IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 14, No. 3, June, 2024, pp. 923-931
Journal homepage: http://iieta.org/journals/ijsse

Network Fortification: Leveraging Support Vector Machine for Enhanced Security in Wireless Body Area Networks

Layth A. Jasim[1], Ahmed Talal Kamil[2], Mohammed F. Ibrahim Alsarraj[3], Israa Ibraheem Al_Barazanchi[4], Ravi Sekhar[5*], Pritesh Shah[5], Shilpa Malge[5]

[1] Department of Electrical Engineering, College of Engineering, Al-Iraqia University, Baghdad 10001, Iraq
[2] Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad 10001, Iraq
[3] Center Education Continuing, Northern Technical University (NTU), Mosul 10001, Iraq
[4] Computer Technology Engineering Department, College of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad 10001, Iraq
[5] Symbiosis Institute of Technology (SIT) Pune Campus, Symbiosis International (Deemed University) (SIU), Pune 412115, India

Corresponding Author Email: Ravi.sekhar@sitpune.edu.in

https://doi.org/10.18280/ijsse.140323

Received: 19 October 2023
Revised: 27 February 2024
Accepted: 5 March 2024
Available online: 24 June 2024

Keywords:
computer science, IT, network, Support Vector Machine (SVM), feature extraction, encryption, artificial intelligence (AI), authentication, healthcare

ABSTRACT

This study focuses on enhancing security in wireless body area networks (WBANs) through the application of Support Vector Machine (SVM)-based anomaly detection. The main problem addressed is the insufficient attention to security measures in WBANs, particularly in terms of secure connections and mitigation strategies. The proposed solution involves utilizing SVM to categorize security measures for WBAN telehealth solutions based on relevant attributes, ensuring ongoing utilization. The primary results showcase the successful prediction of vital signs with a remarkable accuracy of 98.63% using SVM, highlighting its effectiveness in enhancing security in WBANs. This paper explores the application of Support Vector Machines (SVMs) to enhance WBAN security updates and intelligence. Specific access management approaches may prove more effective during crisis situations. This study categorizes security measures for WBAN telehealth solutions exclusively using SVM based on relevant security attributes, ensuring their ongoing utilization. Employing SVM, the study predicts a heart rate of 89.087 beats per minute, an RR interval of 673.5 ms, and a QT interval of 271.3 ms, achieving a remarkable accuracy of 98.63 percent with a training dataset comprising 80 percent of the data and a testing dataset encompassing the remaining 20 percent.

1. INTRODUCTION

With the proliferation of mobile gadgets, wireless sensor networks (WSNs), Internet of Things (IoT) and various sensor technologies, the use of Internet of Things (IoT) devices for collecting information, tracking patients, and communicating with them has increased in the medical field [1]. WBANs are essentially networks of intelligent medical sensors placed on or around a patient. Healthcare professionals, sensors, and gateways are the primary components of a WBAN, as shown in Figure 1. Real-time monitoring of patients' health is possible with the help of these sensors. The elderly can also be monitored continuously, thereby reducing the need to hospitalize them on a regular basis. Using sensors, the patient is monitored remotely at their residence, and the collected data is wirelessly transferred to the medical facility. A healthcare professional can respond immediately to a medical crisis, such as a heart attack. In comparison with the sensors, the nodes serve as a bridge between the medical team and the sensors. Through them, both parties are able to maintain a safe connection. In Wireless Body Area Networks (WBANs), patient health data is accumulated and transmitted from a distance to the medical team, allowing constant monitoring and regulation of the patient's health. Therefore, remote clinical nanosensors can be used to diagnose patients [2]. Various data can be collected, including body temperature, ECG, glucose levels, and blood pressure. Wireless health networks [3] are becoming a burgeoning area in healthcare as they leverage pervasive technologies such as smart sensors, cloud technology, embedded systems, and wireless networks [4]. According to Oleiwi et al. [5], WBAN systems are among the most vital biomedical technologies. A healthcare provider perceives and forwards important patient health parameters and movement to be analyzed and acted upon [6]. WBAN was the driving force behind the development of IEEE 802.15.6 [7], which was created in response to its effectiveness and demand. Wireless communication channels combined with cloud computing have multiple security weaknesses and threats, despite the numerous benefits that this technology has to offer [8]. This can compromise the integrity and privacy of the exchanged data [9]. Message exchanges can be eavesdropped, intercepted, modified, or replayed by an attacker. A mobile tool or sensor can also be accessed to access information. Among the security hazards of Body Area Networks (WBANs) are offline password conjecture, privileged insiders, user surveillance, session key exposure, counterfeit messages, and misrepresentation. Health and lives of patients are directly affected by the privacy of shared data [8]. The resource limitations of the devices involved in WBAN pose a significant problem. While cloud computing could reduce the processing load on these devices, it also exposes them to several vulnerabilities and threats. These challenges can be addressed through encryption [10-27]. The importance of WBANs that use internet connections to link patients to medical servers cannot be overstated. For these networks to prevent multiple active and passive attacks, lightweight, efficient security solutions are needed. Wireless networks can be made more secure by implementing robust mutual authentication [28, 29]. Consequently, only authorized healthcare professionals will have access to highly sensitive and confidential patient data. As a result of this article, the following contributions are made:

- Wireless body area networks are reviewed in detail for their security and privacy.
- Wireless body area networks present both challenges and strengths in terms of security.
- Several recommendations are made based on the shortcomings identified in literature in order to achieve perfect security and privacy.

