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

Mathematical Modelling of Engineering Problems
Vol. 11, No. 8, August, 2024, pp. 2267-2274
Journal homepage: http://iieta.org/journals/mmep

Enhanced Support Vector Machine-Based Intelligent Classification of Trusted Nodes in WBAN for Resilient Infrastructure

Adil M. Salman[1], Haider Hadi Abbas[2], Intisar A.M. Al Sayed[3], Azmi Shawkat Abdulbaqi[4], Ravi Sekhar[5*], Pritesh Shah[5], Sayali Sandbhor[5]

[1] Baghdad College, Economic Sciences University, Baghdad 10001, Iraq
[2] Computer Technology Engineering Department, Al-Mansour University College (MUC), Baghdad 10001, Iraq
[3] Faculty of Technical Engineering, Uruk University, Baghdad 10001, Iraq
[4] Renewable Energy Research Center, University of Anbar, Ramadi 55431, Iraq
[5] Symbiosis Institute of Technology (SIT), Symbiosis International (Deemed University) (SIU), Pune 412115, India

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

https://doi.org/10.18280/mmep.110829

Received: 16 October 2023
Revised: 12 February 2024
Accepted: 5 March 2024
Available online: 28 August 2024

Keywords:
Wireless Body Area Network, Trusted Nodes Classification, Kernel-based Independent Component Analysis (K-ICA), Enhanced Support Vector Machine, process innovation, resilient infrastructure

ABSTRACT

In various medical settings, ranging from hospitals to mental health care facilities and even homes, the Wireless Body Area Network (WBAN) assumes a critical role in enhancing the real-time monitoring of patients' overall health. The significance of the WBAN has grown recently due to its fundamental utility and its broad array of applications within the medical domain. It is basic to guarantee that the security of the touchy quiet information being transmitted over the WBAN framework remains a need since it relates to delicate understanding information. The establishment of a strong security framework holds immense necessity for any WBAN network to ensure the secure exchange of data between sensor nodes and other WBAN networks. This document introduces the Extended Support Vector Machine (ESVM) as an approach to differentiate trusted nodes within WBAN networks. This differentiation is accomplished through a classification method that reinforces the security dimensions of these networks. By employing Kernel-based Independent Component Analysis (K-ICA), relevant features are extracted from the data. The results of conducted tests unequivocally demonstrate that, when compared to various methods used previously, the proposed ESVM technique outperforms all of them in terms of its capacity to accurately classify trusted WBAN nodes in process innovation.

1. INTRODUCTION

Inside therapeutic situations, such as healing centers, mental wellbeing care offices, and indeed residential circles, WBAN expect an essential part in improving the real-time checking of quiet well-being. The basic commitment of WBAN and its wide scope of applications within the restorative division have gathered increased consideration in later periods. Given that the information passed on over the WBAN structure relates to delicate persistent records, guaranteeing security holds vital noteworthiness [1]. To ensure the secure transmission of information between sensor hubs and other WBAN systems, a strong security level is irreplaceable for any WBAN arrange. This report presents the concept of ESVM to distinguish trusted hubs inside WBAN systems. This separation is fulfilled through a classification technique that fortifies the security texture of these systems. Through the application of K-ICA, pertinent highlights are extricated from the information. The comes about of the conducted tests clearly illustrate that, when compared to different other strategies utilized already, the proposed ESVM strategy beats them all in terms of precisely classifying trusted WBAN hubs. WBANs have changed healthcare checking by empowering real-time information collecting from little biosensors embedded or associated to patients. In any case, guaranteeing information exchange security and constancy interior WBANs remains a pivotal concern. The recognizable proof and categorization of trusted hubs interior the organize may be a basic component of handling this trouble [2]. Utilizing a progressed procedure known as ESVM, this investigate proposes an interesting way to moving forward the categorization of dependable hubs interior WBANs. Trusted hubs are basic to guaranteeing the keenness and security of information stream interior WBANs. These gadgets have been approved, verified, and endorsed to perform indicated obligations. Their assignments incorporate defending information exchange and constraining hazard. The proposed strategy makes utilize of the capabilities of ESVM to intellectuals classify reliable hubs interior WBANs. SVMs are well-known machine learning strategies for classification applications. ESVM, an SVM expansion, incorporates changes that increment classification precision by optimizing parameters and include choice [3]. This strategy effectively oversees the complexities and complexities of distinguishing dependable hubs in WBANs, coming about in expanded constancy and security. Extraction of pertinent characteristics:

The strategy starts with the extraction of relevant characteristics from information procured by biosensors within the WBAN organize. These characteristics capture significant physiological changes and designs that offer assistance separate reliable hubs from others.

The utilize of ESVM for classification is at the heart of the strategy. The SVM show is optimized by ESVM by fine-tuning parameters and picking the foremost valuable highlights. This upgrade progresses the model's capacity to recognize between trusted and untrusted hubs.

The ESVM model is prepared employing a dataset of labeled occasions of trusted and untrusted hubs. The demonstrate learns the data's essential designs and relationships. The utilize of a particular dataset for approval guarantees that the model's execution is strong and generalizable.

After training, the ESVM model is deployed to classify nodes within the WBAN network. To assess the model's effectiveness in identifying potential candidates, the results are evaluated using metrics such as accuracy, recall, and the F1-score.

2. WBAN SECURITY CHALLENGES

WBANs face unique security challenges due to limited resources, wireless communications, and proximity to sensitive personal information. Some of the main challenges are listed below.

Resource limitations: WBAN devices are often small, with limited processing power, memory, and battery life. This makes it difficult to implement robust security mechanisms without impacting device performance.

