Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Security-Aware ML-method for Body Area Network Communication Protocol (802.15.6) in IoT-Based Health Monitoring Applications

Meshari H. Alanazi

meshari.alanazi@nbu.edu.sa

Northern Border University

Article

Keywords: Wireless Body Area Network, IEEE 802.15.6, IoMT Security, Machine Learning-Based Intrusion Detection, Attack Probability Estimation, Two-Layer Healthcare Architecture

Posted Date: June 29th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10092811/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Security-Aware ML-method for Body Area Network Communication Protocol (802.15.6) in IoT-Based Health Monitoring Applications

Meshari H. Alanazi[1*]

[1*]Department of Computer Science, College of Science at Northern Border University, Arar, Saudi Arabia.

Corresponding author(s). E-mail(s): meshari.alanazi@nbu.edu.sa;

Abstract

Wireless Body Area Networks (WBANs) play a critical role in IoT-based healthcare monitoring by enabling continuous collection and transmission of physiological data from wearable sensors. However, increasing connectivity and data transmission frequency introduce significant security risks and energy consumption challenges in BAN communication protocols. To address these issues, this paper proposes a Security-Aware Bit-Map Assisted BAN Hybrid (SABMABAN-Hybrid) framework that integrates machine learning-based attack probability estimation with an energy-efficient two-layer communication architecture. In the proposed approach, machine learning models are first employed to analyze healthcare monitoring data and estimate attack probability, which is then used to derive a secure transmission probability controlling data forwarding in the network. The intra-body communication layer utilizes IEEE 802.15.6 EATDMA scheduling with a short CAP, while the gateway communication layer employs a bitmap-assisted IEEE 802.15.4 protocol with a larger CAP to reserve transmission slots. Extensive simulations using Python for attack analysis and MATLAB for energy evaluation demonstrate that the proposed framework improves communication efficiency and reduces network energy consumption compared to conventional BAN protocols. The results confirm that integrating security-aware transmission control with hybrid scheduling mechanisms can significantly enhance the reliability and sustainability of IoT-based healthcare monitoring systems.

Keywords: Wireless Body Area Network, IEEE 802.15.6, IoMT Security, Machine Learning-Based Intrusion Detection, Attack Probability Estimation, Two-Layer Healthcare Architecture.

1 Introduction

The rapid advancement of the Internet of Things (IoT) and the Internet of Medical Things (IoMT) has significantly transformed conventional healthcare systems into intelligent, connected, and patient-centric ecosystems. IoT-enabled health monitoring facilitates continuous tracking of physiological parameters such as ECG, PPG, blood pressure, temperature, and oxygen saturation through wearable and implantable sensors [1, 2]. Remote and in-home healthcare monitoring systems have reduced hospitalization costs and enhanced personalized patient care [3, 4].

Wireless Body Area Networks (WBANs) form the communication backbone of IoT-based health monitoring systems. In WBAN architecture, on-body and implantable sensors communicate using IEEE 802.15.6, while gateway nodes rely on IEEE 802.15.4 for uplink communication [5]. Recent advancements in fog computing, edge computing, and distributed healthcare architectures have further improved scalability and latency performance in smart healthcare environments [6, 7].

Despite these technological advancements, increasing device interconnectivity introduces significant security and privacy challenges [8, 9]. Medical cyber-physical systems are highly vulnerable to cyberattacks that may compromise patient safety and data integrity [10].

WBAN communication operates over open wireless channels and consists of resource-constrained sensor nodes, making them susceptible to replay attacks, identity spoofing, malicious data injection, and eavesdropping [11, 12].

Several lightweight authentication and privacy-preserving schemes have been proposed to enhance WBAN security. Anonymous authentication mechanisms [11, 13], certificateless signature-based authentication [12], and secure signcryption schemes [14] provide confidentiality and identity protection. Blockchain-integrated IoMT frameworks further strengthen data integrity and decentralized validation [15–17].

However, most existing solutions primarily focus on cryptographic authentication and secure data transmission. They do not adequately address real-time intrusion detection or probabilistic attack estimation at the communication layer. Furthermore, strict energy constraints in wearable devices limit the deployment of heavy security mechanisms [18].

Recent studies on medical cyber-physical systems highlight the importance of intrusion detection mechanisms but emphasize the lack of practical ML-integrated communication-layer security models tailored for healthcare networks [10]. Privacy-preserving healthcare monitoring over cloud and distributed systems introduces additional computational and security challenges [19, 20].

Although significant work has been carried out in authentication protocols, blockchain-based security, and privacy-preserving healthcare monitoring [13, 15, 17], limited research has focused on integrating machine learning-based attack probability estimation within IEEE 802.15.6 communication frameworks.

Existing literature either emphasizes:

- Cryptographic authentication and confidentiality mechanisms [12, 13]
- Blockchain-based healthcare validation systems [15, 16]
- Fog and edge-based healthcare architectures [6, 7]

- AI-based healthcare analytics without communication-layer threat modeling [21]

However, there is a lack of:

- Security-aware ML-driven attack prediction integrated with WBAN protocols
- Probabilistic attack estimation instead of binary detection
- Two-layer IEEE 802.15.6–802.15.4 secure BAN architecture with adaptive risk modeling

IEEE 802.15.6-based WBAN communication in IoT healthcare systems remains vulnerable to network-based attacks that may disrupt medical monitoring and compromise patient safety. Traditional cryptographic approaches alone are insufficient for real-time detection of malicious activities. Therefore, a lightweight, security-aware machine learning framework capable of estimating attack probability and integrating it within a two-layer body area network architecture is required.

This work proposes a security-aware ML-based attack prediction framework integrated within a two-layer BAN architecture:

- **Layer 1:** IEEE 802.15.6 WBAN communication among wearable biosensors.
- **Layer 2:** IEEE 802.15.4 gateway communication for uplink transmission.

Machine learning models are trained on health monitoring communication features. After removing feature leakage and addressing class imbalance, threshold optimization is applied to estimate attack probability for each communication instance. The estimated probability is integrated into the BAN decision layer to enable adaptive and risk-aware communication.

The main contributions of this work are:

- The attack probability estimation is integrated with the energy consumption model of IEEE 802.15.6 WBAN communication.
- A threshold-optimized ML framework is developed to handle imbalanced healthcare datasets.
- Two-layer secure BAN architecture is developed by combining IEEE 802.15.6 and IEEE 802.15.4.
- Comprehensive evaluation is done by using Accuracy, Precision, Recall, F1-score, ROC-AUC, and Confusion Matrix along with comparison of the proposed integrated model with the other energy consumption models.

