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
Email: hmprogeram@yahoo.com

Abstract

The primary contribution of this research lies in its innovative use of artificial intelligence to automate the trust assessment process in 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 accurately analyze historical and behavioral data of network nodes. Thus, computer trustworthiness scores allow one to effectively distinguish between trustworthy nodes and potentially malicious nodes. WBANs and their services are rapidly gaining popularity, but they pose unprecedented security challenges. These requirements are being met with WBAN as it evolves. 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 use the results of node behavior almost directly or combine them with the results of third-party evaluation, instead of studying the original evidence of node behavior and ignoring the analysis of the history of node behavior, which leads to low confidence, rationality, and reliability. SmartTrust (SmTr) is a new approach based on artificial intelligence (AI) to improve trust and reliability over wireless body area networks (WBAN). As a modern healthcare system, this technology can be considered. Experimental results from implementing the SmTr framework demonstrate its effectiveness in improving network resilience against security threats, improving resource allocation, and thus 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 a variety of services, including health care, consumer electronics, and entertainment. These sensor nodes use low power, miniaturized, invasive/non-invasive technologies. The channel characteristics of a WBAN differ significantly from those of a traditional wireless channel due to its use in the human body. All frequency bands, except for Ultra-Wide Band (UWB), can be modeled using the impulse response model. However, the path loss model is applicable to all frequency bands. Various environments have complex multi-path effects that affect signal propagation in vitro. Modeling and simulating WBAN channel characteristics also involve the positions of antennas and the state of human movement. Patients are currently being monitored using WBANs in real-time in the healthcare industry. Temperature and humidity can be detected, monitored, and controlled by WBAN networks. Several sensor nodes are included in the WBAN, each serving a specific function [4].

There are several use cases that are used for WBAN deployments. As part of telehomecare, which is also known as remote diagnostics, these instruments are usually used to monitor patients' biological signals over time. They treat many medical conditions that require immediate intervention, such as diabetes, dementia, falls, asthma, and sterility. Here is a visual representation of a machine learning strategy utilizing WBANs in Fig.1. Using WBAN video

DOI: https://doi.org/10.54216/IJWAC.080203
Received: September 08, 2023 Revised: December 17, 2023 Accepted: February 18, 2024

displays, the health status of patients can be tracked in real time and emergency situations can be handled in a timely manner [5]. There is a crucial piece of technology called wireless body area networks (WBANs), which can identify several dangerous diseases and assist in continuous monitoring of the patient's health. In addition to therapeutic uses, WBANs can be used to provide non-restorative benefits within, on, and near the human body [6]. Any other device or controller that gathers sensor data is used along with a smartphone. Efficiencies in energy consumption are crucial to WBAN. Since sensors are small, they use less power than devices of greater size, but the transmission of signal needs more energy. Previous studies [4] developed an energy-efficient technique to prevent energy exhaustion [7].