Radio communications: WBANs rely on radio communications, which are inherently vulnerable to eavesdropping, interception, and jamming. Ensuring secure data transmission in such environments is a major challenge.

Proximity to sensitive data: WBAN collects and transmits sensitive personal data such as: B. Health information that requires strong privacy and confidentiality. Unauthorized access to this data can have serious consequences for individuals.

Lack of standardization: The lack of standardized security protocols and architecture for WBANs makes it difficult to ensure interoperability and compatibility between different devices and systems.

Human factors: User behavior and habits can also pose security risks. For instance, losing a WBAN device or sharing sensitive data without proper precautions can jeopardize the security of the entire network.

WBANs are susceptible to various malicious attacks, such as denial of service attacks, spoofing attacks, and malware infections. These attacks can disrupt network operations, compromise data integrity, and even pose physical risks to individuals. Overcoming these challenges necessitates a comprehensive approach that combines technical security measures, user training, and a regulatory framework to ensure the secure and reliable functioning of WBANs.

3. RELATED WORK

Kaur et al. [4] introduced a system concentrating on identifying sensors utilizing the MICS frequency band. The utilization of radio transmissions from implanted medical devices has expanded our comprehension and preemptive measures against human illnesses. The study provides a methodology applicable across three distinct scenarios for positioning the receiving station. In Al-Suhimat et al.'s [5] study, the proposal of a wireless nurse caller system is made, designed to expedite a swift and seamless setup process. This involved employing Bluetooth modules, specifically the MH-10, as both transmitter and receiver units, integrated with an ATMega8 microprocessor. Data processing was facilitated using an ATMega8 microcontroller, resulting in the display of characters on an LCD, activation of an LED, and initiation of a buzzer for medical assistance summoning.

In Al_Barazanchi et al.'s study [6], the cooperative routing protocol (CRP) was utilized to extend the lifespan of the network and improve the package delivery ratio (PDR) by reducing the End-to-End Delay (EED). EED served as a benchmark for surveying CRP inside WBAN steering frameworks. The execution of CRP driven to assisted parcel exchange and minimized bundle misfortune, advertising an improved EED inside the WBAN framework. Moreover, Ibrahim [7] pointed to raise the execution of WBAN systems. Their proposed strategy centered around developing an enlightening table specifying each sensor's operational parameters and transmission timings. The procedure was built and analyzed utilizing OMNET++, with the expanded throughput of IKS essentially moderating bundle misfortune and end-to-end idleness. This underscores how IKS bolsters network performance amidst WBAN devices, ultimately enhancing the efficiency of patient data transmission.

In Angurala's study [8], the integration of WSN and CC was explored, revealing two often-overlooked hurdles in their alignment: The impedance preventing cloud benefit clients (CSU) from accessing requisite services from the authentic CSP and the challenge for sensor network providers (SNP) to fulfill the CSP's demands. This reference delved into the attributes of CSP and SNP, CSU and CSP requirements, as well as aspects of cost, trust, and reputation in CSP and SNP management. A trust and reputation management framework were introduced to facilitate the coupling of cloud and sensor systems.

Addressing secure data transmission, Al Barazanchi et al. [9] analyzed an AI-fueled solution to encrypt biometric data, highlighting the significance of effective route selection and network architecture. The absence of signal redundancy led to facile network disconnections, which this study aimed to combat. By devising a network topology and connection strategy that minimizes interference and utilizes a broader frequency band, the study presented several algorithms and implementations to counter coverage and connectivity issues in the community spectrum.

Focusing on low-power devices and sensors, Alnawafleh et al. [10] introduced a novel framework to counteract route loss within WBAN, exemplified across three distinct scenarios where crucial human body data was captured to establish parameters. The study's simulations encompassed both on-body and intrabody communication, revealing an increase in route loss with distance and frequency.

Lastly, Bakar et al. [11] proposed an ANFIS classifier-based technique for sensor node (SN) classification, aiming to elevate the effectiveness of WBAN systems. The process involved feature extraction and categorization, ultimately optimizing the trust-related attributes of SNs through evolutionary algorithms.

Hernandez-Jaimes et al. [12] introduced an energy-conserving strategy for ensuring the secure transfer of patient information to medical authorities. To amplify the reliability of the system, the authors suggest a modified rendition of the "adhoc on-demand distance vector (AODV)" protocol, termed "RelAODV (Reliable AODV)." Noteworthy constraints encompass a fixed endpoint and a limited count of sensors. In an alternative source [13], an effective approach to message routing is unveiled, leveraging multiple hops and node categorization to alleviate sensor energy expenditure. This strategy caters to both the secure transmission of medical data and the augmentation of WBAN's dependability. To reinforce the reliability of WBAN communication, an arrangement for categorizing transmitted data is recommended, affording elevated safeguarding to vital communications in contrast to standard ones. This dynamic prioritization is implemented at WBAN's tier-2.

Qu et al. [14] put forth an "Energy-Efficient and Reliable Routing Scheme (ERRS)" designed to elevate the stability and trustworthiness of WBANs. ERRS encompasses the principles of "Forwarder Node Selection and Forwarder Node Rotation" and employs an adaptable static clustering routing mechanism to amplify stability and the enduringness of the network while optimizing reliability.

In another investigation [15], a non-preventative priority scheduling methodology is examined for WBANs, striving to truncate transmission duration and occurrences of data collision. In scenarios involving critical-rescue operations, the upsurge in control packets within the network escalates energy consumption and leads to longer WBAN waiting periods. The proposed approach empowers coordinators to elect channels based on priority, allocating heightened significance to critical and top-tier data signals and designating distinct static channels for individual users. This technique effectively reduces channel access time by dispatching small data packets to the coordinator at brief intervals, thus mitigating substantial collisions among adjacent WBANs.

