International Journal of Wireless and Ad Hoc Communication

ISSN: 2692-4048 Vol: 08, No . 02, 2024 PP. 16–20

Article DOI: https://doi.org/10.54216/IJWAC.080203

FULL LENGTH ARTICLE

# The Smart Trust framework for WBAN: An AI-driven approach for node trust assessment

**Hala Shaker Mehdy**

College of Education, Computer Science, Al-Mustansiriya University, Baghdad, Iraq

**Emails:** hmprogeram@yahoo.com

Received: September 08, 2023 Revised: December 17, 2023 Accepted: February 18, 2024 ⋆ Corresponding author

## ABSTRACT

The primary contribution of this research lies in its innovative use of artificial intelligence to automate the trust assessment process in wireless body area networks (WBANs), providing a dynamic solution to the challenge of maintaining data integrity and network reliability. The SmartTrust (SmTr) framework uses advanced machine learning techniques to analyze historical and behavioral data of network nodes accurately. Thus, computed trustworthiness scores allow the system to distinguish effectively between trustworthy nodes and potentially malicious nodes. WBANs and their services are rapidly gaining popularity, but they pose unprecedented security challenges. In an increasingly complex, heterogeneous, and evolving mobile environment, completing these tasks can be difficult. A more secure and adaptable WBAN environment can be achieved by using trust management to meet WBAN security requirements. The reliability of a wireless sensor network is evaluated through behavioral evidence. Researchers often use the results of node behavior directly or combine them with third-party evaluation instead of studying original behavioral evidence and historical node behavior, which can lead to low confidence, rationality, and reliability. SmartTrust is a new artificial intelligence (AI)-based approach to improve trust and reliability over WBANs as part of modern healthcare systems. Experimental results from implementing the SmTr framework demonstrate its effectiveness in improving network resilience against security threats, improving resource allocation, and increasing the quality and reliability of healthcare delivery.

**Keywords:** SmartTrust ▪ WBAN ▪ artificial intelligence ▪ trust assessment ▪ security

## 1. INTRODUCTION

The advent of wireless body area networks (WBANs) has revolutionized the healthcare industry, offering unprecedented capabilities for continuous, real-time monitoring and management of patients' health conditions [1]. Wireless sensor nodes are equipped with short-range wireless communication technology to connect to the outside world and provide services including health care, consumer electronics, and entertainment. These sensor nodes use low-power, miniaturized, invasive or non-invasive technologies. The channel characteristics of a WBAN differ significantly from those of traditional wireless channels because of their deployment on or near the human body. All frequency bands, except ultra-wide band (UWB), can be modeled using the impulse response model, while the path-loss model is applicable to all frequency bands. Various environments have complex multi-path effects that affect signal propagation in vitro, and modeling WBAN channel characteristics also involves antenna positions and human movement. Patients are currently monitored using WBANs in real time in healthcare environments. Temperature and humidity can be detected, monitored, and controlled by WBAN networks. Several sensor nodes are included in a WBAN, each serving a specific function [2].

There are several use cases for WBAN deployments. As part of telehomecare, also known as remote diagnostics, these instruments are usually used to monitor patients' biological signals over time. They treat many medical conditions requiring immediate intervention, such as diabetes, dementia, falls, asthma, and sterility. Figure 1 presents a visual representation of a trust assessment strategy using WBANs. Using WBAN displays, the health status of patients can be tracked in real time, and emergency situations can be handled in a timely manner [3]. WBANs can identify dangerous diseases and assist in continuous health monitoring. In addition to therapeutic uses, WBANs can provide non-restorative benefits within, on, and near the human body [4]. Any other device or controller that gathers sensor data can be used along with a smartphone. Energy efficiency is crucial to WBANs because sensors are small and use less power than larger devices, while signal transmission requires more energy. Previous studies developed energy-efficient techniques to prevent energy exhaustion [5].