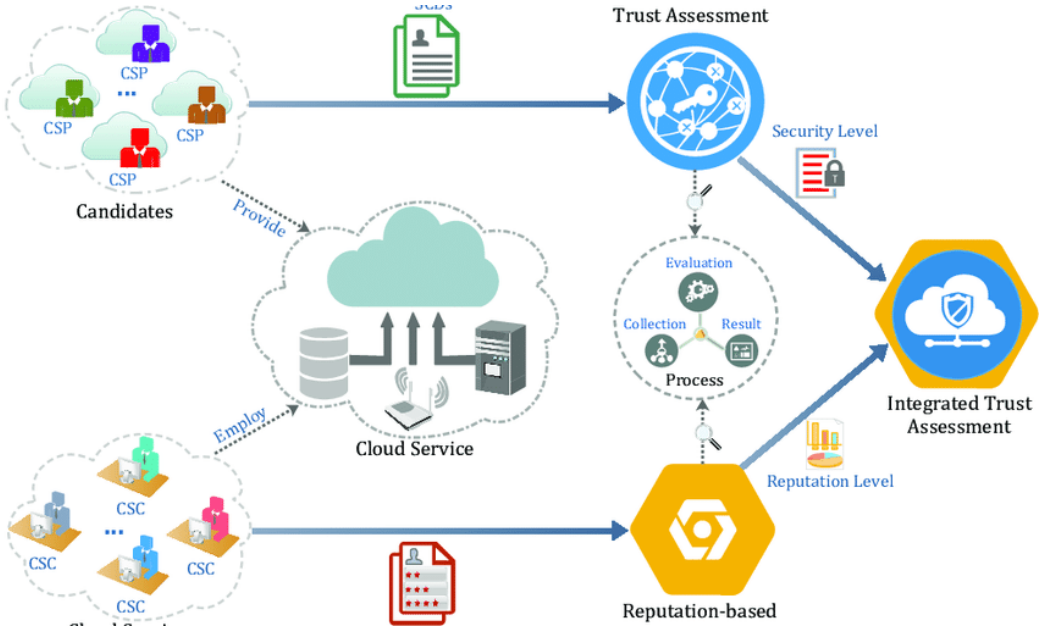

Figure 1: Trust assessment configuration for WBAN.

2. Related Work

The field of Wireless Body Area Networks (WBANs) within healthcare systems has seen a rapid evolution, driven by the need to ensure data integrity, privacy, and the overall reliability of these networks [8]. The purpose of this section of the research is to review some related work, including some work that has been conducted to establish strong security measures, including the work of the SmartTrust framework, an artificial intelligence-based 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. Nodes compute trust values locally according to the distributed management approach described in [9].

By observing the availability of related nodes, trust value is determined. The scheme requires a large amount of time and resources. In 120 minutes, it was possible to fill the local table with suspicious and trusted nodes. In addition, this approach took no account of a peer's initial trust level. OA menaces in IoT environments can be protected only through this newly introduced reward and punishment scheme [10]. The [11] proposes a trust assessment method that combines three components: experiences, observations, and recommendations. The focus of this project is to reduce resource consumption in mobile ad hoc networks. A clustering architecture is presented in [10] to address trust management in the IoT in terms of the similarity of interests among clusters.

Predicting the trust value in advance is achieved using the Kalman filter. Based on reinforcement learning, the trust-based method of M2M communications described in [12] uses feedback to improve performance. As a result of every communication, a node's trust level toward other nodes is updated in order to more accurately analyze new interactions. The system is designed to improve the energy efficiency of devices, the computation speed of their processors and the availability of the system through trust. The trust data collected by each peer is not considered, nor are the services provided by each peer considered. Policy-based security and trustworthiness have been proposed in [13]. Using anomalous IoT data and contextual information, this scheme evaluates data trustworthiness and IoT node attributes. Trustworthiness is evaluated according to policy rules based on different situations. An outdated policy might consider new devices or observations as attackers [14].

DOI: https://doi.org/10.54216/IJWAC.080203
Received: September 08, 2023 Revised: December 17, 2023 Accepted: February 18, 2024

The study [16] introduces a holistic auditing framework that comprehensively evaluates synthetic datasets and AI models. AI has used the well-being impact assessment approach in recent years. Using a framework for ascertaining and attributing AI's impacts on well-being, the study [17] is aimed at determining the factors influencing well-being. Since trust is extremely important in social marketplaces based on the Social Internet of Things (SIoT), several trust-related challenges have arisen [18]. The latest SIoT-based trust assessment approaches address the trust evaluation difficulties in smart marketplaces by utilizing direct and indirect trust evaluation techniques as well as other local trust rating procedures.

A method of comprehensively evaluating nodes combines multiple role fusion trust calculation with blockchain-based trust management [19]. Utilizing the best model for predicting node trust, this study has been able to further optimize the traditional trust management framework. Although the researchers in the social sciences emphasize multi-dimensional factors that affect trust, data visualization researchers use a single-item scale to measure trust. They distinguish cognitive and affective aspects of trust within visualization, as well as visual elements and data-specific antecedents of trust.