For continuous monitoring of patients, wireless body area networks (WBANs) are introduced in healthcare. The monitoring systems have shown success in detecting incidents. An improved reconfiguration process was developed to identify failed nodes in WBANs. Internet transmission of sensitive patient data is, however, accompanied by significant security concerns. To address this concern, the paper suggests the use of certificate-free Anonymous Authentication (AA) technology and Ciphertext-Policy-Attribute-based encryption and signature mechanisms. Role-based access control is implemented using an access tree to secure medical databases. The paper also mentions the importance of scheduling sensor data and suggests using packet priority for inter-WBAN data scheduling and aggregation to meet Quality of Service (QoS) requirements. Support Vector Machine (SVM) scheduling is proposed to enhance QoS. While WBANs are considered cost-effective due to commonly available network devices, the paper emphasizes the critical importance of security in WBAN configurations [12]. Various encryption techniques are available to ensure security, and the concept of security varies depending on different perspectives. Overall, the paper underscores the need for continuous development and improvement in the field of WBANs, particularly regarding security measures. According to the findings of Abdulbaqi et al. [13], the subsequent encryption schemes are extensively employed:

- AES (Advanced Encryption Standard): AES transforms readable data into an unintelligible format, making it reversible by reapplying the process.
- MD5: MD5 generates a 128-bit hash result but is known for its security vulnerabilities. It is commonly used for data integrity verification through checksums.
- HMAC (Hash-based Message Authentication Code): HMAC uses a hash function and a private key to create authentication codes for message verification, ensuring the source and credibility of communications.
- RSA Security: RSA is an asymmetric encryption method that employs two distinct keys: a private key and a public key. Public keys can be shared freely, while private keys must be kept confidential.
- ECC (Elliptic Curve Cryptography): Encrypted data can only be accessed by specific individuals using ECC. It encrypts and decrypts data using elliptic curve mathematics. With wireless security features like encrypted email and online browsing, ECC has been successful in implementing wireless security features [13].

WBANs are extensively discussed in articles [10, 11]. There is information on topics such as security threats, intruders, attack methods, and countermeasures. WBANs are also classified in these articles comprehensively. Medical servers must be secured with three layers of security to ensure the security of electronic medical data:

i. The layer responsible for collecting data: A WBAN's security layer encrypts data collected by various sensors and devices.

ii. Layer of Personal Servers: Within a WBAN, personal servers provide a layer for protecting data during transmission or processing.

iii. Layer of the medical server: This layer protects sensitive medical information stored on medical servers, emphasizing the importance of protecting such information.

This 3-layer architecture of WBAN is shown in the Figure 1.

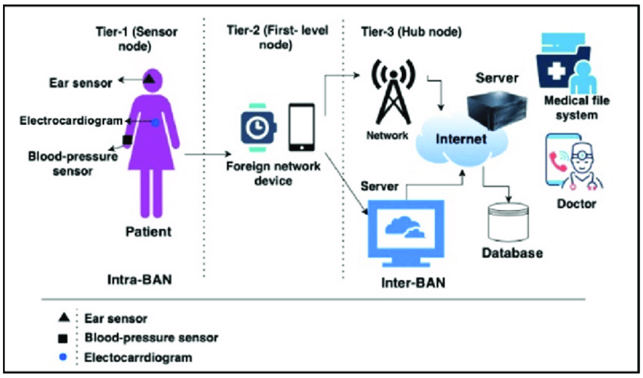

Figure 1. This demonstrates the 3-layer architecture of WBAN

To deploy networks efficiently, multilayered, lightweight systems with strong security are necessary for long-term preparation of scientific parameters. Due to their lack of patentability, wireless body-wide networks (WBANs) are not able to transmit data within the network, making them suitable for certain applications [12]. Overlooking security sensors in wireless local area networks (WLANs) poses challenges in evaluating security measures. High power consumption in wireless communication security components necessitates enhanced security protocols for WBANs. One scholarly article [13] explored Support Vector Machine (SVM) techniques in Body Area Networks (BANs), addressing various aspects like Quality of Service (QoS), synchronization, anomaly detection, fault detection, and secure communication. SVMs proved effective in meeting BAN requirements. Another study [14] examined WBAN frameworks in healthcare, highlighting issues like environmental interference, inadequate security measures, potential attacks, and QoS limitations. It also investigated SVMs in energy control and sensor access. Research suggests further exploration of transmission delays and security measures in WBANs is needed. A recent study [15] employed IEEE 802.15.6 protocol for hospital monitoring, covering topics like spectrum allocation and WBAN signal security. This study emphasized the ongoing need for advanced SVM technology in healthcare systems, especially for older individuals and those with disabilities. Artificial intelligence techniques were used to extract attributes from processed data. Another study [16] employed artificial neural networks and SVMs, particularly the kernel technique, to derive abstract properties from sensory data, improving predictions for wireless body area network security. The proposed multi-step authentication model based on iterative data utilization and predictive modeling demonstrated enhanced accuracy in predicting multi-step authentication of sensory input.

The development of a secure Wireless Body Area Network (WBAN) faces various challenges, including security, lightweight models, security handover, and reliability. Scholars are actively exploring innovative approaches to address these challenges. One such approach is the use of Support Vector Machine (SVM) techniques to enhance security and privacy in WBANs. In this article, the pros and cons of different methods and datasets are discussed. Medical devices, traffic monitoring, and recreational activities are all among the scenarios where AI can identify, prevent, and mitigate threats [17]. Medical databases should prioritize patient privacy, however. Compared to traditional healthcare systems, WBAN delivery faces many challenges regarding security, reliability, performance, and data differentiation. Among the benefits of wireless sensor networks is automatic configuration, which not only increases their lifetime, but also enhances data security. The safety of patients and user confidence play a vital role in ensuring that systems are resilient and sustainable. The use of SVMs facilitates decision-making in a human-like manner, making them more intuitive. Additionally, with SVMs being designed to be fault tolerant, scalable, perform accounting, and secure, they provide an effective tool for automating WBANs. Furthermore, SVM technology can be applied to other traffic management areas as well. Scheduling becomes increasingly challenging with increasing nodes and security levels [18].

Security challenges face WBANs, including the potential for replay attacks. Messages are encrypted with a nonce (a random number) to prevent data from being reused. Larger messages require longer nonces, while smaller messages require shorter nonces. The security of nonces can be improved by using longer ones. It is the objective of this study to demonstrate how Support SVM technology can enhance security in wireless local area networks. Network security issues can be addressed with SVMs, which are increasingly popular. Monitoring structural flaws and detecting structural defects is possible with them. Using a SVM-based model, security quality ratings are generated, and monitoring and translation functions enable security indicators to be translated into numerical security solutions. Within WBANs, SVM techniques were used for ensuring patient privacy in security and control applications. It is the objective of the study to devise a security mechanism compatible with SVM algorithms that enhances security while minimising implementation risks [19]. As a way of improving WBAN security measures and monitoring, a hierarchical clustering approach is introduced in the study. Furthermore, an array of sensor nodes can be rearranged using WBAN controllers. Moreover, statistical techniques from medical science are explored in conjunction with SVM analysis. System vulnerabilities include potential attacks and threats related to WBAN [20].