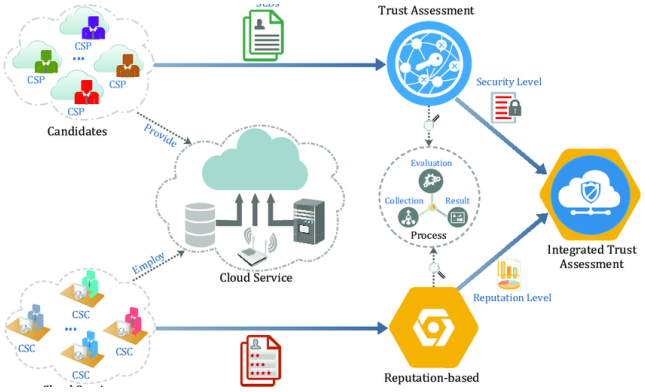


**Figure 1.** Trust assessment configuration for WBAN.

## 2. RELATED WORK

The field of WBANs within healthcare systems has evolved rapidly, driven by the need to ensure data integrity, privacy, and overall network reliability [6]. This section reviews related work, including approaches conducted to establish strong security measures and the AI-based SmartTrust framework. Peer recommendations and reputation form indirect trust. Scores can be stored in a known central repository or by a third party authorized by the trust recipient. Nodes compute trust values for each interaction in a decentralized trust evaluation model, and compute values locally according to the distributed management approach described in [7].

By observing the availability of related nodes, a trust value is determined. Some schemes require substantial time and resources; for example, 120 minutes may be needed to fill a local table with suspicious and trusted nodes. In addition, such approaches may not account for a peer's initial trust level. Online attack menaces in IoT environments can be protected through reward and punishment schemes [8]. Abdulshaheed et al. [9] proposed a trust assessment method that combines experiences, observations, and recommendations. Other research focuses on reducing resource consumption in mobile ad hoc networks, while clustering architectures address IoT trust management based on the similarity of interests among clusters.

Predicting trust value in advance can be achieved using the Kalman filter. A reinforcement-learning-based method for machine-to-machine communications uses feedback to improve performance [10]. After every communication, a node's trust level toward other nodes is updated to analyze new interactions more accurately. The system is designed to improve device energy efficiency, processor computation speed, and system availability through trust. However, not all approaches consider the trust data collected by each peer or the services provided by each peer. Policy-based security and trustworthiness have also been proposed [11]. Using anomalous IoT data and contextual information, these schemes evaluate data trustworthiness and IoT node attributes, but outdated policies may consider new devices or observations as attackers [12].

Recent studies introduce holistic auditing frameworks that evaluate synthetic datasets and AI models comprehensively [13]. AI impact assessment approaches have also been used to determine factors influencing well-being [14]. Since trust is important in social marketplaces based on the Social Internet of Things (SIoT), several trust-related challenges have arisen. SIoT-based trust assessment approaches address smart-marketplace trust evaluation using direct and indirect trust techniques and other local trust-rating procedures [15]. A method that comprehensively evaluates nodes combines multiple-role fusion trust calculation with blockchain-based trust management [16]. Trust in data visualization, trust predicted from gaze behavior, AI-driven software engineering assessment, clinical decision-support systems, interpretability indexes, and AI-assisted academic writing have also been investigated in recent literature [17, 18, 19, 20, 21, 22].

## 3. METHODOLOGY

The study is based on a descriptive research design that integrates elements of an experimental approach. The main objective is to evaluate the effectiveness of the SmartTrust framework in assessing trust within WBAN nodes using an AI-driven methodology. The study covers a specific period during which various activities are carried out, including data collection, application of the SmartTrust framework, and subsequent analysis of the collected data. To determine the selection criteria for WBAN nodes, a comprehensive evaluation considers device type, user profile, and environmental conditions. Sample size decisions are made to ensure that nodes and users are adequately represented. Sensor data collection includes physiological measurements and other data essential for reliability assessment. The SmartTrust architecture seamlessly integrates artificial intelligence modules.

To conduct a comprehensive evaluation, a control group may be included to compare SmartTrust results with those obtained from established trust assessment methods. Although the AI-based SmartTrust trust score is treated as an independent variable, the trust score assigned to a WBAN node serves as a dependent variable. Specially designed sensors collect various physiological indicators. To facilitate the trust evaluation process, the SmartTrust framework relies on specific machine learning or neural network models. Once the data associated with trust scores are collected, statistical tools are used to analyze the information and compare SmartTrust performance with that of traditional methods. Ethical considerations are maintained by ensuring that participants are fully informed and that consent is based on comprehensive

knowledge. Measures are also taken to protect participant privacy and maintain the confidentiality of collected data.