Pal et al. [16] explored techniques for verifying authenticity within these networks, uncovering effective methods of unimodal and multimodal biometric identification based on facial and vocal traits. The research evaluates the suitability of cryptographic and non-cryptographic authentication for medical contexts, emphasizing that cryptographic-based methods might not align well with WBANs. In reference [17], an ingenious and energy-conscious design for WBANs is introduced to aid in diagnosing and monitoring COVID-19 patients. This strategy employs a machine learning model that sorts individuals into two categories—those with COVID-19 and those with a common cold—by analyzing the symptoms they transmit to the cloud.

In Selvaprabhu et al.'s study [18], a comprehensive M-Health system is presented, encompassing secure applications, enhanced cloud components, and predictive analyses driven by machine learning to enhance diagnostic capabilities. Data collected from sensor hubs navigates cellular systems to nearby databases some time recently being put away in cloud-based capacity administrations. In another scholarly study [19], an authentication algorithm is introduced, focusing on the Received Signal Strength Indication (RSSI), which is suitable for scenarios that require a discreet and inherent authentication approach characterized by low hardware costs and modest power consumption. This algorithm utilizes RSSI data from wireless devices to extract characteristics from radio channels that traverse the distance between wrists and waist. Also, reference [20] defines an optimized demonstrate for surveying dangers, depending on reasonable, noninvasive hazard markers. Different calculations are enrolled to decide an individual's vulnerability to creating heart illness [21-25]. WBANs go up against challenges with respect to believe, protection, and information consistency. Farther quiet observing requests certainty in substances and the unwavering quality of information. The scene envelops concerns such as security, compatibility, transferability, differences, bio-compatibility, and vitality effectiveness. Key management methodologies enhance the reliability and integrity of WBANs. However, conventional trust management methods often impose significant demands on resource-constrained WBANs. In response to these challenges, the proposed solution adopts ESVM to both identify and enhance the security of WBANs.

4. PROPOSED WORK

Figure 1 portrays a realistic representation of the proposed approach system. It diagrams the forms utilized in arrange to attain the categorization of dependable hubs interior the WBAN organize. This strategy requires rigorous data dealing with and preparing to realize exact and tried and true results.

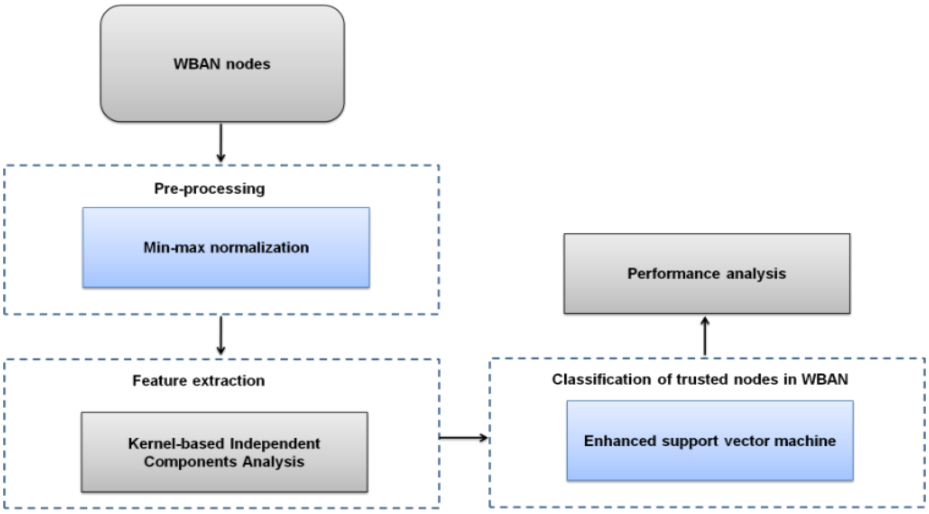
WBAN nodes
Pre-processing
Min-max normalization
Feature extraction
Kernel-based Independent Components Analysis
Classification of trusted nodes in WBAN
Enhanced support vector machine
Performance analysis

Figure 1. Suggested methodology framework

Step 1: Obtaining the SN dataset

The primary stage is procuring the sensor hub (SN) dataset, which contains basic data accumulated from the various hubs working interior the WBAN organize. This dataset serves as the premise for advance investigate and categorization.

Step 2: Data preparation

Utilizing min-max normalization some time recently starting the investigation

It is basic to normalize the information to a uniform scale in arrange to dodge any potential inclination caused by varying information ranges. This method is helped by min-max normalization, which guarantees that all information focuses drop interior a given extend, making strides the exactness and consistency of taking after forms.

Step 3: Extraction of dependable hub characteristics making utilize of kernel-based autonomous component examination (KICA).

The another step is to extricate fundamental characteristics related with reliable hubs within the WBAN arrange. This can be finished by utilizing KICA, a strategy planned to uncover basic designs and relationships in information. KICA permits for the disclosure of separating characteristics that contribute to categorizing hubs as dependable interior a organize.

The recently created field of WBANs, which is expected to convert healthcare and other businesses, is spoken to by the paper titled "Upgraded Bolster Vector Machine-Based Brilliantly Classification of Trusted Hubs in WBAN". The recognizable proof and classification of trusted hubs inside the arrange, a noteworthy trouble in WBANs, is tended to by this imaginative innovation. This innovation is based on the ESVM calculation, a headway of the well-known SVM strategy. By utilizing advanced include determination strategies and inventive optimization methods, ESVM progresses the hub classification process' precision and viability. The steadfastness and security of WBAN systems are expanded since of ESVM's expanded capacity to recognize complex designs and characteristics that set trusted hubs separated from others.