2. LITERATURE REVIEW

As a result, WBANs play a significant role in healthcare monitoring since they monitor the health status of patients at all times and notify them when they are in medical crisis. Recently, WBANs have been subject to security concerns because of the sensitive nature of the data passed through them and the potential risks of unauthorized access. WBANs have been observed to have security deficiencies, particularly when it comes to secure data transmission, privacy protection, and network integrity. WBANs are vulnerable to cyberattacks due to weak security measures and ineffective encryption protocols. Researchers have demonstrated that SVMs can enhance the security of wireless body area networks. A SVM method has been proven to be safe in medical settings for detecting anomalous behavior and securing communications. If SVMs are used for power and sensor regulation in WBAN environments, security and performance may be compromised [21]. Although these advancements have taken place, security frameworks specially designed for WBANs have largely remained a niche in the literature. By leveraging SVM technology for anomaly detection, this study proposes a novel framework for addressing this gap while ensuring the integrity and confidentiality of patient data in WBANs. The literature cited directly contributes to the understanding of challenges and opportunities in improving security in wireless local area networks [22-25]. By focusing on recent developments in SVM technology and its applications in healthcare monitoring systems, the reviewed studies provide a foundation for the proposed research framework [26-28]. References have been selected to support the critical analysis of existing security measures in WBANs and to identify the gaps that the current study seeks to fill. Figure 2 shows the WBAN interference mitigation system for patient monitoring [29].

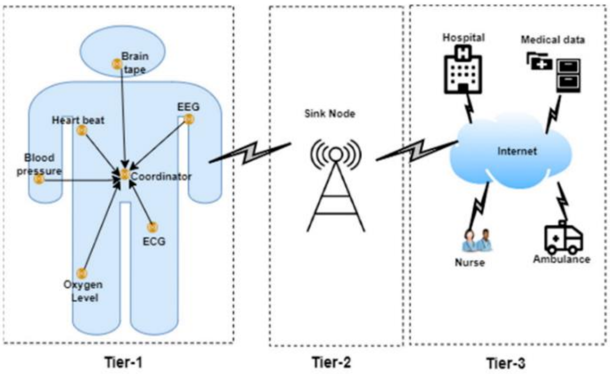

Figure 2. The WBAN interference mitigation system for patient monitoring [29]

The Support Vector Machine (SVM) is used with a soft-margin approach to enhance safety protocols. Reducing the number of sensors per node is economically feasible for SVM applications, emphasizing the importance of efficient sensor node placement. A comprehensive search approach is employed to find the best location for sensor nodes. When selecting a cluster's header for efficient and secure routing, priority is given to the sensor node with the highest remaining life percentage. Non-functional nodes focus on energy harvesting and transmitting available data to the central sink. Efficient routing improves node performance by directing data along the shortest path to the sink nodes. In the context of cybersecurity, it's observed that each individual node has a significant amount of remaining energy, and the total number of nodes is limited. To enhance data transfer security, threshold data on sensor data and cost value metrics are used. It is crucial that transceivers meet the secure optimization constraints in WBANs while ensuring the longevity of these networks. Table 1 shows the WBAN system is prone to attack at every level.

Table 1. WBAN system is prone to attack at every level [23]

Data collection level security attacks	▪ Data modification ▪ Drain the battery ▪ Modify the software of the device Jamming attack ▪ Node tampering Data collision attack Exhaustion
Transmission level security attacks	▪ Eavesdropping ▪ Man In the middle attack ▪ Scrambling attacks ▪ Signalling attacks ▪ Message modification attack ▪ Data interception attack ▪ Wormhole attack ▪ Denial of service attack ▪ Homing attack ▪ Selective forwarding attack ▪ Sybil attacks ▪ Path-dos attack ▪ Reprogramming attacks

A SVM approach that incorporates SVM with a regression strategy is proposed in this study to mitigate security concerns. The classification of authentication is facilitated by a SVM model using machine learning. Added security to this model has been achieved through the addition of a second layer of security.

3. METHODOLOGY

The wireless body area networks, or WBANs, facilitate communication between medical devices and central hubs. A great deal of use is made of these networks in hospitals, clinics, and nursing homes. The wireless body area networks, or WBANs, facilitate communication between medical devices and central hubs. A great deal of use is made of these networks in hospitals, clinics, and nursing homes. Patients' privacy is threatened by two main factors; (1) Lack of knowledge about the several policies and regulations in place regarding patient data handling, and (2) Hacker attacks.

An adversary may intentionally tamper with the transmitted medical data as well as disrupt authorized access to services and patient information, even if the messages received are authenticated. Consequently, the paper focused on improving the security of sending and receiving patient information in the medical field. Secure encryption using a strong and unbreakable method. When medical data is corrupt, the receiving node must reject the message. Poor wireless channel conditions can also cause data corruption. This can be accomplished with SVM. The SVM uses a hyperplane to divide the message into different classes. An accurate classification is most likely to take place when the selected hyperplane has the largest margin between it and all points. A hyperplane with the greatest margin is used to separate data points with SVM classifiers. Data points from new messages can be classified using SVM by finding an optimal hyperplane. Security in WBAN is based on two categories: legitimate traffic and malicious traffic. A WBAN has shown efficacy for detecting malicious traffic using SVMs. It is because SVMs are able to analyze and identify legitimate traffic by gaining knowledge about its characteristics. An exploration of SVM as a way to enhance WBAN security holds great promise. To protect WBANs against possible vulnerabilities, SVMs are a robust and effective solution.

3.1 Privacy and security requirements in WBAN

When it comes to finances, it's no secret that accruing wealth is vital. However, safeguarding these accumulated funds carries even more weight to ensure that they never fall into the wrong hands, thus preventing your hard-earned money from going to waste. This concept is not just exclusive to monetary matters - it also pertains to the gathering of personal or health-related data via several sensors in a wireless body area network (WBAN). Just like money, preserving the confidentiality and security of this sensitive information about a person's health status is of utmost importance [30-41].