2 Related Work

Recent research in IoT-enabled healthcare and Wireless Body Area Networks (WBANs) has primarily focused on secure communication, authentication mechanisms, blockchain integration, and intelligent healthcare monitoring. Survey-based works [1–4, 8, 17, 18, 20] provide broad overviews of IoT healthcare architectures, wearable systems, blockchain-based IoMT, and energy efficiency challenges.

Table 1: Comparison of Existing Works Based on Contributions and Findings

Ref	Contribution	Method	Tools Used	Result Findings	Conclusion
[4]	Secure RPM survey	Literature review	Survey analysis	Security gaps	Need ML integration
[3]	IoT home monitoring	Architecture study	Middleware design	Scalability issues	Future AI support
[1]	HIoT survey	Clinical survey	IoT framework	Privacy challenges	Security essential
[2]	WBAN review	Sensor analysis	Wearable systems	Energy constraints	Lightweight needed
[5]	Wearable patch	Hardware design	BLE IoT	Real-time monitoring	Efficient integration
[6]	Fog RPM	Fog computing	IoT platform	Latency reduced	Edge effective
[7]	Fog simulation	Modeling study	Simulation tools	Bandwidth optimized	Scalable solution
[11]	Anonymous auth	Cryptographic scheme	ECC-based	Secure authentication	Privacy enhanced
[13]	Lightweight auth	Authentication scheme	WBAN model	Confidentiality improved	Energy efficient
[12]	CLSS scheme	Certificateless auth	WBAN protocol	Revocability support	Privacy preserved
[14]	Signcryption WBAN	Hybrid crypto	Security model	Secure transmission	Lightweight achieved
[22]	Data aggregation	Aggregation scheme	Multi-receiver model	Anonymity ensured	Efficient aggregation
[15]	IoMT blockchain	Blockchain storage	Distributed ledger	Data integrity	Secure validation
[16]	Quantum auth	Blockchain-based	Q-Sim tool	Strong authentication	Quantum secure
[23]	Blockchain healthcare	Technology review	Conceptual model	Scalability limits	Optimization needed
[17]	Blockchain survey	Survey study	IoMT systems	Scalability issue	Further research
[10]	Attack detection	IDS survey	CPS analysis	Detection gaps	ML required
[21]	AI trust protocol	ML security	Trust modeling	Improved reliability	AI effective
[24]	Fault-tolerant IoT	ML fusion	Sensor fusion	Decision accuracy	Fault tolerant
[25]	Depression IoT	Systematic review	IoT analytics	Mental monitoring	Data-driven
[8]	Smart healthcare	Survey review	Big data AI	Security concerns	AI adoption
[9]	AI healthcare	AI survey	ML framework	Smart monitoring	AI essential
[19]	Privacy cloud	HMM model	Cloud computing	Privacy preserved	Secure monitoring
[18]	Energy wearable	Systematic review	Energy analysis	Consumption high	Optimization needed
[20]	Digital twin	Networking survey	Edge-cloud model	Integration issues	Advanced architecture

Fog- and edge-assisted healthcare platforms [6, 7] enhance latency performance and system scalability. Security-oriented works propose lightweight authentication [11–13], secure signcryption [14], privacy-preserving aggregation [22], and blockchain-assisted validation [15, 16, 23]. Intrusion detection and attack detection in medical cyber-physical systems are reviewed in [10]. AI-based and trust-aware healthcare security frameworks are explored in [21, 24]. Emotional and mental health IoT monitoring is investigated in [25]. Privacy-preserving cloud healthcare monitoring is studied in [19].

Although these works significantly enhance authentication, privacy, scalability, and blockchain integration, most of them emphasize cryptographic or architectural improvements rather than communication-layer attack probability estimation. Very limited attention has been given to integrating machine learning-based probabilistic intrusion detection within IEEE 802.15.6-based WBAN systems. Existing studies either provide surveys, propose authentication schemes, or focus on blockchain-enabled validation, leaving a research gap in lightweight, security-aware ML integration for real-time attack probability estimation in multi-layer BAN communication systems.

Table I demonstrates that the majority of existing works focus on authentication schemes, blockchain validation, fog/edge computing, or survey-based architectural analysis. Cryptographic mechanisms such as anonymous authentication, certificateless signatures, and signcryption enhance privacy but do not incorporate probabilistic intrusion prediction. Survey-based studies highlight scalability and security challenges but lack implementation of ML-based communication-layer risk estimation. Very few works combine machine learning with communication-layer security, indicating a clear research gap in security-aware ML integration within IEEE 802.15.6 WBAN systems.

Table II highlights that while several works address IEEE 802.15.6 communication security, most rely solely on cryptographic approaches. Blockchain-based frameworks improve integrity but introduce computational overhead. Machine learning-based approaches are explored in limited contexts and are not integrated with probabilistic attack modeling within WBAN communication. None of the reviewed works combine IEEE 802.15.6 communication, ML-based attack probability estimation, and multi-layer BAN architecture. This reinforces the necessity of the proposed security-aware ML framework for probabilistic intrusion detection in IoT-based healthcare systems.

3 System Model and Mathematical Formulation

This section presents the formal system architecture and mathematical modeling of the proposed security-aware machine learning framework integrated within a two-layer Body Area Network (BAN). The objective is to model IEEE 802.15.6 intra-body communication and IEEE 802.15.4 gateway transmission while incorporating probabilistic attack estimation and adaptive risk control. The proposed formulation captures communication dynamics, adversarial behavior, machine learning-based attack probability prediction, and energy-aware security optimization in a unified analytical framework. The model aims to maximize intrusion detection performance while maintaining energy efficiency and communication reliability in IoT-based healthcare monitoring systems.

Table 2: Comparison Based on System Parameters

Ref	IEEE 802.15.6	ML Used	Blockchain	Fog/Edge	IDS Focus	Probabilistic Model
[4]	No	Limited	No	Yes	No	No
[3]	Partial	No	No	Yes	No	No
[11]	Yes	No	No	No	No	No
[13]	Yes	No	No	No	No	No
[12]	Yes	No	No	No	No	No
[14]	Yes	No	No	No	No	No
[15]	No	No	Yes	Yes	No	No
[16]	No	No	Yes	No	No	No
[10]	Partial	Yes	No	No	Yes	No
[21]	No	Yes	No	No	No	No
[24]	No	Yes	No	No	No	No

3.1 Two-Layer Body Area Network Architecture

The hierarchical structure enables efficient separation of intra-body sensing and inter-network communication while maintaining scalability and security. The first layer ensures low-power, real-time physiological data acquisition using IEEE 802.15.6, whereas the second layer facilitates reliable data aggregation and forwarding through IEEE 802.15.4. The gateway and cloud components provide computational support for attack probability estimation and adaptive security control. The proposed system is modeled as a hierarchical two-layer Body Area Network (BAN) defined as:

$$\mathcal{S} = \{\mathcal{L}_1, \mathcal{L}_2, \mathcal{G}, \mathcal{C}\} \tag{1}$$

where:

- $\mathcal{L}_1$ denotes the intra-body communication layer (IEEE 802.15.6),
- $\mathcal{L}_2$ denotes the gateway communication layer (IEEE 802.15.4),
- $\mathcal{G}$ represents the edge/fog gateway,
- $\mathcal{C}$ represents the cloud or medical server.