Data preprocessing alludes to the control of crude information to render it reasonable for consequent expository strategies. Customarily, this constitutes an essential stage going before the start of information investigation. A procedure known as Min-Max normalization is commonly utilized to directly change information inside a particular run. This strategy jam the characteristic connections between different information focuses whereas guaranteeing adherence to predefined bounds. The utilization of pre-established boundaries stands as an imperative approach in viably adjusting information for exact fitting. With this procedure to normalization, as appeared in Eq. (1):

$$Q' = \left(\frac{Q - min\ \_value\ of\ Q}{maxvalue\ of\ Q - min\ value\ of\ Q}\right) * (T - K) \tag{1}$$

The dataset has Min-Max scaling, and inside this scaling, one of the boundaries is characterized as [K, T]. Q symbolizes the first information run, while Q speaks to the changed information extend [26-32].

4.1 Feature extraction

The method of highlight extraction is pivotal to both information investigation and design acknowledgment. It involves the lessening of dimensionality whereas highlighting the foremost vital data from crude and complex data to display it in a arrange that's briefer and agent. Highlights are a condensed adaptation of the first data that keeps as it were the imperative aspects and takes off out any unessential or excess data [33, 34]. The most objective of highlight extraction is to extend the adequacy and proficiency of taking after information investigation errands counting modeling, clustering, and classification. The computing stack is diminished, and the analysis's precision is as often as possible expanded, by choosing and extricating basic features. A vital step in information investigation and design recognizable proof is include extraction, which compresses complex and crude information into a arrange that holds the foremost critical points of interest whereas bringing down dimensionality [35]. By emphasizing germane components, this condensed representation, or highlights, progresses explanatory exactness and proficiency. Selecting related and non-redundant characteristics, bringing down dimensionality for way better understanding, ensuring generalizability to unused information, and including space skill are critical variables to consider. Supported by strategies such as Vital Component Investigation (PCA), Free Component Investigation (ICA), and fact-finding, highlight extraction techniques that transform information into clear and interpretable structures have gained importance in various fields due to successful research and development. play a role. Support knowledge [11, 36]. This comprehensive strategy captures fundamental information contrasts to ensure relevance, eliminates redundancies that represent noise, reduces dimensionality for better understanding of high-dimensional raw data, we address important aspects such as achieving generalization for strong show-running on current and unused data sets. Tailoring spatial information to select important highlights for specific problem settings and spatial criteria. Techniques that contribute to this comprehensive approach include PCA, ICA, wavelet modification, fact measurement, and highlight scaling. Ultimately, raw data extraction is transformed into a system that enables effective exploration and design recognition [9, 37]. This is an urgent step to improve accuracy, proficiency, and interpretability across the space, from image recognition to processing common dialects. As indicated in Eq. (2), the input data is translated into an implicit feature space E through a nonlinear map function to fully leverage specific sequences correlations among spectral bands [38].

$$Y \in S^I \xrightarrow{\Phi} \in \Phi(Y) \in E \tag{2}$$

where x is a randomly generated vector in the input space S^I and $\Phi(Y)$ is its image in the feature space E. The feature space E has the potential to have substantially higher (perhaps infinite) dimensionality than its equivalent S^I.

To reconstitute the nonlinear independent components, we must first find a demixing matrix U_Φ in the feature space, as illustrated in Eq. (3) [39].

$$\hat{T}=U_\Phi(Y) \tag{3}$$

To make classical ICA estimate easier and better-conditioned, whiten the observed variables using PCA transform. KPCA in feature space E can be used to leverage high order correlation between spectral bands. Then, ICA is applied on the whitened data to identify nonlinear independent components.

4.2 Classification of trusted nodes in WBAN

The ESVM technique functions as a classification approach to differentiate among trustworthy nodes within the WBAN system. In the context of binary classification, the samples are partitioned by a hyperplane represented by the equation $x^U y+c=0$, where x is a coefficient vector in the space normal to the hyperplane, c is the origin's offset, and y denotes data points [40]. The primary aim of ESVM is to determine the values of x and c. For linear scenarios, the equation can be solved using Lagrangian multipliers. The data points lying along the outermost boundary are known as support vectors. Consequently, the solution for the equation x takes the form $x=\sum_{j=1}^{n} \alpha_j z_j y_j$, where n represents the total count of support vectors, and y_j signifies the labels for sample Y. By considering y_j as support vectors and observing that $y_j(x^U y_j+c)-1=0$, the value of c can be inferred. The linear discriminant function can be established once x and c have been determined in Eq. (4) [6, 41].

The function $h(y)$ is determined as

$$sgn(\sum_{j=1}^{n} \alpha_j z_j y_j^U y+c) \tag{4}$$

embodying the classification outcome. To address nonlinear scenarios, a bit approach is presented. The choice work can at that point be spoken to by Eq. (5).

$$h(y)= sgn(\sum_{j=1}^{n} \alpha_j z_j L(y_j,y)+c) \tag{5}$$

The ESVM classifier excels in managing multi-class separations, even when they're linearly complex. By utilizing SVM's bit procedure, the direct space is changed into a higher-dimensional space, empowering the classification of nonlinear input designs [42].