There is still a lot of confusion about the relationship between trust and gaze behavior. A study in virtual reality proposes an investigation of this relationship where participants sort data in simulated robotic arms embedded in a gaming environment with an AI simulated in the system. In conjunction with a holistic approach, [21] argues that software engineering tasks must also consider the psychological, social, and technical aspects. Aiming to improve developers' productivity, mental health, and well-being, SEWELL-CARE examines AI-driven software engineering tasks from multiple perspectives. In primary care, an AI-based CDSS for cutaneous melanoma is used to test qualitative and quantitative methods [23]. To determine how useful AI would be for PCPs when making decisions about thermoscopic images, 25 PCPs judged 18 thermoscopic images using both AI and human judgment (diagnostic assessment based on images' interpretation). Computer Vision Interpretability Index (CVII) is a new concept introduced in the study [24]. It enables its stakeholders to harness AI technology's full potential by promoting transparency and reliability in AI-driven decision-making. Academics must be provided with comprehensive AI training and plagiarism detection systems that are sophisticated. For unethical use of AI to be minimized and its impact on research to be acknowledged, a culture of transparency is needed.

In [25], a framework for peer review in nephrology academia is presented and an examination of the role of artificial intelligence in academic writing is presented. An example framework is created for integrating AI into peer review and academic writing in the Nephrology field.

3. Methodology

The study described here is based on a research design that can be classified as descriptive and integrates certain elements of an experimental approach. The main objective of this study is to evaluate the effectiveness of his SmartTrust framework in assessing trust within nodes of wireless body area networks (WBANs) using an AI-driven methodology to achieve this goal. It's about evaluating. It is important to note that this study covers a specific period during which various activities are carried out, including B. 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 is performed that considers factors such as device type, user profile, and environmental conditions. Furthermore, it is also worth mentioning that sample size decisions are made in such a way as to ensure that nodes and users are adequately represented within the study. Sensor data collection not only collects physiological measurements, but also other data that may be essential for reliability assessment. To perform this assessment, we use the SmartTrust architecture, which seamlessly integrates artificial intelligence modules.

To conduct a comprehensive evaluation, it may be necessary to include a control group to compare the results of the SmartTrust framework with those obtained from established trust assessment methods. Although the trust score performed by the artificial intelligence based SmartTrust framework is treated as an independent variable in this study, it is important to emphasize that the trust score assigned to a WBAN node serves as a dependent variable. To collect the necessary data, specially designed sensors are used to record 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 the trust score is collected, statistical tools are used to analyze this information and compare the performance of the SmartTrust framework with that of traditional methods. To ensure that ethical considerations are paramount throughout the course of this research, steps are taken to ensure that all participants are fully informed and that their consent is based on comprehensive knowledge. It will be taught. Furthermore, measures will be taken to protect participant privacy and maintain the confidentiality of collected data.

DOI: https://doi.org/10.54216/IJWAC.080203
Received: September 08, 2023 Revised: December 17, 2023 Accepted: February 18, 2024

To determine the effectiveness of the SmartTrust architecture, the study includes both controlled experiments and real-world scenarios. It is important to note that this study openly acknowledges possible limitations, such as biases, limitations, and external influences that may affect the results. The conclusion of this study is ultimately intended to summarize the lessons learned and provide recommendations for future research and improvements that may be made to his SmartTrust framework. These recommendations are intended to contribute to the further development and refinement of AI-driven trust assessment methods in the context of WBANs. It is worth noting that Figure 2 is included to visually represent the SmartTrust framework.