3.2 Layer-1 Communication Model (IEEE 802.15.6)

Let $\mathcal{N} = \{n_1, n_2, \ldots, n_K\}$ denote the set of wearable sensor nodes deployed on the human body, where each node continuously monitors specific physiological parameters. For each node n_i, a multi-dimensional physiological feature vector $\mathbf{x}_i(t) \in \mathbb{R}^d$ is generated at time t, containing measurements such as heart rate $HR_i(t)$, blood pressure $BP_i(t)$, temperature $Temp_i(t)$, oxygen saturation $SpO_2(t)$, and other biomedical signals. This vector represents the real-time health state of the patient captured by the i^{th} sensor node.Each sensor node generates a physiological feature vector:

$$\mathbf{x}_i(t) = \left[HR_i(t), BP_i(t), Temp_i(t), SpO_2(t), \ldots\right] \in \mathbb{R}^d \tag{2}$$

The transmission process is modeled by the operator $\mathcal{T}_{802.15.6}(\cdot)$, which represents IEEE 802.15.6 physical and MAC layer processing applied to $\mathbf{x}_i(t)$, producing the transmitted signal $s_i(t)$. The transmitted signal from node i is:

$$s_i(t) = \mathcal{T}_{802.15.6}(\mathbf{x}_i(t)) \tag{3}$$

During wireless propagation, the signal experiences channel fading characterized by the time-varying coefficient $h_i(t)$ and additive white Gaussian noise $\eta_i(t) \sim \mathcal{N}(0, \sigma^2)$. Consequently, the received signal at the BAN coordinator is expressed as $r_i(t) = h_i(t)s_i(t) + \eta_i(t)$, capturing realistic wireless communication impairments within the intra-body network. The received signal at the coordinator is:

$$r_i(t) = h_i(t)s_i(t) + \eta_i(t) \tag{4}$$

where $h_i(t)$ is the channel fading coefficient and $\eta_i(t) \sim \mathcal{N}(0, \sigma^2)$ denotes additive Gaussian noise.

3.3 Layer-2 Gateway Model (IEEE 802.15.4)

At the BAN coordinator, the signals received from all K wearable sensor nodes are aggregated to form a composite signal represented as $R(t) = \sum_{i=1}^{K} r_i(t)$. This aggregation process models data fusion at the coordinator level, where multiple physiological streams are combined for unified processing. The summation operator reflects collective signal reception and may include preprocessing steps such as filtering, normalization, or packet framing prior to forwarding. The aggregated signal at the coordinator is:

$$R(t) = \sum_{i=1}^{K} r_i(t) \tag{5}$$

The aggregated signal $R(t)$ is then transmitted to the upper communication layer through the gateway using IEEE 802.15.4 protocol, represented by the operator $\mathcal{T}_{802.15.4}(\cdot)$. The forwarded signal $y(t) = \mathcal{T}_{802.15.4}(R(t))$ encapsulates MAC scheduling, channel access mechanisms, and low-power wide-area transmission characteristics. This layered transmission ensures reliable uplink communication from the intra-body network to the edge or cloud infrastructure while maintaining energy efficiency and protocol compatibility. The gateway forwards the aggregated data via:

$$y(t) = \mathcal{T}_{802.15.4}(R(t)) \tag{6}$$

3.4 Attack Model

To mathematically model security threats within the BAN communication framework, an attack indicator variable $\mathcal{A}(t) \in \{0, 1\}$ is defined, where $\mathcal{A}(t) = 1$ denotes the presence of malicious activity at time t, and $\mathcal{A}(t) = 0$ represents normal operation. This binary variable enables probabilistic modeling of adversarial behavior within the communication process. Let the attack indicator variable be defined as:

$$\mathcal{A}(t) \in \{0, 1\} \tag{7}$$

where $\mathcal{A}(t) = 1$ represents the presence of an attack. Under adversarial manipulation, the received signal is no longer purely composed of legitimate transmission and channel noise; instead, it is altered by an additional perturbation term $\delta_i(t)$, yielding the compromised signal $r_i^*(t) = r_i(t) + \delta_i(t)$. The perturbation $\delta_i(t)$ is assumed to follow an attack-specific distribution $\mathcal{D}_{attack}$, which may represent replay attacks, spoofing signals, injection noise, or malicious packet modifications.

$$r_i^*(t) = r_i(t) + \delta_i(t) \tag{8}$$

where $\delta_i(t) \sim \mathcal{D}_{attack}$ denotes malicious perturbation.To quantify the likelihood of such adversarial events, the conditional attack probability is defined as $P(\mathcal{A} = 1 \mid \mathbf{x}) = \pi(\mathbf{x})$, where $\mathbf{x}$ represents the observed feature vector extracted from communication and physiological data.

$$P(\mathcal{A} = 1 \mid \mathbf{x}) = \pi(\mathbf{x}) \tag{9}$$

The function $\pi(\mathbf{x})$ models the probability that the observed data corresponds to an attack scenario, thereby enabling probabilistic intrusion detection instead of deterministic classification. This formulation forms the foundation for integrating machine learning-based attack probability estimation within the IEEE 802.15.6–802.15.4 layered BAN architecture.