Three main points in which security must be applied within WBAN are:

1. The user's body is equipped with sensors.
2. Data is stored and processed offline (where aggregated data is stored).
3. Various points of entry and exit or gateways.
4. Online (for connecting the medical community outside the WBAN).
5. In clinics or by medical professionals.

In order to ensure security, there are a number of factors to consider [42]:

I. An attacker compromising the health information of elderly and non-tech-savvy users could put their lives at risk.

II. A woman in the delicate stages of pregnancy wishes to keep her condition under wraps. However, an unauthorized individual breaches this confidentiality and broadcasts it, negatively impacting her social reputation and possibly threatening her safety.

III. It is possible for some insurance companies (through the use of private patient information) to modify (to reduce benefits) their policy for a user by obtaining this information.

IV. Insecure channel trespassing can lead to wrong information being entered. These modified information could be used to provide inappropriate medical treatment. Thus, a hospital or doctor's reputation and goodwill could be damaged, as well as the life of the patient [43].

The development of the project under WBAN will be adversely affected. Target customers/users will be slandered and defamed. Research progress could be hindered by a diminished trust in technology.

There are several important criteria that must be met by WBANs to develop accurate, reliable, secure, and trustworthy remote healthcare observation systems [44, 45].

The patient will be allocated a physician promptly following the completion of the registration process. Furthermore, it should be noted that patients are limited to perceiving only their current state of health, whereas doctors possess comprehensive knowledge and control over the entirety of their patients' medical records. When the doctor logs in, they will be presented with an encrypted version of the thumb or palm print they have selected, as outlined in the study of Shokeen and Parkash [27]. The physicians are granted access once their thumb and palm prints have been authenticated. Upon employing the Error Correcting Code (ECC) technique, which is grounded in Support Vector Machines (SVM), the physician will acquire the capability to assess the health condition of the patient. The flowchart in Figure 3 shows how this research is being conducted and the steps taken.

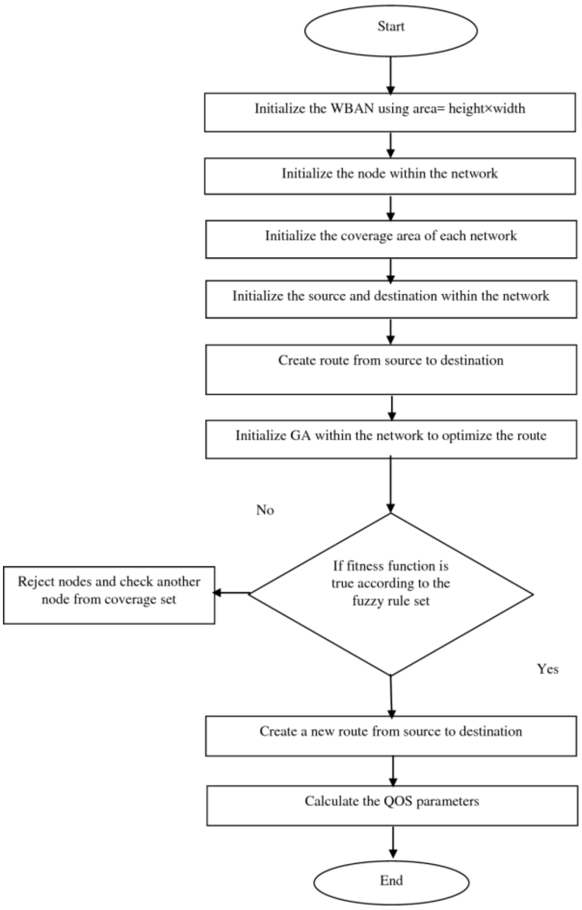
Start
Initialize the WBAN using area= height×width
Initialize the node within the network
Initialize the coverage area of each network
Initialize the source and destination within the network
Create route from source to destination
Initialize GA within the network to optimize the route
No
If fitness function is true according to the fuzzy rule set
Reject nodes and check another node from coverage set
Yes
Create a new route from source to destination
Calculate the QOS parameters
End

Figure 3. The methodology is depicted by the flowchart and steps being followed in this research

3.2 WBAN security enhancement with SVM

The Support Vector Machine (SVM) is a powerful tool for addressing complex scenarios, especially in dynamic environments like the Wireless Body Area Network (WBAN) system. SVM demonstrates adaptability and data protection capabilities in various ways, making it useful for enhancing WBAN security. Training an SVM model with labeled inputs is essential for prediction and categorization of new data, as mentioned in the study of Gautam et al. [28]. SVMs are versatile and can be used for both regression and classification tasks in supervised learning. Regression predicts continuous variables based on historical data, while classification categorizes data into distinct categories. There are specific procedures that must be followed for data to be classified as secure. A SVM uses a hyperplane model to cluster data, aiming to minimize deviations by selecting optimal boundaries. According to Figure 4, illustrates the importance of SVM in locating optimal hyperplanes for WBAN classification.

Based on similar characteristics, materials can be classified into groups. A secure system is essential for protecting sensitive medical data. SVM is one of the most popular and important technologies for securing data throughout its lifecycle. Keeping patient privacy protected from unauthorized access is crucial to prevent malicious entities from accessing sensitive information. Furthermore, it is imperative to improve security measures while incorporating the diversity, volume, and dynamics of medical data produced by WBANs.