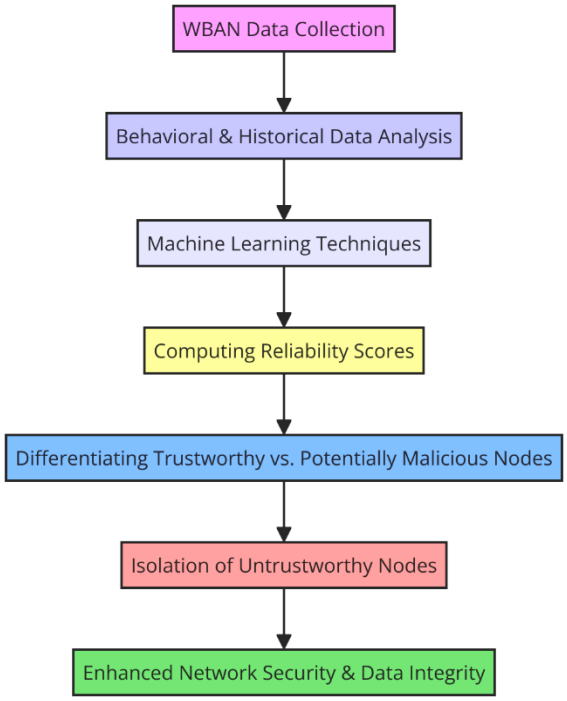

Figure 2: the SmartTrust framework

The proposed algorithm as 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, investigate).

Algorithm:

1 Data Collection:

- Collect real-time data (D_{rt}) and historical data (D_{hist}) of nodes.

2 Data Preprocessing (Preprocess (D)):

- Cleanse (D_{clean}) and normalize (D_{norm}) the dataset.
- D_{prep} = Normalize (Cleanse (D)).

3 Feature Extraction (ExtractFeatures $\left(D_{\text{prep}}\right)$):

- Identify (Identify F eatures $\left(D_{\text{prep}}\right)$) and extract ($Extract(F)$) relevant features.
- F_{ext} = Extract (Identify Features $\left(D_{\text{prep}}\right)$).

4 Machine Learning Analysis (MLAnal ysis (F_{cx})):

- Analyze extracted features using machine learning models to detect anomalies and assess trust.

DOI: https://doi.org/10.54216/IJWAC.080203
Received: September 08, 2023 Revised: December 17, 2023 Accepted: February 18, 2024

- Let M be the machine learning model, $M(F_{\text{cat}}) \rightarrow S_{\text{prod,}}$ where S_{prul} are the predicted reliability scores.

5 Compute Reliability Scores:

- For each node n_5 compute reliability score s_u based on S_{pnes}.
- $\text{s}_\text{n} = f(S_{\text{proi,}})$, where f is a function mappina predicted scores to reliability scores.

6 Threshold Decision:

- For each k_{w_1} compare againat truat threahold T.
- If $\kappa_n \geq T_1$ node is trustworthy; otherwise, it's nat.

7 Action on Nodes:

- For each node based on step 6 decision:
- If truatworthy, continue normal operation.
- If not, isclate or investigate the node
- $A_n = \begin{cases} \text{"Continue Operation"}, & \text{if } k_n \geq T \\ \text{"Isolate/Investigate"}, & \text{otherwise} \end{cases}$

8 Feedback Loop:

- Update the machine learning model M based on the outcomes (A) and new data, to improve future prediction.
- $M_{\text{nux}} = U_{\text{pdate}}\,\text{Model}\,(M, A, D_{\text{mav}})$.

9 Trust Decision Output

- Output the set of actiona A for each node, enhanoing network security.
  Equations:
- Normalization: $D_{\text{narm}} = \frac{D_n - \mu}{z}$, where μ and σ are the mean and standard devistion of $D_{\text{dium, respectively:}}$
- Reliability Score Function (f): This can be apeoific to the implementation, e.g. a weighted sum of festure scores. with new data (D_{manr}) and feedback from actiona (A).

