging Technologies in Learning (iJET),* vol. 18, no. 02, 2023. https://doi.org/10.3991/ijet.v18i01.35987

[5] S. H. Abbood, M. Rahim, and A. M. Alaidi, "DR-LL Gan: Diabetic Retinopathy Lesions Synthesis using Generative Adversarial Network," *International Journal of Online and Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28005

[6] A. Odesile and G. Thamilarasu, "Distributed intrusion detection using mobile agents in wireless body area networks," in *2017 Seventh International Conference on Emerging Security Technologies (EST)*, 2017: IEEE, pp. 144–149. https://doi.org/10.1109/EST.2017.8090414

[7] I. A. Aljazaery, J. S. Qateef, A. H. M. Alaidi, and R. a. M. Al_airaji, "Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 8, 2022. https://doi.org/10.3991/ijim.v16i08.30107

[8] I. A. Aljazaery and M. R. Aziz, "Combination of Hiding and Encryption for Data Security," *International Journal of Interactive Mobile Technologies,* vol. 14, no. 9, pp. 34–47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[9] H. T. Hazim, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[10] H. Salim and H. Tauma, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[11] D. K. Anguraj and S. Smys, "Trust-Based Intrusion Detection and Clustering Approach for Wireless Body Area Networks," *Wireless Personal Communications,* vol. 104, no. 1, pp. 1–20, 2019. https://doi.org/10.1007/s11277-018-6005-x

[12] O. H. Yahya and I. Aljazaery, "Reducing the Data Rate in Internet of Things Applications by Using Wireless Sensor Network," *International Journal of Online and Biomedical Engineering (iJOE),* vol. 16, no. 03, pp. 107–116, 2020. https://doi.org/10.3991/ijoe.v16i03.13021

[13] N. Al-dabag and H. Alrikabi, "Encryption System for Hiding Information Based on Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 15, no. 2, 2021. https://doi.org/10.3991/ijim.v15i02.19869

[14] H. R. Abdulshaheed and M. S. B. Sidek, "Innovative Technologies of Wireless Sensor Network: The Applications of WBAN System and Environment," *Sustainable Engineering and Innovation, ISSN 2712-0562,* vol. 1, no. 2, pp. 98–105, 2019. https://doi.org/10.37868/sei.v1i2.69

[15] H. R. Abdulshaheed, I. Al Barazanchi, and M. S. Binti Sidek, "Survey: Benefits of Integrating Both Wireless Sensors Networks and Cloud Computing Infrastructure," *Sustainable Engineering and Innovation*, vol. 1, no. 2, pp. 67–83, 2019. https://doi.org/10.37868/sei.v1i2.29

[16] I. Al Barazanchi, H. R. Abdulshaheed, and A. Shibghatullah, "The Communication Technologies in WBAN," *Int. J. Adv. Sci. Technol,* vol. 28, no. 8, pp. 543–549, 2019.

[17] A. S. Shibghatullah and S. R. Selamat, "A New Routing Protocols for Reducing Path Loss in Wireless Body Area Network (WBAN)," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC),* vol. 9, no. 1–2, pp. 93–97, 2017.

[18] F. Alsubaie, M. Al-Akhras, and H. A. Alzahrani, "Using machine learning for intrusion detection system in wireless body area network," in *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, 2020: IEEE, pp. 100–104. https://doi.org/10.1109/SMART-TECH49988.2020.00036

[19] S. E. Medina and H. A. Kholidy, "An Analysis of a Signature-based Approach for an Intrusion Detection System in a Wireless Body Area Network (WBAN) using Data Mining Techniques," 2020.