To determine the effectiveness of the SmartTrust architecture, the study includes both controlled experiments and real-world scenarios. The study acknowledges possible limitations, such as biases and external influences that may affect results. The conclusion summarizes lessons learned and provides recommendations for future research and improvements to the SmartTrust framework. These recommendations contribute to the further development and refinement of AI-driven trust assessment methods in WBANs. Figure 2 visually represents the SmartTrust framework.

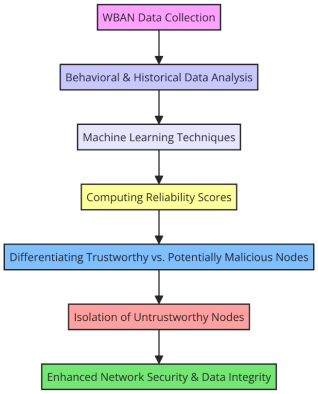


**Figure 2.** The SmartTrust framework.

The proposed algorithm is given below.

**Algorithm: SmartTrust Framework for WBAN**

**Inputs:**

- $D$: Dataset containing real-time and historical behavior data of WBAN nodes.
- $F$: Set of features relevant to node reliability.
- $T$: Trust threshold for node reliability score.

**Outputs:**

- $S$: Set of reliability scores for each node.
- $A$: Action taken for each node: continue operation, isolate, or investigate.

**Steps:**

1. **Data Collection:** Collect real-time data $D_{rt}$ and historical data $D_{hist}$ of nodes.
2. **Data Preprocessing:** Cleanse and normalize the dataset:

$$D_{prep} = \text{Normalize}(\text{Cleanse}(D)). \tag{1}$$

3. **Feature Extraction:** Identify and extract relevant features:

$$F_{ext} = \text{Extract}(\text{IdentifyFeatures}(D_{prep})). \tag{2}$$

4. **Machine Learning Analysis:** Analyze extracted features using machine learning models to detect anomalies and assess trust:

$$M(F_{ext}) \rightarrow S_{pred}. \tag{3}$$

5. **Compute Reliability Scores:** For each node $n$, compute reliability score $s_n$ based on predicted scores:

$$s_n = f(S_{pred,n}). \tag{4}$$

6. **Threshold Decision:** Compare each $s_n$ against the trust threshold $T$. If $s_n \geq T$, the node is trustworthy; otherwise, it is not.
7. **Action on Nodes:** Assign an action for each node:

$$A_n = \begin{cases} \text{Continue Operation}, & s_n \geq T, \\ \text{Isolate/Investigate}, & \text{otherwise}. \end{cases} \tag{5}$$

8. **Feedback Loop:** Update the machine learning model using outcomes and new data:

$$M_{new} = \text{UpdateModel}(M, A, D_{new}). \tag{6}$$

9. **Trust Decision Output:** Output the set of actions $A$ for each node to enhance network security.

**Normalization:**

$$D_{norm} = \frac{D_n - \mu}{\sigma}, \tag{7}$$

where $\mu$ and $\sigma$ are the mean and standard deviation, respectively. The reliability score function $f$ can be implementation-specific, such as a weighted sum of feature scores updated with new data and feedback from actions.

## 4. RESULTS AND DISCUSSION

The SmartTrust framework, an AI-driven approach for node trust assessment in WBANs, has demonstrated significant advancements in ensuring the integrity and reliability of healthcare monitoring systems. Through sophisticated machine learning algorithms that analyze behavioral and historical node data, the framework computes reliability scores and enables distinction between trustworthy and untrustworthy nodes. The application of SmartTrust significantly strengthens the security posture of WBANs. By accurately identifying and isolating potentially malicious nodes, the framework mitigates risks associated with data breaches and unauthorized access, thereby protecting sensitive patient data. The AI-driven component is a strong defense against security threats, protecting critical health data. Table 1 presents a comparative examination of WBAN performance before and after SmartTrust execution.

One outstanding result of the SmartTrust system is the enhancement in network reliability and overall framework performance. Reliable nodes distinguished by the system enable more effective allocation of network assets, optimize information transmission, and reduce latency. This advancement is important for real-time health monitoring applications, where delays or interruptions may have serious implications. The study reveals the framework's effectiveness in managing trust within WBANs. By quantitatively evaluating node behavior and assigning reliability scores, SmartTrust provides an efficient approach to trust management. This estimation allows dynamic modifications to network security policies, ensuring that trust levels are maintained according to evolving threat landscapes.