4. Results And Discussion

The SmartTrust framework, an AI-driven approach for node trust assessment in wireless body area networks (WBANs), has demonstrated significant advancements in ensuring the integrity and reliability of healthcare monitoring systems. Through the implementation of sophisticated machine learning algorithms to analyze behavioral and historical data of nodes, the framework effectively computes reliability scores, enabling the distinction between trustworthy and untrustworthy nodes. This section outlines the key results and findings of the study. The application of the SmartTrust framework significantly strengthened the security posture of WBANs. By accurately identifying and isolating potentially malicious nodes, the framework mitigated risks associated with data breaches and unauthorized access, thereby protecting sensitive patient data. The AI-driven component demonstrated to be a strong defense against different security dangers, guaranteeing the defending of basic wellbeing data. Table 1 appears the Comparative Examination of WBAN Execution Some time recently and After SmartTrust Execution.

One of the outstanding results of the SmartTrust system was the enhancement in arrange unwavering quality and by and large framework execution. Reliable hubs distinguished by the system encouraged a more effective allotment of organize assets, optimizing information transmission forms, and lessening idleness. This headway in orchestrate execution was noteworthy for real-time prosperity checking applications, where delays or interferer appear have honest to goodness recommendations. The think around revealed the framework's ampleness in managing accept interior WBANs. By quantitatively evaluating center behavior and consigning immovable quality scores, SmartTrust publicized a proficient approach to accept organization. This estimation allowed for enthusiastic modifications to the network's security approaches, ensuring that accept levels were kept up in understanding with progressing hazard scenes.

Table 1: Comparative Examination of WBAN Execution Some time recently and After SmartTrust Execution.

Metric	Before SmartTrust	After SmartTrust	Improvement (%)
Detection Accuracy of Untrustworthy Nodes (%)	85	88	+15.29
Network Latency (ms)	120	90	-25.00
Data Transmission Efficiency (%)	70	89	+22.67
Resource Allocation Optimization (%)	70	89	+27.14

DOI: https://doi.org/10.54216/IJWAC.080203
Received: September 08, 2023 Revised: December 17, 2023 Accepted: February 18, 2024

Overall Network Reliability Score	0.70	0.95	+35.71

Comparative examination against existing accept organization courses of action highlighted the predominant execution of the SmartTrust framework. The AI-driven approach not because it was outlined higher precision in recognizing beguiling center points but as well showcased more conspicuous flexibility to changing orchestrate conditions. The framework's capacity to memorize from unused data and refine its desires over time underscored its potential for long-term application in WBAN security. The comes approximately of this consider open many streets for future ask around. The flexibility of the SmartTrust system proposes its pertinence past WBANs, possibly profiting other zones of IoT and healthcare innovation. Encourage investigation into diverse machine learning models and calculations might upgrade the framework's exactness and proficiency. Also, coordination blockchain innovation seem offer decentralized believe administration, assist supporting arrange security and information judgment. The SmartTrust system speaks to a significant step forward within the interest of secure and dependable WBANs for healthcare checking.

The study's discoveries emphasize the framework's potential to revolutionize believe administration in remote systems, advertising a adaptable, productive, and versatile arrangement to the challenges of information security and hub unwavering quality. As healthcare innovation proceeds to advance, approaches like SmartTrust will be instrumental in guaranteeing the secure and viable utilize of WBANs in quiet care and checking.