3.5 Machine Learning-Based Attack Probability Estimation

Let $\mathbf{X} \in \mathbb{R}^{n \times d}$ denote the feature matrix constructed from n communication instances, where each row $\mathbf{x}_i \in \mathbb{R}^d$ represents a d-dimensional feature vector extracted from physiological and communication-layer attributes.

$$\mathbf{X} \in \mathbb{R}^{n \times d}, \quad \mathbf{y} \in \{0, 1\}^n \tag{10}$$

The corresponding label vector $\mathbf{y} \in \{0, 1\}^n$ represents the ground truth attack indicator, where $y_i = 1$ denotes an attack and $y_i = 0$ indicates normal operation. The objective of the machine learning model is to learn a parametric mapping f_θ, parameterized by θ, that transforms input features into a probabilistic attack score within the interval $[0, 1]$. The ML classifier is defined as:

$$f_\theta : \mathbb{R}^d \to [0, 1] \tag{11}$$

The classifier function $f_\theta : \mathbb{R}^d \to [0, 1]$ outputs the predicted attack probability $\hat{p}_i = f_\theta(\mathbf{x}_i)$ for each instance. The predicted attack probability is:

$$\hat{p}_i = f_\theta(\mathbf{x}_i) \tag{12}$$

In the case of logistic regression, this probability is modeled using a linear decision function followed by a sigmoid activation, expressed as $\hat{p}_i = \sigma(\mathbf{w}^T \mathbf{x}_i + b)$, where $\mathbf{w}$ is the weight vector and b is the bias term. For logistic regression:

$$\hat{p}_i = \sigma(\mathbf{w}^T \mathbf{x}_i + b) \tag{13}$$

The sigmoid function $\sigma(z) = \frac{1}{1+e^{-z}}$ ensures that the output is bounded between 0 and 1, thereby enabling probabilistic interpretation.

$$\sigma(z) = \frac{1}{1 + e^{-z}} \tag{14}$$

This probabilistic formulation allows the system to estimate attack likelihood rather than producing a strict binary decision, which is essential for adaptive security control in the proposed two-layer BAN architecture.

3.6 Attack-Aware Transmission Probability

Instead of binary attack detection, the proposed system estimates the attack-aware data transmission probability obtained from the machine learning model. Let the predicted attack probability for node i be $\hat{p}_i$. The secure transmission probability is defined as

$$p_1 = 1 - \frac{1}{K} \sum_{i=1}^{K} \hat{p}_i \tag{15}$$

where K denotes the total number of sensor nodes.

3.7 Transmission Probability Model

Consider a hierarchical two-layer BAN architecture. Let N denote the total number of wearable sensor nodes deployed on the human body, including the central coordinator (CH). Each sensor node generates physiological data events with probability p.

The number of active sensor nodes transmitting data in the IEEE 802.15.6 layer is therefore

$$n_x = (N - 1)p \tag{16}$$

while the remaining nodes remain inactive:

$$m_x = (N - 1) - n_x \tag{17}$$

where n_x represents the number of active sensor nodes and m_x represents idle nodes that do not generate events during the frame.

3.8 Cluster Head Transmission Model

Let N_0 denote the total number of cluster heads including the base station (BS) in the IEEE 802.15.4 communication layer. Unlike the sensor layer, the transmission probability of cluster heads is derived from the machine learning based attack analysis.

Let p_1 denote the attack-aware event transmission probability obtained from the ML prediction stage. The number of active cluster heads forwarding data is defined as

$$n = \lceil (N_0 - 1)p_1 \rceil \tag{18}$$

while the remaining cluster heads remain idle

$$m = (N_0 - 1) - n \tag{19}$$

In the proposed framework, the ML-based attack analysis estimates the secure transmission probability.

3.9 IEEE 802.15.6 Layer (EATDMA with Short CAP)

The first layer operates using the EATDMA protocol with a short Control Access Period (CAP). During CAP, nodes exchange control information for slot scheduling.

The CAP energy consumption is expressed as

$$E_{CAP}^{802.15.6} = P_{tx}T_{cx} + (N-1)P_{rx}T_{cx} \tag{20}$$

During the Contention Free Period (CFP), only the active nodes transmit data while inactive nodes remain in idle mode. Therefore the CFP energy consumption becomes

$$E_{CFP}^{802.15.6} = n_x P_{tx} T_{dx} + m_x P_{ix} T_{dx} + n_x P_{rx} T_{dx} + m_x P_{ex} T_{ex} \tag{21}$$

The total energy consumption of the IEEE 802.15.6 layer is

$$E_{802.15.6} = E_{CAP}^{802.15.6} + E_{CFP}^{802.15.6} \tag{22}$$

3.10 IEEE 802.15.4 Layer (Bit-Mapping Based CAP)

The second communication layer operates using a Bit-Mapping assisted scheduling mechanism with a large CAP. During this phase, each cluster head transmits a short control packet to reserve a dedicated transmission slot.

The energy consumption during CAP is defined as

$$E_{CAP}^{802.15.4} = (N_0 - 1)P_r T_c + P_t T_{ch} + (N_0 - 1)\Big(P_t T_c + (N_0 - 2)P_i T_c + P_r T_{ch}\Big) \tag{23}$$

During the CFP period, only the active cluster heads transmit data while inactive nodes remain in idle mode.

$$E_{CFP}^{802.15.4} = nP_t T_d + nP_r T_d \tag{24}$$

Thus the total energy consumption of the IEEE 802.15.4 layer is

$$E_{802.15.4} = E_{CAP}^{802.15.4} + E_{CFP}^{802.15.4} \tag{25}$$

3.11 Energy Model of SABMABAN-Hybrid

The proposed Security-Aware Bit-Map Assisted BAN Hybrid protocol combines the energy consumption of both communication layers. The total network energy consumption is expressed as

$$E_{SABMABAN} = (E_{802.15.6} + E_{802.15.4}) \times l \tag{26}$$

where l denotes the number of frames per round.

3.12 Energy Model of SAEATDMA-Hybrid

For comparison, the security-aware EATDMA scheme replaces idle listening with buffer checking energy consumption during second layer, however, first layer energy consumption remains same. In this case second layer also operates using the EATDMA protocol with a short CAP. The CAP energy consumption is expressed as

$$E_{CAP}^{SAEATDMA_{L2}} = P_t T_c + (N-1) P_r T_c \tag{27}$$

During the Contention Free Period, only the active nodes transmit data while inactive nodes remain in sleep mode after buffer checking. Therefore the CFP energy consumption becomes

$$E_{CFP}^{SAEATDMA_{L2}} = nP_t T_d + mP_i T_d + nP_r T_d + mP_e T_e \tag{28}$$

The total energy consumption of the SAEATDMA-Hybrid protocol is therefore

$$E_{SAEATDMA} = (E_{802.15.6} + E_{CAP}^{SAEATDMA_{L2}} + E_{CFP}^{SAEATDMA_{L2}}) \times l \tag{29}$$

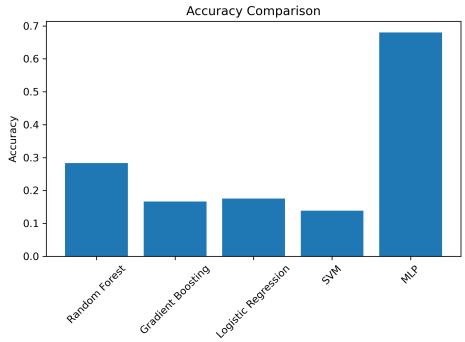
In addition to the proposed SABMABAN-Hybrid protocol, the performance of the system is also evaluated against several existing BAN communication schemes including BANTDMA, EATDMABAN, and BMABAN-based hybrid approaches. These protocols represent conventional scheduling and energy-aware transmission mechanisms commonly used in WBAN and IoT healthcare networks. The comparative analysis focuses on evaluating the impact of attack-aware transmission probability and bit-map assisted scheduling on overall network energy consumption and communication efficiency. This comparison enables a comprehensive assessment of the proposed model under varying network sizes and event probabilities.