4.3 An algorithm for a WBAN based on ESVM

The calculation custom fitted for a WBAN grounded in ESVM presents a strong strategy to guarantee secure, dependable, and productive information transmission inside the organize. It utilizes ESVM's progressed capabilities to make strides the classification of hubs, including information procurement, preprocessing, include extraction, ESVM show preparing, approval, and real-time hub classification. This algorithm's sending upgrades the WBAN's in general security and unwavering quality, making it proficient at scholarly people categorizing hubs as dependable or not, eventually contributing to secure information communication and reliable arrange execution over differing applications. The ESVM-based calculation runs through a number of vital stages: The strategy starts with the collection of information from scattered sensor hubs inside the WBAN, at that point preprocessing to standardize and expel errors, which may incorporate commotion filtration, tending to lost values, and guaranteeing consistency. In arrange to recognize between trusted and untrusted hubs within the organize, key highlights are at that point extricated from the preprocessed information. KICA may at that point be utilized to find latent information designs. The most assignment of the calculation is to prepare the ESVM show utilizing these extricated highlights. It varies from other approaches in that it chooses and optimizes highlights and parameter values for improved classification precision. Measurements like exactness, review, and F1-score are utilized in approval to survey the strength of the show utilizing an untested dataset. Given a set of hubs inside the WBAN, a communication convention for information verification and encryption, and a security observing framework, the calculation points to distinguish a list of trusted hubs within the WBAN. The method includes initializing a purge list for trusted hubs and successively handling each hub: verifying it utilizing the communication convention and adding it to the trusted hubs list in the event that verification succeeds. Amid WBAN operation, the calculation persistently screens hub action through the security observing framework. In case suspicious behavior is detected from a hub, this can be detailed to the trusted hubs. Hence, the trusted hubs assess the detailed action and actualize suitable measures, such as barring the suspicious hub or re-authenticating it. Compromised or breaking down hubs are evacuated and supplanted with new ones. Guaranteeing progressing security, the calculation advocates for schedule upgrades of security conventions and calculations to counter advancing dangers. Customary security reviews and entrance tests are conducted to expeditiously distinguish and amend organize vulnerabilities. Eventually, the calculation outfits the list of trusted hubs as the yield, giving a solid establishment for secure WBAN operation.

5. RESULTS AND DISCUSSIONS

This investigate is centered on looking at 50 Sensor Hubs (SNs) that transmit information at a steady rate of 512 B per moment. Each SN advances bundles of 512 Bytes, went with by a 100 ms transmission hole between progressive cycles of information trade. The SNs depend on batteries with a beginning vitality capacity of 1000 J, empowering nonstop information transmission and gathering. This area presents a comparison between set up and imaginative approaches, evaluating their viability utilizing measurements like throughput, End-to-End Delay, bundle conveyance proportion (PDR), and precision. The set-up procedures envelop Choice Trees (DT), Fake Neural Systems (ANN), and Versatile Neuro-Fuzzy Induction Frameworks (ANFIS). PDR means the extent of effectively transmitted parcels from source to central controller hubs, measured in Kbps. The differentiate in PDR assessment between proposed and customary methodologies is visualized in Figure 2. The proposed Upgraded Bolster Vector Machine (ESVM) accomplishes a noteworthy PDR of 95%, eclipsing winning methods—ANFIS, DT, and ANN—with comparing scores of 67%, 76%, and 83%. This underscores the prevalent execution of ESVM in comparison to other accessible strategies.

The End-to-End Delay (EED) refers to the overall duration a packet takes to travel from the source Sensor Node (SN) to the central controller node, measured in milliseconds. A comparative analysis of EED assessment is depicted in Figure 3, showcasing the contrast between proposed and conventional strategies. The recommended Enhanced Support Vector Machine (ESVM) exhibits an EED of 73 ms, differing from the existing approaches—ANFIS, Decision Trees (DT), and Artificial Neural Networks (ANN)—which display respective EEDs of 91 ms, 89 ms, and 77 ms. In this aspect, ESVM presents a certain level of inferiority in relation to other available techniques. Nevertheless, it continues to demonstrate higher throughput when compared to the presently utilized methods.

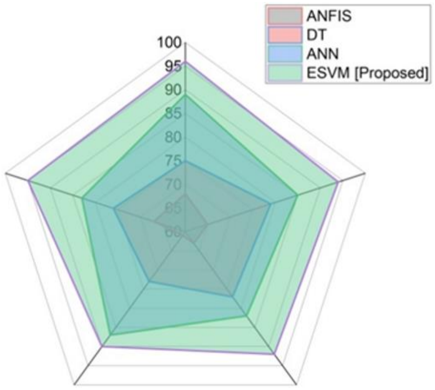

Figure 2. PDR evaluation in comparison between proposed and conventional methods

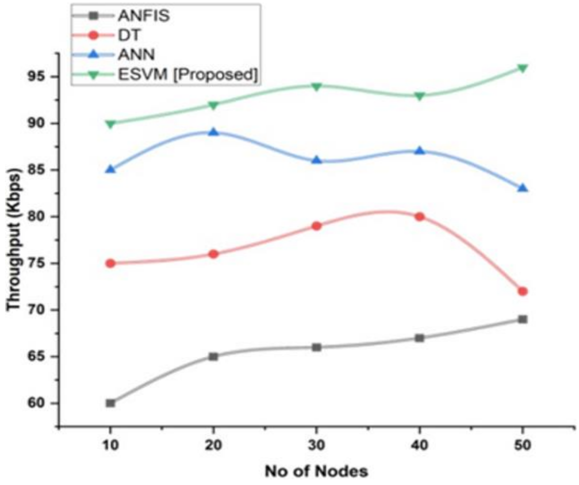

Figure 3. Comparative evaluation of throughput in suggested and traditional methods