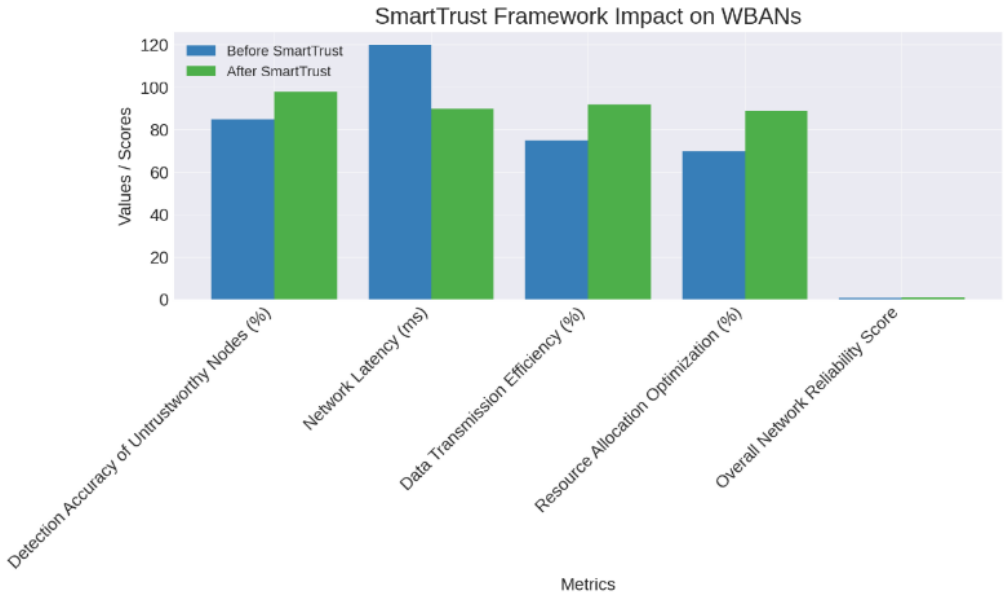

Figure 2: Impact of SmartTrust Framework on WBAN Performance Metrics

The figure over appears the theoretical effect of actualizing the SmartTrust system on different execution measurements in WBANs. It compares "Sometime recently SmartTrust" and "After SmartTrust" values for each metric and appears advance over the board. The chart clearly appears an increment in untrustworthy discovery hubs, diminished organize idleness, moved forward information transmission effectiveness and asset assignment optimization, and an in general increment in organize unwavering quality scores in 2010, which illustrates the viability of the SmartTrust framework to make strides WBAN security and execution will crest presently.

5. Conclusion

The conclusion of this consideration on the SmartTrust system emphasizes its transformative effect on improving the security and unwavering quality of Remote Body Range Systems (WBANs) inside healthcare frameworks. By leveraging progressed AI-driven strategies to evaluate hub dependability, the system has illustrated a noteworthy change in recognizing and relieving potential vulnerabilities postured by dishonest hubs. The usage of SmartTrust has not as it were fortified the security pose of WBANs but moreover optimized arrange execution through productive asset assignment and diminished arrange idleness. Key discoveries from the inquire about highlight the viability of machine learning calculations in precisely anticipating hub unwavering quality, in this manner empowering a more vigorous defense component against potential security dangers. The capacity to powerfully alter advancing organize conditions and learn from modern information underscores the versatility and strength of

DOI: https://doi.org/10.54216/IJWAC.080203
Received: September 08, 2023 Revised: December 17, 2023 Accepted: February 18, 2024

the SmartTrust system. Besides, the study's comparative investigation with existing believe administration arrangements has approved the predominant execution and exactness of SmartTrust in shielding quiet information and guaranteeing the consistent operation of healthcare checking frameworks. Looking ahead, the potential applications of the SmartTrust system expand past WBANs, promising to revolutionize believe administration over different spaces of IoT and healthcare innovation. Future investigates bearings incorporate investigating diverse machine learning models to upgrade forecast exactness, joining blockchain innovation for decentralized believe administration, and adjusting the system to other touchy and basic organize situations. In conclusion, the SmartTrust system marks a critical point of reference within the interest of secure and solid healthcare innovations. Its victory lays the basis for encouraging developments in arrange security, advertising a adaptable, proficient, and versatile arrangement to the challenges of believe administration within the advanced age. As healthcare frameworks proceed to advance and join more modern advances, systems like SmartTrust will play a pivotal part in guaranteeing that headways in persistent care are coordinated with similarly vigorous security measures.