4 Result Analysis and Discussion

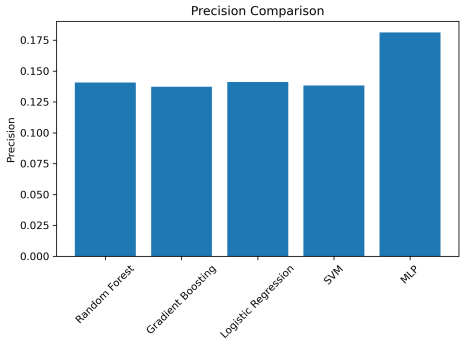
The result analysis and discussion are divided into two parts. The first part focuses on machine learning-based attack probability estimation implemented in Python, where multiple classifiers are evaluated using performance metrics such as Accuracy, Precision, Recall, F1-score, and ROC-AUC. The second part analyzes the energy consumption performance of the proposed SABMABAN-Hybrid protocol using MATLAB simulations based on the estimated attack-aware transmission probability.

4.1 Machine Learning Based Attack Probability Estimation

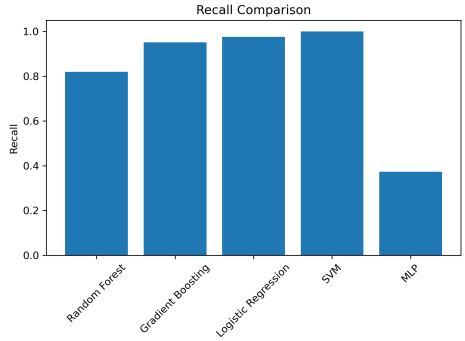
The first phase of the proposed framework focuses on estimating the attack-aware transmission probability using machine learning techniques. The patient health monitoring dataset was processed using Python-based ML models including Random Forest, Gradient Boosting, Logistic Regression, Support Vector Machine (SVM), and Multi-Layer Perceptron (MLP). The models were trained to classify normal and attack events using physiological and network features extracted from the dataset. Performance evaluation was conducted using standard classification metrics including Accuracy, Precision, Recall, F1-score, and ROC-AUC.



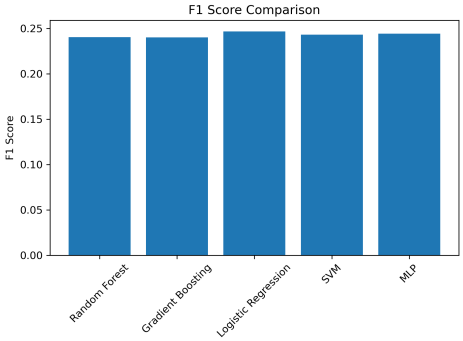
(a) Accuracy Comparison



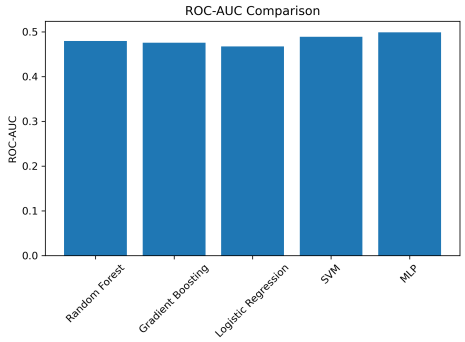
(b) Precision Comparison



(c) Recall Comparison

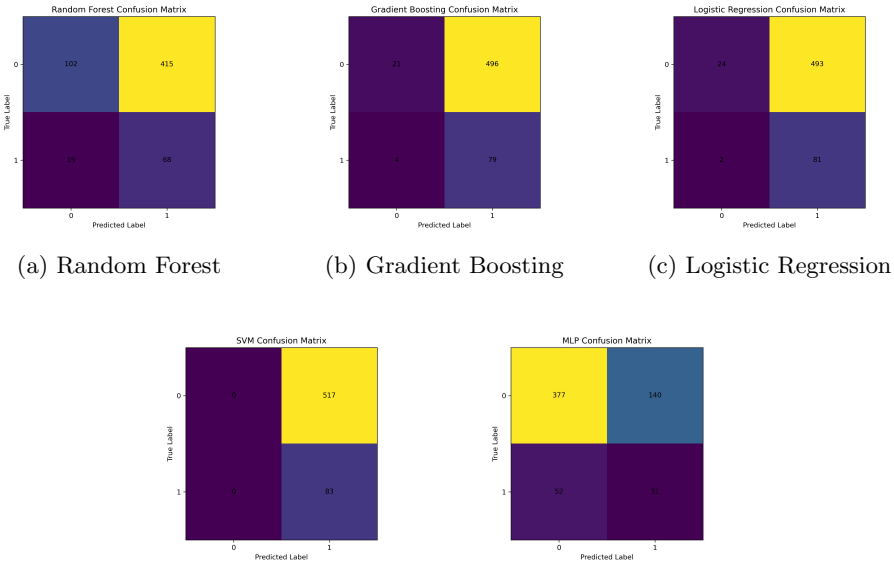


(d) F1 Score Comparison



(e) ROC-AUC Comparison

Fig. 1: Performance comparison of machine learning models for attack probability estimation in the BAN health monitoring dataset.



(a) Random Forest (b) Gradient Boosting (c) Logistic Regression

(d) SVM (e) MLP

Fig. 2: Confusion matrices of evaluated ML models for attack classification.

Figure 1 illustrates the performance comparison of the evaluated models. Among all the algorithms, the MLP classifier achieved the highest classification accuracy of approximately 0.68, indicating superior capability in capturing nonlinear relationships within the dataset. Tree-based ensemble methods such as Random Forest and Gradient Boosting demonstrated moderate performance with accuracies around 0.28 and 0.17 respectively. Logistic Regression and SVM showed relatively lower accuracies, indicating that linear decision boundaries may not adequately capture the complex patterns present in the health monitoring data.