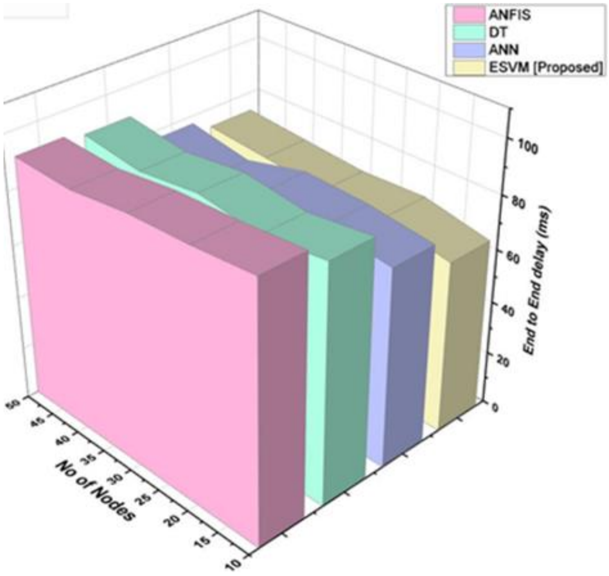

Figure 4. Comparative evaluation of EED in suggested and traditional methods

The total length of time a packet spends traveling from the source SN to the main controller node is known as the EED. Milliseconds are used to measure it. The comparison of the evaluation of EED using recommended and conventional approaches is shown in Figure 4. The suggested ESVM have 73 ms as opposed to the present techniques ANFIS, DT, and ANN, which have 91 ms, 89 ms, and 77 ms, respectively. ESVM is weak in comparison to other available methods.

Accuracy is defined as the ratio of correctly predicted events, whether positive or negative, to all cases. It is described in percentage form. Figure 5 illustrates a comparison of the recommended and traditional approaches' accuracy. The current methods ANFIS, DT, and ANN, which have 80%, 84%, and 82%, respectively, each have a lower score than the suggested ESVM, which has 85%. ESVM is a highly accurate method when compared to other ones currently in use.

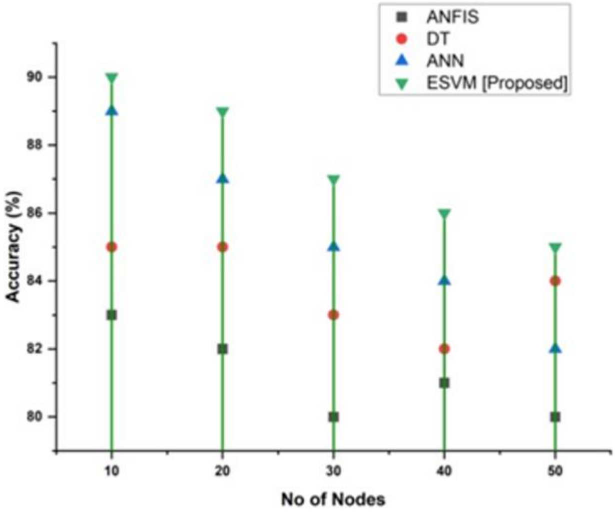

Figure 5. Accuracy evaluation in comparison between proposed and conventional methods

The ANFIS technique's limitation lies in its susceptibility to untrusted Sensor Nodes (SNs), affecting the broader performance of the WBAN network. On the other hand, Decision Trees (DT) suffer from instability, posing a notable drawback. Artificial Neural Networks (ANNs) demand substantial computational resources and often lack interpretability, making their application intricate. Moreover, training a neural network necessitates a substantial volume of data.

6. CONCLUSION

Utilizing Improved Bolster Vector Machine (ESVM) for the classification of trusted hubs inside a Remote Body Region Arrange (WBAN) presents a promising approach. This cleverly technique leverages numerous highlights, counting flag quality, separate, and battery control, to discover the validity of hubs inside the arrange. This approach holds the potential to set up secure and tried and true communication among WBAN hubs, a vital prerequisite in restorative settings. By the by, approving the approach's adequacy in real-world scenarios and evaluating its execution beneath different arrange conditions requires assist examination. Its growing importance and increasing therapeutic applications eventually increased its fame. Information security is a key concern because the understanding of the information depends on the operation of his WBAN system. the ESVM show is conveyed to classify hubs inside the WBAN arrange. To gage the model's adequacy in distinguishing potential candidates, the results are evaluated utilizing measures like exactness, review, and the F1-score. A comprehensive paper for the most part follows to the consequent A strong security system is required to ensure secure information exchange between the SN and other his WBAN systems. In this study, his ESVM is introduced as a classification strategy to discover trusted hubs within WBAN systems, and kernel-based free component analysis is used for include extraction. The main parameter values of counting throughput (96 Kbit/s), EED (73 ms), PDR (95%), and accuracy (85%) were determined by the system. A confinement lies within the moderately unassuming dataset utilized within the consider; extending the dataset through advance information collection rises as future work to increase the recommended system's execution potential.

ACKNOWLEDGEMENTS

Most frequently, acknowledgements of sponsors and financial support are given to the authors, along with their appreciation.

REFERENCES

[1] Pregnolato, M., Gunner, S., Voyagaki, E., De Risi, R., Carhart, N., Gavriel, G., Tully, P., Tryfonas, T., Macdonald, J., Taylor, C. (2022). Towards civil engineering 4.0: Concept, workflow and application of digital twins for existing infrastructure. Automation in Construction, 141: 104421. https://doi.org/10.1016/j.autcon.2022.104421

[2] Singla, R., Kaur, N., Koundal, D., Bharadwaj, A. (2022). Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. Wireless Personal Communications, 122: 1767-1806. https://doi.org/10.1007/s11277-021-08969-0

[3] Almuhaideb, A.M., Alghamdi, H.A. (2022). Secure and efficient WBAN authentication protocols for intra-BAN tier. Journal of Sensor and Actuator Networks, 11(3): 44. https://doi.org/10.3390/jsan11030044

[4] Kaur, K., Kaur, A., Gulzar, Y., Gandhi, V. (2024). Unveiling the core of IoT: Comprehensive review on data security challenges and mitigation strategies. Frontiers in Computer Science, 6: 1420680. https://doi.org/10.3389/fcomp.2024.1420680

[5] Al-Suhimat, R.I., Mohammed AI, N., Ibrahim, A., Maaitah, N.O., Al-Dmour, N.A. (2024). Review of security challenges encountered in Internet of Things Technology. In 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, pp. 1-6. https://doi.org/10.1109/ICCR61006.2024.10533052

[6] Al_Barazanchi, I., Shibghatullah, A.S., Selamat, S.R. (2017). A new routing protocols for reducing path loss in wireless body area network (WBAN). Journal of Telecommunication, Electronic and Computer Engineering, 9(1-2): 93-97.