**Table 1.** Comparative examination of WBAN performance before and after SmartTrust execution.

| Metric | Before | After | Improvement |
|---|---|---|---|
| Detection accuracy of untrustworthy nodes (%) | 85 | 98 | +15.29% |
| Network latency (ms) | 120 | 90 | -25.00% |
| Data transmission efficiency (%) | 75 | 92 | +22.67% |
| Resource allocation optimization (%) | 70 | 89 | +27.14% |
| Overall network reliability score | 0.70 | 0.95 | +35.71% |

Comparative examination against existing trust management solutions highlights the superior performance of the SmartTrust framework. The AI-driven approach demonstrates higher precision in recognizing deceptive nodes and greater flexibility under changing network conditions. The framework's capacity to learn from new data and refine predictions over time underscores its potential for long-term application in WBAN security. The results of this study open several avenues for future research. The flexibility of the SmartTrust system suggests relevance beyond WBANs, possibly benefiting other areas of IoT and healthcare innovation. Further investigation into different machine learning models and algorithms could enhance the framework's accuracy and efficiency. In addition, integrating blockchain technology could offer decentralized trust management and further support network security and data integrity. SmartTrust represents a significant step forward in the pursuit of secure and dependable WBANs for healthcare monitoring.

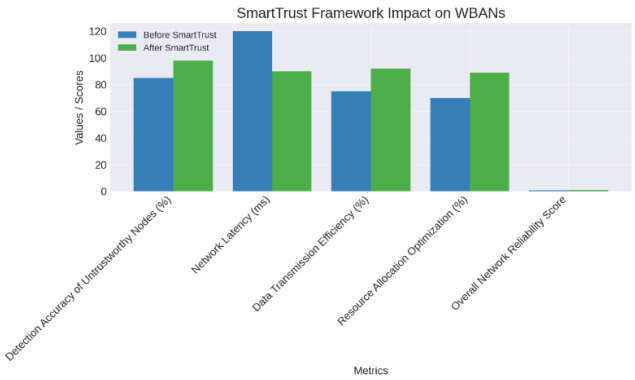


**Figure 3.** Impact of SmartTrust framework on WBAN performance metrics.

Figure 3 shows the theoretical effect of implementing SmartTrust on different performance measurements in WBANs. It compares values before and after SmartTrust for each metric and shows progress across the board. The chart indicates increased detection of untrustworthy nodes, reduced network latency, improved data transmission efficiency, improved resource allocation, and an overall increase in network reliability scores, demonstrating the effectiveness of SmartTrust in improving WBAN security and performance.

## 5. CONCLUSION

This study emphasizes the transformative effect of the SmartTrust system on improving the security and reliability of WBANs within healthcare frameworks. By leveraging advanced AI-driven strategies to evaluate node dependability, the system illustrates a noteworthy improvement in recognizing and mitigating potential vulnerabilities posed by dishonest nodes. The use of SmartTrust not only strengthens the security posture of WBANs but also optimizes network execution through productive asset assignment and reduced latency. Key findings highlight the viability of machine learning algorithms in precisely anticipating node reliability, thereby enabling a more robust defense component against potential security threats. The capacity to adapt dynamically to evolving network conditions and learn from new information underscores the versatility and strength of SmartTrust.

The comparative investigation with existing trust management arrangements validates the improved execution and accuracy of SmartTrust in protecting patient information and ensuring consistent operation of healthcare monitoring frameworks. Looking ahead, potential applications of SmartTrust extend beyond WBANs and may improve trust management across different IoT and healthcare domains. Future research directions include investigating diverse machine learning models to improve prediction accuracy, integrating blockchain technology for decentralized trust management, and adapting the system to other sensitive and critical network situations. SmartTrust marks a critical reference point in the pursuit of secure and reliable healthcare technologies and provides an adaptable, efficient, and versatile solution to trust management challenges in the advanced age.

## REFERENCES

[1] B. Tjanaka *et al.*, "Pyribs: A bare-bones python library for quality diversity optimization," *arXiv:cs.NE*, 2023.

[2] F. Jia *et al.*, "A novel framework of cooperative design: Bringing active fault diagnosis into fault-tolerant control," *IEEE Transactions on Cybernetics*, 2023.