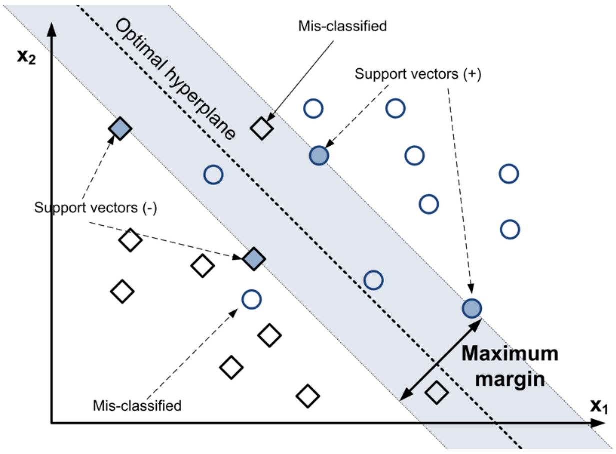

Figure 4. Demonstration of SVM hyperplane with optimal and minimum margins for classification of security measures

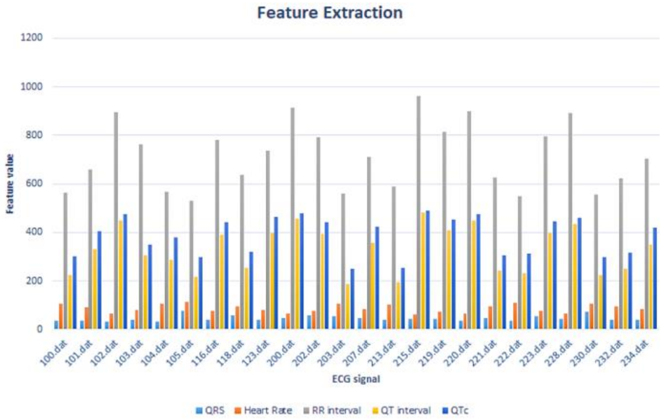

Figure 5. The extraction of patient’s body characteristics and features to be used with SVM for encrypting them for security reasons

3.3 Patient’s body feature extraction

Training data for vectors often lacks labels, as manual data labeling requires human involvement and not all data can be easily categorized. A study mentioned in reference [29-32] highlights the feasibility of using sensors attached to patients' bodies for automated medical interventions, particularly for individuals with chronic illnesses. However, wireless transmission of medical data to a personal server and the use of programming devices to configure medical equipment raise potential security concerns. These concerns encompass both unintentional environmental impacts and deliberate hacking attempts. To address these security issues, there is a need for a safety system that can detect and differentiate potential risks from genuine emergencies. Such a system should also prevent the delivery of pharmaceuticals that could have life-threatening consequences. Key metrics like QRS, heart rate, RR interval, QT interval, and QTC are essential for feature extraction in this context, and the extraction of nominal data from the patient's wearable sensors heavily relies on feature values [33-35]. Figure 5 shows the extraction of patient's body characteristics and features to be used with SVM for encrypting them for security reasons.

3.4 Training and testing

This study involves the training of a model using inputs that have been tagged, with the objective of making predictions or classifying incoming data. To train the SVM model for network-level abnormality detection, it is imperative that it outperforms other approaches in terms of accuracy and the number of epochs required. The duration of training is like that of a solitary machine learning model. Increasing the patient population leads to enhanced accuracy, decreased epochs, and does not impact the time of training. During the testing phase, the Support Vector Machine (SVM) solely relies on the new data to generate predictions, hence minimizing the volume of data transmitted via the network. The model is not submitted for remote storage [36-38]. The suggested method allows for the identification of anomalies, which occur when the value of a characteristic deviates from its regular range or has an unusual correlation with other attributes. The model evaluated, which was based on NS3, had the best level of accuracy in terms of approval (reaching up to 97%) and autonomous test precision (about 96%) among all the designs that were subjected to testing. Given the advantages of incorporating measurements, the utilization of this third model was employed to evaluate alternate setups and hyperparameters [39-41]. Figure 6 shows the SVM Model Accuracy (accuracy vs epochs) Model Loss (loss vs epochs).

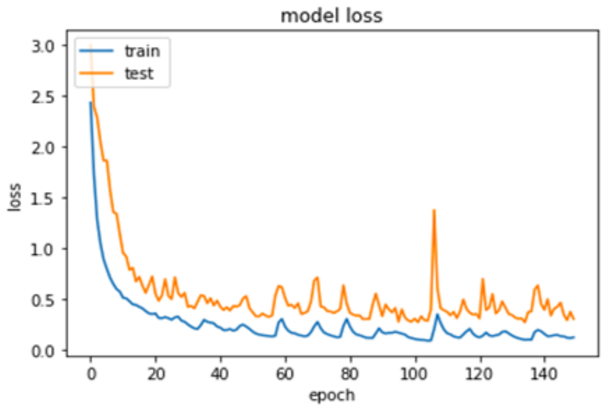

Figure 6. The SVM model accuracy (accuracy vs epochs) model loss (loss vs epochs)

The Support Vector Machine (SVM) model demonstrates a consistent ability to assign accurate labels to uncertain new instances by leveraging ranking techniques. The initial focus of investigation in the accuracy vs epochs plot is on the high-scoring event. The support vector machine (SVM) model, which utilized the elliptic curve cryptography (ECC) technique, was trained using a 10-fold cross-validation approach. With the goal of applying iterative refinement, occurrences are assigned labels with utmost precision, or alternatively, they are classified as Epochs. The tests conducted, as seen in Figure 6, indicate that the Area Under the Curve (AUC) exceeds 0.90, with the number of epochs exceeding 0.75. Statistical methods and SVM were found to be more effective than rule-based solutions at detecting suspicious access. In training a SVM, backpropagation is used to protect patient privacy, maintain confidentiality of recorded medical data, and ensure the accuracy and availability of diagnostic data. A study published in [28] suggests that models educated using shallow learning techniques, such as SVM decision trees, may not be able to detect underlying patterns in complicated leukemia datasets. Each SVM level extracts underlying patterns from the data using nonlinear transformations.

4. RESULTS AND DISCUSSION

Analyzing the data with statistical analysis helped determine whether the SVM framework contributed to increased security in WBANs. The effectiveness of this framework has been evaluated, trained and tested in real-world scenarios using several different machine learning models. WBAN describes the security guarantees based on an SVM trained with labeled input examples. Validating the model followed by evaluating its legitimacy and consistency in identifying errors and violations was conducted. WBAN sensor nodes were monitored with a real-time SVM platform to determine the platform's ability to anticipate risks and prevent them. SVM framework improves the security properties of WBAN significantly according to the study results. A WBAN provides high levels of confidentiality and confidence in the transmission of patient information due to its high success in identifying and categorizing anomalies. There is mounting evidence that SVM-based methods are more accurate, precise, and safe than existing approaches. Further research is necessary to address some of the issues identified in this study. As datasets become larger and security scenarios become more complex, further improvements to SVM frameworks are needed. Combined with research, other machine learning methods can enhance wireless network security. This area has seen an important development with the introduction of a SVM-enabled platform that enhances WBAN security. It allows healthcare providers and system administrators to monitor patients via wireless technology in a safe and effective manner and protect patient information in the process. It is our hope that the results of this study will improve the safety of healthcare environments, which will help ensure the greatest level of data validity and confidentiality. Further research and improvement of the SVM framework could come from further exploration in the future. This framework could conceivably be adapted for use with other IoT devices or network security systems in order to improve overall cybersecurity. SVM technology can be applied to a variety of security contexts, allowing for further innovation and advancements in data protection, anomaly detection, and security theory.