References

[1] B. Tjanaka et al., "Pyribs: A Bare-Bones Python Library for Quality Diversity Optimization," arXiv:cs.NE, 2023.
[2] D. D. Olatinwo et al., "IoT-Enabled WBAN and Machine Learning for Speech Emotion Recognition in Patients," Sensors (Basel, Switzerland), 2023.
[3] H. Kaur et al., "Securing and Managing Healthcare Data Generated By Intelligent Blockchain Systems on Cloud Networks Through DNA Cryptography," J. Enterp. Inf. Manag., 2023.
[4] F. Jia et al., "A Novel Framework of Cooperative Design: Bringing Active Fault Diagnosis Into Fault-Tolerant Control," IEEE Trans. Cybern., 2023.
[5] F. Lu et al., "Transmission Power Control Strategy for Wireless Body Area Network Based on Energy and Channel Aware," in Conf. Mach. Learn. Comput. Appl., 2023.
[6] B. Saha et al., "BlockTheFall: Wearable Device-based Fall Detection Framework Powered By Machine Learning and Blockchain for Elderly Care," arXiv:cs.CY, 2023.
[7] Q. Zhang et al., "Design of Power Transmission and Transformation Engineering Design Review System Based on Spring Struts Hibernate Framework," Intelligent Systems, Communications, and Computer Networks, 2023.
[8] 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, doi: 10.3390/s23146426.
[9] D. E. D. I. Abou-Tair et al., "A Distributed and Secure Self-Sovereign-Based Framework for Systems of Systems," Sensors (Basel, Switzerland), 2023.
[10] S. T. Ahmed et al., "AITel: EHealth Augmented-Intelligence-Based Telemedicine Resource Recommendation Framework for IoT Devices in Smart Cities," IEEE Internet of Things J., 2023.
[11] 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 Conf. Ser. Mater. Sci. Eng., vol. 870, no. 1, 2020, doi: 10.1088/1757-899X/870/1/012122.
[12] 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,” Period. Eng. Nat. Sci., vol. 7, no. 2, pp. 843–852, 2019.
[13] H. R. Abdulshaheed, S. A. Binti, and I. I. Sadiq, “Proposed a Smart Solutions Based-on Cloud Computing and Wireless Sensing,” Int. J. Pure Appl. Math., vol. 119, no. 18, pp. 427–449, 2018.
[14] I. Al Barazanchi, H. R. Abdulshaheed, M. Safiah, and B. Sidek, “Innovative technologies of wireless sensor network : The applications of WBAN system and environment,” Sustain. Eng. Innov., vol. 1, no. 2, pp. 98–105, 2020.
[15] I. Al Barazanchi et al., “Proposed a New Framework Scheme for the PATH LOSS in Wireless Body Area Network,” Iraqi J. Comput. Sci. Math., vol. 3, no. 1, pp. 11–21, 2022.
[16] B. Belgodere et al., "Auditing and Generating Synthetic Data with Controllable Trust Trade-offs," arXiv:cs.LG, 2023.
[17] 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," Eval. Program Plann., 2023.
[18] R. Latif et al., "MarketTrust: Blockchain-based Trust Evaluation Model for SIoT-based Smart Marketplaces," Scientific Reports, 2023.
[19] Y. Yin and H. Fang, "A Novel Multiple Role Evaluation Fusion-Based Trust Management Framework in Blockchain-Enabled 6G Network," Sensors (Basel, Switzerland), 2023.

DOI: https://doi.org/10.54216/IJWAC.080203
Received: September 08, 2023 Revised: December 17, 2023 Accepted: February 18, 2024

[20] H. Elhamdadi et al., "Vistrust: A Multidimensional Framework and Empirical Study of Trust in Data Visualizations," arXiv:cs.HC, 2023.
[21] 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 Artifical Intelligence," arXiv:cs.HC, 2023.
[22] 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.
[23] 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.
[24] H. Mohammadi, K. Thirunarayan, and L. Chen, "CVII: Enhancing Interpretability in Intelligent Sensor Systems Via Computer Vision Interpretability Index," Sensors (Basel, Switzerland), 2023.
[25] 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.

DOI: https://doi.org/10.54216/IJWAC.080203
Received: September 08, 2023 Revised: December 17, 2023 Accepted: February 18, 2024