[7] Ibrahim, A. (2024). Guarding the future of gaming: The imperative of cybersecurity. In 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, pp. 1-9, http://doi.org/10.1109/ICCR61006.2024.10532843

[8] Angurala, M., Bala, M., Singh, P. (2023). IoT-based healthcare systems and their security concerns. In Computational Health Informatics for Biomedical Applications, pp. 1-25, Apple Academic Press.

[9] Al Baeazanchi, I., Abdulshaheed, H.R., Shawkat, S.A., Selamat, S.R.B. (2019). Identification key scheme to enhance network performance in wireless body area network. Periodicals of Engineering and Natural Sciences, 7(2): 895-906. http://doi.org/10.21533/pen.v7i2.606

[10] Alnawafleh, N.M., Ibrahim, A., Pradhan, M.R. (2024). Review of the mechanisms used to protect the big data from attacks. In 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, pp. 1-4, http://doi.org/10.1109/ICCR61006.2024.10533073

[11] Bakar, K.B.A., Zuhra, F.T., Isyaku, B., Sulaiman, S.B. (2023). A review on the immediate advancement of the Internet of Things in wireless telecommunications. IEEE Access, 11: 21020-21048. https://doi.org/10.1109/ACCESS.2023.3250466

[12] Hernandez-Jaimes, M.L., Martinez-Cruz, A., Ramírez-Gutiérrez, K.A., Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. Internet of Things, 23: 100887. https://doi.org/10.1016/j.iot.2023.100887

[13] Kalaiselvi, K., Suresh, G.R., Ravi, V. (2019). Genetic algorithm based sensor node classifications in wireless body area networks (WBAN). Cluster Computing, 22(S5): 12849-12855. https://doi.org/10.1007/s10586-018-1770-6

[14] Qu, Y., Zheng, G., Wu, H., Ji, B., Ma, H. (2019). An energy-efficient routing protocol for reliable data transmission in wireless body area networks. Sensors, 19(19): 4238. https://doi.org/10.3390/s19194238

[15] Ghadi, Y.Y., Mazhar, T., Aurangzeb, K., Haq, I., Shahzad, T., Laghari, A.A., Anwar, M.S. (2024). Security risk models against attacks in smart grid using big data and artificial intelligence. PeerJ Computer Science, 10: e1840.

[16] Pal, S., Jhanjhi, N.Z., Abdulbaqi, A.S., Akila, D., Almazroi, A.A., Alsubaei, F.S. (2023). A hybrid edge-cloud system for networking service components optimization using the internet of things. Electronics, 12(3): 649. https://doi.org/10.3390/electronics12030649

[17] Ullah, F., Khan, M. Z., Faisal, M., Rehman, H.U., Abbas, S., Mubarek, F.S. (2021). An energy efficient and reliable routing scheme to enhance the stability period in wireless body area networks. Computer Communications, 165: 20-32. https://doi.org/10.1016/j.comcom.2020.10.017

[18] Selvaprabhu, P., Chinnadurai, S., Tamilarasan, I., Venkatesan, R., Kumaravelu, V.B. (2022). Priority-based resource allocation and energy harvesting for WBAN smart health. Wireless Communications and Mobile Computing, 2022(1): 8294149. https://doi.org/10.1155/2022/8294149

[19] Alzuabi, W., Elmedany, W., Saeed, M.S. (2023). Using machine learning for security issues in cognitive IoT. In 7th IET Smart Cities Symposium (SCS 2023), Hybrid Conference, Bahrain, pp. 512-520. https://doi.org/10.1049/icp.2024.0980

[20] El-Bendary, M.A.M., Kasban, H., Haggag, A. (2020). Investigating of nodes and personal authentications utilizing multimodal biometrics for medical application of WBANs security. Multimedia Tools and Applications, 79: 24507-24535. https://doi.org/10.1007/s11042-020-08926-2

[21] Pal, S., Jhanjhi, N.Z., Abdulbaqi, A.S., Akila, D., Alsubaei, F.S., Almazroi, A.A. (2023). An intelligent task scheduling model for hybrid Internet of Things and cloud environment for big data applications. Sustainability, 15(6): 5104. https://doi.org/10.3390/su15065104

[22] Bilandi, N., Verma, H.K., Dhir, R. (2021). An intelligent and energy-efficient wireless body area network to control coronavirus outbreak. Arabian Journal for Science and Engineering, 46(9): 8203-8222. https://doi.org/10.1007/s13369-021-05411-2

[23] Qureshi, K.N., Din, S., Jeon, G., Piccialli, F. (2020). An accurate and dynamic predictive model for a smart M-Health system using machine learning. Information Sciences, 538: 486-502. https://doi.org/10.1016/j.ins.2020.06.025

[24] Mohamed, M., Cheffena, M. (2018). Received signal strength based gait authentication. IEEE Sensors Journal, 18(16): 6727-6734. https://doi.org/10.1109/JSEN.2018.2850908

[25] Mahmoud, H.H., Al_Shammari, M.K.M., Hameed, I.M., Al-Barazanchi, I.I., Sekhar, R., Shah, P., Solke, N. (2024). Eco-friendly and secure data center to detection compromised devices utilizing swarm approach. International Journal of Intelligent Engineering and Systems, 17(3): 102-115. http://doi.org/10.22266/ijies2024.0630.09

[26] Ramkumar, A., Kulkarni, P., Obaid, A.J., Abdulbaqi, A.S., Yakin, A.A. (2023). Big data analytics and its application in E-commerce. AIP Conference Proceedings, 2736(1). https://doi.org/10.1063/5.0170687

[27] Asha, A., Arunachalam, R., Poonguzhali, I., Urooj, S., Alelyani, S. (2023). Optimized RNN-based performance prediction of IoT and WSN-oriented smart city application using improved honey badger algorithm. Measurement, 210: 112505.