The findings of an illustrative evaluation based upon Key Performance Indicators (KPIs) for security measures in the proposed WBAN system have been illustrated. The SVM-advised model exhibits better accuracy, shorter training and prediction times, and a reduced number of false positives in trials. The utilization of machine learning (ML) techniques, namely non-linear support vector machines (SVM), is employed in WBAN for the purpose of anomaly identification, as the constituent sensors have limited power reserves. The aforementioned procedure demonstrates a high level of energy efficiency. Furthermore, the paucity of this informative subset contributes to the infrequency of attacks targeting it. This pertains to the agents falling inside the second category, encompassing low-power electronics [33].

Upon doing an analysis of the existing system, we subsequently proceed to evaluate the proposed system and juxtapose our findings with those obtained from the current system. The Support Vector Machine (SVM) algorithm processes these distinctive attributes and categorizes them into separate groups, so offering a hitherto unattainable level of cloud-based protection for patient data. This comparison analysis establishes that the proposed system exhibits superiority due to its capability to facilitate swift and secure data transmission. The test findings are being utilized to assess both the proposed and established methodologies. The concluding assessments within the application allow customers the opportunity to observe the projected enhancement of WBAN security through several parameter bases, encompassing perfect prediction, randomization, flipping, and the recommended support vector machine (SVM) approach. The investigation of the hyperplane reveals that the iterations under examination span from 0 to 50%, while the power level (expressed in dBm) has a negative scale. Figure 7 shows the classification of multiple patient's ECG and heart rate using SVM in terms of secure WBAN system.

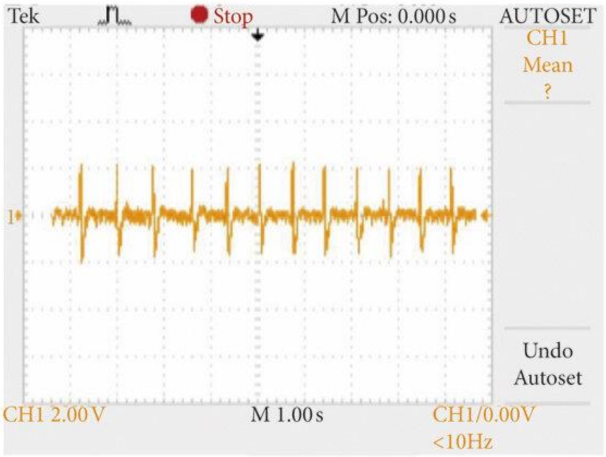

Figure 7. The classification of multiple patient's ECG and heart rate using SVM in terms of secure WBAN system

Table 2. Analyze SVM accuracy against existing literature

Article	Algorithm	Accuracy
[30]	K-Nearest Neighbor (KNN)	95.78%
[31]	Advanced Encryption Standard (AES-256)	96.36%
Proposed	Support Vector Machine (SVM)	98.63%

The Support Vector Machine (SVM) classifier has been selected for the purpose of anomaly detection using electrocardiogram (ECG) signals. This choice is motivated by the SVM's advantageous characteristics, including its cheap processing cost, minimal performance loss, and accuracy reduction. Results showed satisfactory performance for SVM classifiers, and the results were also in line with machine learning capabilities and benchmarks. Using WBAN devices for patient monitoring in non-traditional healthcare environments requires highly precise data acquisition to avoid serious consequences for patients. Inaccuracies in the data could have catastrophic consequences. As a direct result of their exceptional performance and ability to predict outcomes accurately, SVM algorithms and distributed learning frameworks are extensively used in contemporary healthcare systems. According to the source, 98.63% is a higher accuracy rate than 96.36% and 95.78% respectively for the AES-256 and KNN methods. Table 2 shows the Analyze SVM accuracy against existing literature.

5. CONCLUSION

WBAN security protocols are optimized using SVM using this document. By applying SVM with AI classifiers, this study provides valuable insights. WBAN nodes collect data from medical records in order to collect evaluation parameters. The proposed SVM-based WBAN showed a high level of accuracy of 98.63%. To achieve this accuracy, 80% of the data is used for training, while the remaining 20% is allocated to patient health tests in hospitals and clinics. SVM will improve data security, privacy and authentication by implementing the WBAN system. Hybrid SVM models have the ability to increase data security, reduce system complexity, and enhance data integrity. The best course of action to increase the safety of this probe was determined by using an SVM with a wireless sensor network. The approach we used resulted in the most effective network security measures with the fewest possible consequences. During data transmission, the SVM output is sent to the node responsible for maintaining data integrity. Through a series of standardized tests, the algorithm is used to classify medical data and assess the level of risk by comparing its effectiveness with that of established metrics. From the research results, it is clear that there is a high degree of accuracy in identifying risks associated with improving the reliability and security of the system, which makes it more suitable for WBANs.

ACKNOWLEDGEMENTS

The authors are grateful to the Iraqi Ministry of Higher Education and Scientific Research (MOHESR) for technically supporting the current research.