Precision values across most models remained relatively low, ranging between 0.13 and 0.18, which indicates that the models produced several false positive predictions. However, the recall values were significantly high for most algorithms, particularly SVM and Logistic Regression, which achieved recall values close to 1.0. High recall is desirable in healthcare monitoring systems because it ensures that potential attack events are rarely missed, even at the cost of increased false alarms. The F1-score values ranged between 0.23 and 0.25 for most models, indicating balanced performance between precision and recall.

The ROC-AUC results further highlight the discriminative capability of the classifiers. MLP and SVM achieved the highest ROC-AUC scores approaching 0.5, suggesting moderate ability to distinguish between attack and non-attack events. Ensemble methods such as Random Forest and Gradient Boosting also demonstrated stable ROC-AUC performance but with slightly lower predictive capability compared to neural networks.

Table 3: Simulation Parameters Used in MATLAB Energy Analysis

Parameter	Symbol	Value	Description
Number of sensor nodes	N	8 – 24	Sensors deployed on human body
Number of patients per cluster	N_0	10 – 100	Patients connected to a gateway
Event probability	p	0.1 – 1.0	Event generation probability of sensors
Attack-aware probability	p_1	0.14	Transmission probability from ML model
Packet size	T_d	50 – 250 Bytes	Size of physiological data packet
Sessions per cycle	l	10 – 100	Number of data sessions per cycle
IEEE 802.15.6 BAN Layer Parameters			
Transmission power	P_{tx}	0.006 W	Sensor transmission power
Reception power	P_{rx}	0.0052 W	Sensor reception power
Buffer check power	P_{ex}	0.0052 W	Power to check data buffer
Idle power	P_{ix}	0.0015 W	Idle listening power
Sleep power	P_{sx}	10^{-6} W	Sensor sleep state power
Control packet duration	T_{cx}	1 ms	CAP control packet transmission
Data transmission duration	T_{dx}	10 ms	CFP data transmission slot
Buffer check duration	T_{ex}	1 ms	Time to check buffer status
IEEE 802.15.4 Gateway Layer Parameters			
Transmission power	P_t	0.05 W	Cluster head transmission power
Reception power	P_r	0.054 W	Cluster head reception power
Buffer check power	P_e	0.05 W	Buffer checking energy
Idle power	P_i	0.05 W	Idle listening power
Control packet duration	T_c	1.5625 ms	CAP control packet duration
CH control packet time	T_{ch}	1.5625 ms	Cluster head control transmission
CH overhead time	T_{cho}	$2T_{ch}$	Control overhead duration

The confusion matrices shown in Figure 2 provide deeper insight into model behavior. The Random Forest model correctly classified 102 normal instances and 68 attack instances while misclassifying a portion of the samples. Gradient Boosting exhibited similar classification patterns with a high number of correctly detected attack samples. Logistic Regression showed slightly improved detection of attack events with fewer false negatives. In contrast, the SVM model produced extreme predictions, classifying nearly all samples as attack events, resulting in perfect recall but very low precision. The MLP model demonstrated the most balanced behavior with improved classification of both normal and attack samples.

Based on the overall analysis, the ML-based prediction framework was used to estimate the attack probability in the BAN communication network. The resulting attack-aware event probability was calculated as $p_1 = 0.14$, which represents the probability of attack occurrences in the communication layer. This probability was subsequently integrated into the MATLAB-based energy consumption model to evaluate the performance of the proposed SABMABAN-Hybrid protocol under security-aware transmission conditions.

4.2 Energy Consumption Analysis

To evaluate the performance of the proposed SABMABAN-Hybrid protocol, MATLAB-based simulations were conducted under a two-layer Body Area Network

(BAN) architecture consisting of IEEE 802.15.6 for intra-body communication and IEEE 802.15.4 for gateway communication. The simulation scenario considers multiple wearable sensor nodes deployed on the human body communicating with a central coordinator (CH), which forwards aggregated data to the base station. The attack-aware transmission probability p_1 obtained from the machine learning model is incorporated into the communication framework to control secure data transmissions. The energy consumption of the proposed scheme is compared with existing protocols including BMABAN-Hybrid, BANTDMA, SABAN-EATDMA, and EATDMABAN under varying network parameters such as number of sessions, packet size, event probability, number of sensors per patient, and number of patients in a cluster. The simulation parameters used in the MATLAB experiments are summarized in Table 3.

The second part of the performance evaluation focuses on analyzing the energy efficiency of the proposed SABMABAN-Hybrid protocol using MATLAB simulations. The energy consumption of the network was evaluated under varying system parameters including number of sessions per cycle, packet size, event probability, number of sensors per patient, and number of patients in a cluster. The proposed protocol was compared with existing schemes such as BMABAN-Hybrid, BANTDMA, SABAN-EATDMA, and EATDMABAN.

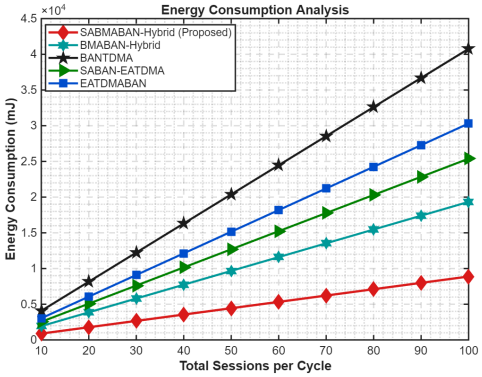
Figure 3 illustrates the comparative energy consumption behavior of the evaluated protocols. When the number of sessions per cycle increases, the energy consumption of all protocols increases proportionally due to the increased number of data transmissions. However, the proposed SABMABAN-Hybrid protocol consistently demonstrates the lowest energy consumption across all session levels due to the integration of attack-aware transmission probability and bitmap-assisted scheduling.

Similarly, when the packet size increases from 50 bytes to 250 bytes, the overall transmission energy increases for all schemes. The proposed method maintains significantly lower energy consumption compared to conventional protocols because only selected nodes transmit data based on the security-aware event probability obtained from the ML model.

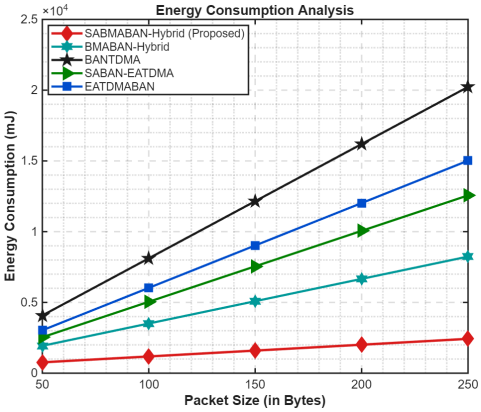
The effect of event probability is also analyzed to observe how frequently sensor nodes generate events. As the event probability increases, the number of active transmissions increases, resulting in higher energy consumption. Nevertheless, the SABMABAN-Hybrid protocol exhibits better energy efficiency by controlling unnecessary transmissions through security-aware scheduling.