[28] Salih, S.Q., Alsewari, A.A., Yaseen, Z.M. (2019). Pressure vessel design simulation: Implementing of multi-swarm particle swarm optimization. In Proceedings of the 2019 8th International Conference on Software and Computer Applications, Penang, Malaysia, pp. 120-124. https://doi.org/10.1145/3316615.3316643

[29] Salih, S.Q. (2019). A new training method based on black hole algorithm for convolutional neural network. Journal of Southwest Jiaotong University, 54(3): 22. https://doi.org/10.35741/issn.0258-2724.54.3.22

[30] Malik, A., Rai, P., Heddam, S., Kisi, O., Sharafati, A., Salih, S.Q., Al-Ansari, N., Yaseen, Z.M. (2020). Pan evaporation estimation in Uttarakhand and Uttar Pradesh States, India: Validity of an integrative data intelligence model. Atmosphere, 11(6): 553. https://doi.org/10.3390/atmos11060553

[31] Tao, H., Awadh, S.M., Salih, S. Q., Shafik, S.S., Yaseen, Z.M. (2022). Integration of extreme gradient boosting feature selection approach with machine learning models: Application of weather relative humidity prediction. Neural Computing and Applications, 34(1): 515-533. https://doi.org/10.1007/s00521-021-06362-3.

[32] Agarwal, P., Idrees, S.M., Obaid, A.J., Abdulbaqi, A.S., Mahmood, S.D. (2022). An effective diagnostic framework for COVID-19 using an integrated approach. In Next Generation of Internet of Things: Proceedings of ICNGIoT 2022, pp. 129-141. https://doi.org/10.1007/978-981-19-1412-6_11

[33] Malik, A., Kumar, A., Kisi, O., Khan, N., Salih, S.Q., Yaseen, Z.M. (2021). Analysis of dry and wet climate characteristics at Uttarakhand (India) using effective drought index. Natural Hazards, 105: 1643-1662. https://doi.org/10.1007/s11069-020-04370-5

[34] Ismail, I., Iksan, N., Subramaniam, S.K., Abdulbaqie, A.S., Pillai, S.K., Panessai, I.Y. (2021). Usefulness of augmented reality as a tool to support online learning. Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, 7(2): 277-285

[35] Tao, H., Al-Sulttani, A.O., Salih Ameen, A.M., Ali, Z.H., Al-Ansari, N., Salih, S.Q., Mostafa, R.R. (2020). Training and testing data division influence on hybrid machine learning model process: Application of river flow forecasting. Complexity, 2020(1): 8844367. https://doi.org/10.1155/2020/8844367

[36] Sinha, S., Gochhait, S., Obaid, A.J., Abdulbaqi, A.S., Alwan, W., Mahdi, M.I., Muthmainnah. (2023). Internet of things (IoT) enabled healthcare system for tackling the challenges of Covid-19 – A bibliometric study. AIP Conference Proceedings, 2736(1). https://doi.org/10.1063/5.0170680

[37] Karimi, B., Mohammadi, P., Sanikhani, H., Salih, S.Q., Yaseen, Z.M. (2020). Modeling wetted areas of moisture bulb for drip irrigation systems: An enhanced empirical model and artificial neural network. Computers and Electronics in Agriculture, 178: 105767. https://doi.org/10.1016/j.compag.2020.105767

[38] Islam, U., Muhammad, A., Mansoor, R., Hossain, M.S., Ahmad, I., Eldin, E.T., Khan, J.A., Rehman Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models. Sustainability, 14(14): 8374. https://doi.org/10.3390/su14148374

[39] Cui, F., Salih, S.Q., Choubin, B., Bhagat, S.K., Samui, P., Yaseen, Z.M. (2020). Newly explored machine learning model for river flow time series forecasting at Mary River, Australia. Environmental Monitoring and Assessment, 192: 761. https://doi.org/10.1007/s10661-020-08724-1

[40] Hussain, M., Mehmood, A., Khan, S., Khan, M.A., Iqbal, Z. (2019). Authentication techniques and methodologies used in wireless body area networks. Journal of Systems Architecture, 101: 101655. https://doi.org/10.1016/j.sysarc.2019.101655

[41] Hai, T., Bhuiyan, M.Z.A., Wang, J., Wang, T., Hsu, D. F., Li, Y., Salih, S.Q., Wu, J., Liu, P. (2020). DependData: Data collection dependability through three-layer decision-making in BSNs for healthcare monitoring. Information Fusion, 62: 32-46. https://doi.org/10.1016/j.inffus.2020.03.004

[42] Salih, S.Q., Habib, M., Aljarah, I., Faris, H., Yaseen, Z. M. (2020). An evolutionary optimized artificial intelligence model for modeling scouring depth of submerged weir. Engineering Applications of Artificial Intelligence, 96: 104012. https://doi.org/10.1016/j.engappai.2020.104012