REFERENCES

[1] Abdulshaheed, H.R., Abbas, H.H., Ahmed, E.Q., Al-Barazanchi, I. (2022). Big data analytics for large scale wireless body area networks; challenges, and applications. Saeed, F., Mohammed, F., Ghaleb, F. (eds) Advances on Intelligent Informatics and Computing. IRICT 2021. Lecture Notes on Data Engineering and Communications Technologies, vol 127. Springer, Cham, 423-434. https://doi.org/10.1007/978-3-030-98741-1_35

[2] Barazanchi, I.A., Hashim, W., Alkahtani, A.A., Abbas, H.H., Abdulshaheed, H.R. (2021). Overview of WBAN from literature survey to application implementation. In 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Semarang, Indonesia, pp. 16-21. https://doi.org/10.23919/eecsi53397.2021.9624301

[3] Farooq, S., Prashar, D., Jyoti, K. (2018). Hybrid encryption algorithm in wireless body area network (WBAN). In: Singh, R., Choudhury, S., Gehlot, A. (eds)

Intelligent Communication, Control and Devices. Advances in Intelligent Systems and Computing, vol 624. Springer, Singapore, 401-410. https://doi.org/10.1007/978-981-10-5903-2_41

[4] Al Barazanchi, I., Abdulshaheed, H.R., Shibghatullah, A. (2019). The communication technologies in WBAN. Int International Journal of Advanced Science and Technology, 28(8):543-549.

[5] Oleiwi, S.S., Mohammed, G.N., Al-Barazanchi, I. (2022). Mitigation of packet loss with end-to-end delay in wireless body area network applications. International Journal of Electrical and Computer Engineering (IJECE), 12(1): 460-470. https://doi.org/10.11591/ijece.v12i1.pp460-470

[6] Aburomman, A.A., Reaz, M.B.I. (2017). A novel weighted support vector machines multiclass classifier based on differential evolution for intrusion detection systems. Information Sciences, 414: 225-246. https://doi.org/10.1016/j.ins.2017.06.007

[7] Abdulshaheed, H.R., Yaseen, Z.T., Salman, A.M., Al-Barazanchi, I. (2020). A survey on the use of WiMAX and Wi-Fi on Vehicular Ad-Hoc Networks (VANETs). IOP Conference Series: Materials Science and Engineering, 870: 012122. https://doi.org/10.1088/1757-899X/870/1/012122

[8] Wang, H., Zheng, B., Yoon, Ko, S.W., Hoo, H.S. A Support Vector Machine-Based Ensemble Algorithm for Breast Cancer Diagnosis. European Journal of Operational Research. 267(2): 687-699. https://doi.org/10.1016/j.ejor.2017.12.001

[9] Ma, Q., Sun, C., Cui, B.J. Jin, X.H. (2021). A novel model for anomaly detection in network traffic based on kernel support vector machine. Computers & Security, 104: 102215. https://doi.org/10.1016/j.cose.2021.102215

[10] Park, S., Hah, J., Lee, J. (2017). Inductive ensemble clustering using kernel support matching. Electronics Letters, 53(25): 1625-1626. https://doi.org/10.1049/el.2017.2159

[11] Prameela, S., Ponmuthuramalingam, P. (2016). A robust energy efficient and secure data dissemination protocol for wireless body area networks. In 2016 IEEE International Conference on Advances in Computer Applications (ICACA), Coimbatore, India, p. 14. https://doi.org/10.1109/ICACA.2016.7887937

[12] Rana, E.S., Kang, S.S. (2019). Implementation of biological key based security technique in wireless body area networks. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(8): 2156-2163.

[13] Abdulbaqi, A.S., Najim, S.A.M., Al-Barizinji, S.M., Panessai, I.Y. (2021). A secured system for tele cardiovascular disease monitoring. In Advances in Intelligent Systems and Computing, Springer, Singapore, pp. 209-222. https://doi.org/10.1007/978-981-33-6862-0_18

[14] Rani, C.R., Jagan, L.S., Harika, C.L., Amara, V.V.D.R. (2018). Light weight encryption algorithms for wireless body area network. International Journal of Engineering & Technology, 7(2): 64-66. https://doi.org/10.14419/ijet.v7i2.20.11754

[15] Roy, M., Chowdhury, C., Kundu, A., Aslam, N. (2017). Secure lightweight routing (SLR) strategy for wireless body area networks. In 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, pp. 4. https://doi.org/10.1109/ANTS.2017.8384119

[16] Sandhu, A., Malik, A. (2020). PAP: priority aware protocol for healthcare application in wireless body area network. International Journal of Recent Technology and Engineering (IJRTE), 8(5): 2733-2739. https://doi.org/10.35940/ijrte.E6373.018520

[17] Goeschel, K. (2016). Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive bayes for off-line analysis. In SoutheastCon 2016, Norfolk, VA, USA, pp. 1-6. https://doi.org/10.1109/SECON.2016.7506774

[18] Manirabona, A., Fourati, L.C. (2018). A 4-tiers architecture for mobile WBAN based health remote monitoring system. Wireless Networks, 24: 2179-2190. https://doi.org/10.1007/s11276-017-1456-7

[19] Morales, L.V., Delgado-Ruiz, D., Rueda, S.J. (2019). Comprehensive security for Body Area Networks: A survey. International Journal of Network Security, 21(2): 342-354. https://doi.org/ 10.6633/IJNS.20190321(2).19

[20] Mariani, M., Tweneboah, O.K., Beccar-Varela, M.P. (2021). Support vector machines. Data Science in Theory and Practice: Techniques for Big Data Analytics and Complex Data Sets. https://doi.org/10.1002/9781119674757.ch16

[21] Yaqoob, T., Abbas, H., Atiquzzaman, M. (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. IEEE Communications Surveys & Tutorials, 21(4): 3723-3768. https://doi.org/10.1109/COMST.2019.2914094

[22] Biggio, B., Corona, I., Nelson, B., Rubinstein, B.I.P., Maiorca, D., Fumera, G., Giacinto, G, Roli, F. (2014). Security evaluation of support vector machines in adversarial environments. Support Vector Machines Applications, 105-153. https://doi.org/10.1007/978-3-319-02300-7_4

[23] Barazanchi, I.A., Razali, R.A., Hashim, W., Alkahtani, A.A., Abdulshaheed, H.R., Shawkat, S.A., Jaaz, Z.A. (2021). WBAN system organization, network performance and access control: A review. In 2021 International Conference on Engineering and Emerging Technologies (ICEET), Istanbul, Turkey, pp. 27-28. https://doi.org/10.1109/ICEET53442.2021.9659564