Furthermore, the scalability of the protocol is evaluated by varying the number of sensors per patient and the number of patients within a cluster. The results indicate that the proposed scheme scales efficiently with network size while maintaining lower energy consumption compared to existing methods. This improvement is mainly achieved through the combination of EATDMA scheduling in the IEEE 802.15.6 layer and bitmap-assisted slot reservation in the IEEE 802.15.4 layer.

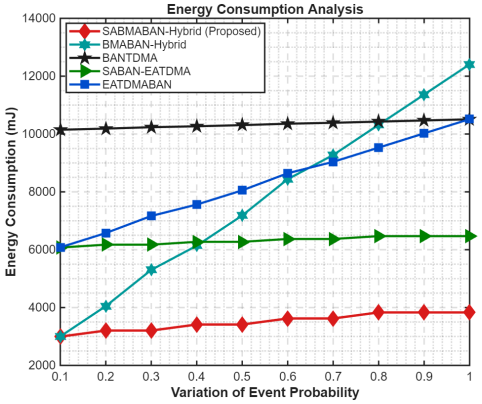
The MATLAB simulation results confirm that the proposed SABMABAN-Hybrid protocol significantly reduces energy consumption in BAN-based healthcare monitoring networks while maintaining secure and efficient communication.



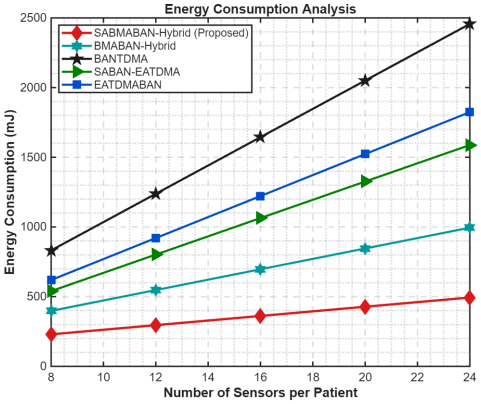
(a) Energy vs Sessions per Cycle



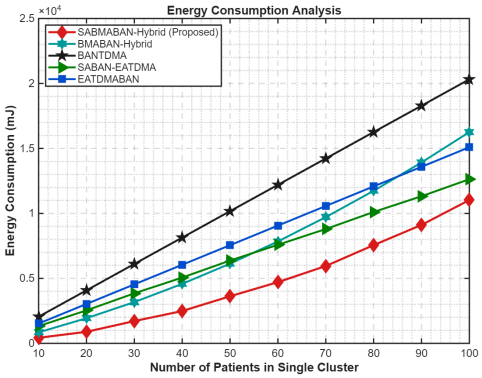
(b) Energy vs Packet Size



(c) Energy vs Event Probability



(d) Energy vs Number of Sensors



(e) Energy vs Number of Patients

Fig. 3: Energy consumption comparison of the proposed SABMABAN-Hybrid protocol with existing BAN communication schemes under varying network parameters.

5 Conclusion

In the present work, a novel Security-Aware Bit-Map Assisted Body Area Network hybrid protocol is proposed that integrates machine learning based attack probability estimation with energy-efficient MAC scheduling for two-layer BAN communication using IEEE 802.15.6 and IEEE 802.15.4 standards. The proposed approach first estimates the attack-aware transmission probability using ML models and then incorporates this probability into the energy consumption model to control secure transmissions. The experimental results from the python-based ML analysis show that the MLP classifier achieved the highest accuracy of approximately 0.68 with an F1-score of about 0.24, while SVM and Logistic Regression achieved higher recall values approaching 1.0, ensuring reliable detection of attack events. Based on these results, the attack-aware transmission probability was estimated as $p_1 = 0.14$. Using this probability, MATLAB simulations demonstrate that the proposed SABMABAN-Hybrid protocol significantly reduces network energy consumption compared to existing protocols including BMABAN-Hybrid, SABAN-EATDMA, EATDMABAN, and BANTDMA. The proposed SABMABAN-Hybrid protocol demonstrates significant energy efficiency compared to existing schemes. When the number of patients increases to 100, the proposed method achieves approximately 26.7% energy reduction compared to EATDMABAN and about 45% reduction compared to BANTDMA. Similarly, when the number of sensors increases to 24 per patient, the proposed scheme reduces energy consumption by nearly 50% compared to BMABAN-Hybrid and approximately 79.6% compared to BANTDMA. The results demonstrate that integrating security-aware transmission probability with bitmap-assisted scheduling effectively reduces unnecessary transmissions and improves energy efficiency in BAN-based healthcare monitoring systems. In the future, our focus will be on implementing the proposed protocol in real IoT healthcare platforms and extending the framework with deep learning-based adaptive intrusion detection mechanisms for large-scale smart healthcare environments.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2026-1180-xx".

Declarations

Data Availability

The Secure Healthcare IoT Monitoring Dataset used in this study is obtained from Kaggle and contains simulated healthcare monitoring data generated from IoT-enabled medical devices. It includes physiological parameters such as heart rate, body temperature, and blood pressure, along with device-related information like device ID, IP address, and access type for security analysis.
https://www.kaggle.com/datasets/programmer3/secure-healthcare-iot-monitoring-dataset

Author Contribution

Meshari H. Alanazi conceived the study, designed the methodology, drafted manuscript, and supervised the overall research direction. He also contributed to the methodological design and assisted in data analysis and validation. The author performed the analysis, interpreted the results, and contributed to result visualization.

Funding

This work is not funded by any agency.

Conflict of interest/Competing interests

The authors have no competing interests to declare that are relevant to the content of this article.