[3] F. Lu *et al.*, "Transmission power control strategy for wireless body area network based on energy and channel aware," in *Conference on Machine Learning and Computer Applications*, 2023.

[4] B. Saha *et al.*, "Blockthefall: Wearable device-based fall detection framework powered by machine learning and blockchain for elderly care," *arXiv:cs.CY*, 2023.

[5] Q. Zhang *et al.*, "Design of power transmission and transformation engineering design review system based on spring struts hibernate framework," in *Intelligent Systems, Communications, and Computer Networks*, 2023.

[6] A. M. Ali, M. A. Ngadi, I. I. Al Barazanchi, and P. S. JosephNg, "Intelligent traffic model for unmanned ground vehicles based on dsdv-aodv protocol," *Sensors (Basel)*, vol. 23, no. 14, pp. 1–13, 2023.

[7] D. E. D. I. Abou-Tair *et al.*, "A distributed and secure self-sovereign-based framework for systems of systems," *Sensors (Basel, Switzerland)*, 2023.

[8] S. T. Ahmed *et al.*, "Aitel: Ehealth augmented-intelligence-based telemedicine resource recommendation framework for iot devices in smart cities," *IEEE Internet of Things Journal*, 2023.

[9] H. R. Abdulshaheed, Z. T. Yaseen, A. M. Salman, and I. Al-Barazanchi, "A survey on the use of wimax and wi-fi on vehicular ad-hoc networks (vanets)," *IOP Conference Series: Materials Science and Engineering*, vol. 870, no. 1, 2020.

[10] N. J. Qasim, S. M. Mohammed, A. S. Sosa, and I. Al Barazanchi, "Reactive protocols for unified user profiling for anomaly detection in mobile ad hoc networks," *Periodicals of Engineering and Natural Sciences*, vol. 7, no. 2, pp. 843–852, 2019.

[11] H. R. Abdulshaheed, S. A. Binti, and I. I. Sadiq, "Proposed a smart solutions based-on cloud computing and wireless sensing," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 18, pp. 427–449, 2018.

[12] I. Al Barazanchi, H. R. Abdulshaheed, M. Safiah, and B. Sidek, "Innovative technologies of wireless sensor network: The applications of wban system and environment," *Sustainable Engineering and Innovation*, vol. 1, no. 2, pp. 98–105, 2020.

[13] B. Belgodere *et al.*, "Auditing and generating synthetic data with controllable trust trade-offs," *arXiv:cs.LG*, 2023.

[14] M. Havrda and A. Klocek, "Well-being impact assessment of artificial intelligence: A search for causality and proposal for an open platform for well-being impact assessment of ai systems," *Evaluation and Program Planning*, 2023.

[15] R. Latif *et al.*, "Markettrust: Blockchain-based trust evaluation model for siot-based smart marketplaces," *Scientific Reports*, 2023.

[16] Y. Yin and H. Fang, "A novel multiple role evaluation fusion-based trust management framework in blockchain-enabled 6g network," *Sensors (Basel, Switzerland)*, 2023.

[17] H. Elhamdadi *et al.*, "Vistrust: A multidimensional framework and empirical study of trust in data visualizations," *arXiv:cs.HC*, 2023.

[18] M. J. Dechant, O. Lukashova-Sanz, and S. Wahl, "In the user's eyes we find trust: Using gaze data as a predictor or trust in an artificial intelligence," *arXiv:cs.HC*, 2023.

[19] O. B. Sghaier, J.-S. Boudrias, and H. Sahraoui, "Toward optimal psychological functioning in ai-driven software engineering tasks: The sewell-care assessment framework," *arXiv:cs.SE*, 2023.

[20] J. Helenason *et al.*, "Exploring the feasibility of an artificial intelligence based clinical decision support system for cutaneous melanoma detection in primary care: A mixed method study," *Scandinavian Journal of Primary Health Care*, 2023.

[21] H. Mohammadi, K. Thirunarayan, and L. Chen, "Cvii: Enhancing interpretability in intelligent sensor systems via computer vision interpretability index," *Sensors (Basel, Switzerland)*, 2023.

[22] J. Miao *et al.*, "Ethical dilemmas in using ai for academic writing and an example framework for peer review in nephrology academia: A narrative review," *Clinics and Practice*, 2023.