[24] Paul, P.C., Loane, J., Regan, G., McCaffery, F. (2019). Analysis of attacks and security requirements for wireless body area networks—a systematic literature review. In: Walker, A., O'Connor, R., Messnarz, R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2019. Communications in Computer and Information Science, vol 1060. Springer, Cham, 439-4525. https://doi.org/10.1007/978-3-030-28005-5_34

[25] Rani, C.R., Rao, M.R.N., Venkateswarlu, S. (2018). Review on the security issues in human sensor networks for healthcare applications. International Journal of Engineering & Technology, 7(2): 269-274. https://doi.org/10.14419/ijet.v7i2.32.15582

[26] Bhawna, N., Amar, K.M. (2021). A survey on security and authentication in wireless body area networks. Journal of Systems Architecture, 113: 101883. https://doi.org/10.1016/j.sysarc.2020.101883

[27] Shokeen, S., Parkash, D. (2019). A systematic review of wireless body area network. In 2019 International Conference on Automation, Computational and Technology Management (ICACTM), London, United Kingdom, pp. 5. https://doi.org/10.1109/ICACTM.2019.8776847

[28] Gautam, M.B., Leena, H.P., Dilip, D., Ankush. H. (2019). A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. Sustainable Computing: Informatics and Systems, 23: 120-135. https://doi.org/10.1016/j.suscom.2019.06.002

[29] Mamoun, A., Farag, S., Khaled, S., Faisal, N. (2022). Artificial intelligence-based fault prediction framework for WBAN. Journal of King Saud University - Computer and Information Sciences, 34(9): 7126-7137. https://doi.org/10.1016/j.jksuci.2021.09.017

[30] Ali, M.J., Moungla, H., Younis, M., Mehaoua, A. (2019). Interference mitigation techniques in wireless body area networks. Mission-Oriented Sensor Networks and Systems: Art and Science, 677-718. https://doi.org/10.1007/978-3-319-92384-0_19

[31] Ali, M.H., Ibrahim, A., Wahbah, H., Barazanchi, I.A. (2021). Survey on encode biometric data for transmission in wireless communication networks. Periodicals of Engineering and Natural Sciences (PEN), 9(4): 1038-1055. https://doi.org/10.21533/pen.v9i4.2570

[32] Khalilian, R., Rezai, A., Mesrinejad. F. (2016). Secure wireless body area network (WBAN) communication method using new random key management scheme. International Journal of Security and Its Applications. 10(11): 13-22. https://doi.org/10.14257/ijsia.2016.10.11.02

[33] Ali, A.M., Ngadi, M.A., Sham, R., Barazanchi, I.I.A. (2023). Enhanced QoS Routing Protocol for an Unmanned Ground Vehicle, Based on the ACO Approach. Sensors, 23(3): 1431. https://doi.org/10.3390/s23031431

[34] Abdulbaqi, A.S., Panessai, I.Y. (2020). Designing and implementation of a biomedical module for vital signals measurements based on embedded system. International Journal of Advanced Science and Technology, 29(3): 3866-3877. http://sersc.org/journals/index.php/IJAST/article/view/5141

[35] Alnajjar, A.B., Kadim, A.M., Jaber, R.A., Hasan, N.A., Ahmed, E.Q., Sahib, M., Khalaf, A.L. (2022). Wireless sensor network optimization using genetic algorithm. Journal of Robotics and Control, 3(6): 827-835.

[36] Barazanchi, I.A., Hashim, W., Alkahtani, A.A., Abdulshaheed, H.R., Daghighi, E., Jaaz, Z.A., Shawkat, S.A. (2021). Survey: The impact of the Corona pandemic on people, health care systems, economic: Positive and negative outcomes. Journal of Applied Social and Informatics Science, 1(1): 13-20. https://doi.org/10.26555/jasis.v1n1

[37] Barazanchi, I.A., Sahy, S.A., Jaaz, Z.A., Abdulshaheed, H.R. (2021). Traffic management with deployment of Li-Fi technology. Journal of Physics: Conference Series, 1804: 012141. https://doi.org/10.1088/1742-6596/1804/1/012141

[38] Al-Barazanchi, I., Jaaz, Z.A., Abbas, H.H., Abdulshaheed, H.R. (2020). Practical application of IOT and its implications on the existing software. In 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), Yogyakarta, Indonesia, pp. 10-14. https://doi.org/10.23919/EECSI50503.2020.9251302

[39] AbdulQadir, A.A. (2015). Lempel - Ziv implementation for a compression system model with sliding window buffer. International Journal of Advanced Computer Science and Applications (IJACSA), 6(10): 101-104. https://doi.org/10.14569/ijacsa.2015.061014

[40] Al-Rababah, A.A., AlTamimi, T., Shalash, N. (2014). A new model for software engineering systems quality improvement. Research Journal of Applied Sciences, Engineering and Technology, 7(13): 2724-2728. https://doi.org/10.19026/rjaset.7.592

[41] AlRababah, A.A., Alghamdi, B.A. (2019). Information protection method in distributed computer networks based on routing algorithms. International Journal of Computer Science and Network Security, 19(2): 66-73.

[42] AlRababah, A.A.Q. (2017). Watermarking implementation on digital images and electronic signatures. International Journal of Advanced and Applide Sciences, 4(10): 160-164. https://doi.org/10.21833/ijaas.2017.010.022

[43] Alrababah, A.A. (2017). Implementation of software systems packages in visual internal structures. Journal of Theoretical and Applied Information Technology, 95(19): 5237-5244.

[44] Abdulbaqi, A.S., Nejrs, S.M., Mahmood, S.D., Panessai, I.Y. (2021). A tele encephalopathy diagnosis based on EEG signal compression and encryption. In: Anbar, M., Abdullah, N., Manickam, S. (eds) Advances in Cyber Security. ACeS 2020. Communications in Computer and Information Science, vol 1347. Springer, Singapore, 148-166. https://doi.org/10.1007/978-981-33-6835-4_10

[45] Abdulbaqi, A.S., Abdulhameed, A., Obaid, A.J. (2021). A secure ECG signal transmission for heart disease diagnosis. International Journal of Nonlinear Analysis and Applications, 12(2): 1353-1370. https://doi.org/10.22075/ijnaa.2021.5235