[20] X. Hou, J. Wang, C. Jiang, S. Guan, and Y. Ren, "A sink node assisted lightweight intrusion detection mechanism for WBAN," in *2018 IEEE International Conference on Communications (ICC)*, 2018: IEEE, pp. 1–6. https://doi.org/10.1109/ICC.2018.8422794

[21] A. Bengag, O. Moussaoui, and M. Moussaoui, "A new IDS for detecting jamming attacks in WBAN," in *2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS)*, 2019: IEEE, pp. 1–5. https://doi.org/10.1109/ICDS47004.2019.8942268

[22] M. K. Abdul-Hussein, I. Obod, and I. Svyd, "Evaluation of the Interference's Impact of Cooperative Surveillance Systems Signals Processing for Healthcare," *International Journal of Online and Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28015

[23] R. K. Dhanaraj, L. Krishnasamy, O. Geman, and D. R. Izdrui, "Black Hole and Sink Hole Attack Detection in Wireless Body Area Networks," *Computers, Materials & Continua,* vol. 68, no. 2, pp. 1949–1965, 2021. https://doi.org/10.32604/cmc.2021.015363

[24] N. Alseelawi and H. T. Hazim, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[25] M. Soni and D. K. Singh, "New Directions for Security Attacks, Privacy, and Malware Detection in WBAN," *Evolutionary Intelligence,* pp. 1–18, 2022. https://doi.org/10.1007/s12065-022-00759-2

[26] I. A. Aljazaery and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[27] W. Chen, L. Yu, and J. Li, "Forecasting Teleconsultation Demand with an Ensemble Attention-Based Bidirectional Long Short-Term Memory Model," *International Journal of Computational Intelligence Systems,* vol. 14, no. 1, pp. 821–833, 2021. https://doi.org/10.2991/ijcis.d.210203.004

[28] X. Xue, C. Jiang, J. Zhang, and C. Hu, "Biomedical Ontology Matching Through Attention-Based Bidirectional Long Short-Term Memory Network," *Journal of Database Management (JDM),* vol. 32, no. 4, pp. 14–27, 2021. https://doi.org/10.4018/JDM.2021100102

[29] A. Kumar, V. T. Narapareddy, V. A. Srikanth, A. Malapati, and L. B. M. Neti, "Sarcasm Detection using Multi-Head Attention Based Bidirectional LSTM," *Ieee Access,* vol. 8, pp. 6388–6397, 2020. https://doi.org/10.1109/ACCESS.2019.2963630

[30] J. Zhang, X. Qi, and G. Ji, "Self Attention based Bi-directional Long Short-Term Memory Auto Encoder for Video Anomaly Detection," in *2021 Ninth International Conference on Advanced Cloud and Big Data (CBD)*, 2022: IEEE, pp. 107–112. https://doi.org/10.1109/CBD54617.2021.00027

8 Authors

Dr Shaymaa Adnan Abdulrahman: She is a lecture at University of Information Technology & Communications, College of Business Informatics, Business information technology Department. She graduated from Al Rafidain University – Iraq 2001 in computer science. In 2008 she received her M.S degree in information Technology and computer science college from Yarmouk University – Jordan. She graduated her Ph.D in 2021 from Ain shams University, Egypt – in computer Science department. Major Fields of Scientific Research: Artificial intelligence (AI), Computational intelligence, Machine learning, Knowledge engineering, Big data analytics, Intelligent biomedical informatics and Healthcare systems, and AI education Ph.D Thesis Title: Computational Intelligent Paradigms for Personal Identification based on Biometrics.

Ehsan Qahtan Ahmed: Dr in Computer Department – College of Science – AlNahrain University, Jadriya, Baghdad, Iraq.

Zahraa A. Jaaz received her Master degree in 2014 in computer sciences, now she is a lecturer at Al-Nahrain University, she has around 18 years teaching in different fields of computer sciences, her research interest areas are: computer networks, IoT, blockchain technologies, information systems, artificial intelligence and others. She can be contacted by email: zahraa.jaaz@nahrainuniv.edu.iq

Alya'a R. Ali holds a master of Computer Science from College of Science/Al-Nahrain University, Baghdad, Iraq in 2019. She also received B.Sc. (Computer Science) from al-Turath University, Baghdad, Iraq in 2012. She is currently an assistant lecturer at Public Relations Department in College of Media, Al-Farahidi University, Iraq. Her research includes pattern recognition, image processing, multimedia, Department of Public Relations, College of Media, Al-Farahidi University, Baghdad, Iraq. She can be contacted at email: a.rifat@uoalfarahidi.edu.iq

Article submitted 2022-12-12. Resubmitted 2023-01-23. Final acceptance 2023-01-24. Final version published as submitted by the authors.