References

[1] Habibzadeh, H., Dinesh, K., Rajabi Shishvan, O., Boggio-Dandry, A., Sharma, G., Soyata, T.: A survey of healthcare internet of things (hiot): A clinical perspective. IEEE Internet of Things Journal **7**(1), 53–71 (2020) https://doi.org/10.1109/JIOT.2019.2946359

[2] Gravina, R., Fortino, G.: Wearable body sensor networks: State-of-the-art and research directions. IEEE Sensors Journal **21**(11), 12511–12522 (2021) https://doi.org/10.1109/JSEN.2020.3044447

[3] Philip, N.Y., Rodrigues, J.J.P.C., Wang, H., Fong, S.J., Chen, J.: Internet of things for in-home health monitoring systems: Current advances, challenges and future directions. IEEE Journal on Selected Areas in Communications **39**(2), 300–310 (2021) https://doi.org/10.1109/JSAC.2020.3042421

[4] Sharma, U., Khara, S., Roy, N.R.: Development of secure remote health monitoring system: A survey. Journal of Mobile Multimedia **21**(3-4), 619–632 (2025) https://doi.org/10.13052/jmm1550-4646.213416

[5] Wu, T., Wu, F., Qiu, C., Redouté, J.-M., Yuce, M.R.: A rigid-flex wearable health monitoring sensor patch for iot-connected healthcare applications. IEEE Internet of Things Journal **7**(8), 6932–6945 (2020) https://doi.org/10.1109/JIOT.2020.2977164

[6] Baucas, M.J., Spachos, P.: Improving remote patient monitoring systems using a fog-based iot platform with speech recognition. IEEE Sensors Journal **23**(15), 17611–17618 (2023) https://doi.org/10.1109/JSEN.2023.3287916

[7] Pati, A., Panigrahi, A., Parhi, M., Kumar Pattanayak, B., Sahu, B., Kant, S.: Simulating fog of medical things: Research challenges and opportunities. IEEE Access **12**, 146527–146550 (2024) https://doi.org/10.1109/ACCESS.2024.3468015

[8] Navaz, A.N., Serhani, M.A., El Kassabi, H.T., Al-Qirim, N., Ismail, H.: Trends, technologies, and key challenges in smart and connected healthcare. IEEE Access **9**, 74044–74067 (2021) https://doi.org/10.1109/ACCESS.2021.3079217

[9] Alshehri, F., Muhammad, G.: A comprehensive survey of the internet of things (iot) and ai-based smart healthcare. IEEE Access **9**, 3660–3678 (2021) https://doi.org/10.1109/ACCESS.2020.3047960

[10] Weber, S.B., Stein, S., Pilgermann, M., Schrader, T.: Attack detection for medical cyber-physical systems–a systematic literature review. IEEE Access **11**, 41796–41815 (2023) https://doi.org/10.1109/ACCESS.2023.3270225

[11] Vijayakumar, P., Obaidat, M.S., Azees, M., Islam, S.H., Kumar, N.: Efficient and secure anonymous authentication with location privacy for iot-based wbans. IEEE Transactions on Industrial Informatics **16**(4), 2603–2611 (2020) https://doi.org/10.1109/TII.2019.2925071

[12] Yuan, J., Zhao, Y., Yu, J.: A conditional privacy-preserving efficient authentication scheme with revocability for wireless body area networks. IEEE Internet of Things Journal **12**(23), 49942–49954 (2025) https://doi.org/10.1109/JIOT.2025.3605911

[13] Subramani, J., Maria, A., Rajasekaran, A.S., Al-Turjman, F.: Lightweight privacy and confidentiality preserving anonymous authentication scheme for wbans. IEEE Transactions on Industrial Informatics **18**(5), 3484–3491 (2022) https://doi.org/10.1109/TII.2021.3097759

[14] Zhang, Q., Zhang, J., Yang, N., Tian, Y.: Secure and lightweight signcryption scheme with group equality test for heterogeneous wban. IEEE Internet of Things Journal **12**(13), 25314–25332 (2025) https://doi.org/10.1109/JIOT.2025.3558230

[15] Syed Muhammad Ali, A., Ali, S., Ziaullah, K., Joo, M.-I., Kim, H.-C.: Iomt and blockchain synergy: A novel approach to health data validation and storage. IEEE Access **13**, 57753–57766 (2025) https://doi.org/10.1109/ACCESS.2025.3555289

[16] Prajapat, S., Kumar, P., Kumar, D., Kumar Das, A., Shamim Hossain, M., Rodrigues, J.J.P.C.: Quantum secure authentication scheme for internet of medical things using blockchain. IEEE Internet of Things Journal **11**(23), 38496–38507 (2024) https://doi.org/10.1109/JIOT.2024.3448212

[17] Adavoudi Jolfaei, A., Aghili, S.F., Singelee, D.: A survey on blockchain-based iomt systems: Towards scalability. IEEE Access **9**, 148948–148975 (2021) https://doi.org/10.1109/ACCESS.2021.3117662

[18] Qaim, W.B., Ometov, A., Molinaro, A., Lener, I., Campolo, C., Lohan, E.S., Nurmi, J.: Towards energy efficiency in the internet of wearable things: A systematic review. IEEE Access **8**, 175412–175435 (2020) https://doi.org/10.1109/

ACCESS.2020.3025270

[19] Zheng, Y., Lu, R., Zhang, S., Guan, Y., Shao, J., Zhu, H.: Toward privacy-preserving healthcare monitoring based on time-series activities over cloud. IEEE Internet of Things Journal **9**(2), 1276–1288 (2022) https://doi.org/10.1109/JIOT.2021.3079106

[20] Chen, J., Yi, C., Okegbile, S.D., Cai, J., Shen, X.: Networking architecture and key supporting technologies for human digital twin in personalized healthcare: A comprehensive survey. IEEE Communications Surveys & Tutorials **26**(1), 706–746 (2024) https://doi.org/10.1109/COMST.2023.3308717

[21] Sankaran, K.S., Kim, T.-H., Renjith, P.N.: An improved ai-based secure m-trust privacy protocol for medical internet of things in smart healthcare system. IEEE Internet of Things Journal **10**(21), 18477–18485 (2023) https://doi.org/10.1109/JIOT.2023.3280592

[22] Zhang, J., Dong, C.: Secure and lightweight data aggregation scheme for anonymous multi-receivers in wban. IEEE Transactions on Network Science and Engineering **10**(1), 81–91 (2023) https://doi.org/10.1109/TNSE.2022.3205044

[23] Ramzan, S., Aqdus, A., Ravi, V., Koundal, D., Amin, R., Al Ghamdi, M.A.: Healthcare applications using blockchain technology: Motivations and challenges. IEEE Transactions on Engineering Management **70**(8), 2874–2890 (2023) https://doi.org/10.1109/TEM.2022.3189734

[24] Gope, P., Gheraibia, Y., Kabir, S., Sikdar, B.: A secure iot-based modern healthcare system with fault-tolerant decision making process. IEEE Journal of Biomedical and Health Informatics **25**(3), 862–873 (2021) https://doi.org/10.1109/JBHI.2020.3007488

[25] Zamani, S., Sinha, R., Nguyen, M., Madanian, S.: Enhancing emotional well-being with iot data solutions for depression: A systematic review. IEEE Journal of Biomedical and Health Informatics **29**(3), 1919–1930 (2025) https://doi.org/10.1109/JBHI.2024.3501254