scientific reports

OPEN

Physically secure and fog-enabled lightweight authentication scheme for WBAN

Jegadeesan Subramani[1], Arun Sekar Rajasekaran[2], Arunkumar Balakrishnan[3]✉ & G. Anantha Rao[4]

Wireless Body Area Networks (WBANs) are vital for healthcare, fitness monitoring, and remote patient care by means of combining sensors and wearable technologies for data collection and transmission. However, ensuring secure communication in WBANs remains a critical challenge and is generally insecure against the manipulation of data, breaches of privacy, and unauthorized access. Current authentication methods are vulnerable to security risks and have a significant computational burden. The above-said shortcomings are addressed by proposing a lightweight, physically secure, fog-enabled authentication scheme that guarantees data privacy and system resilience by integrating Physically Unclonable Functions ($PUFs$) and Fog Computing. This approach involves two phases: WBAN node registration and secure anonymous authentication. The proposed system incurs a reduction in computational overhead of 64.33% and communication overhead of 29.58% compared to existing protocols. Short-life session keys are used to achieve mutual authentication between WBAN sensors and monitoring devices. The proposed scheme is analyzed using BAN logic against attacks on impersonation, replay, and unauthorized access using BAN logic. Its practical effectiveness is confirmed via informal analysis, which shows that it is a scalable and efficient solution for practical WBAN environments.

Keywords Wireless body area network, Data privacy, System resilience, Fog computing, Session key management

The increased adoption of WBANs in healthcare, fitness, and emergency monitoring systems has been catalyzed by rapid progress in wearable technologies. Wearable or implantable sensor nodes constitute devices within a WBAN for monitoring vital physiological parameters (e.g. heart rate, blood glucose levels, body temperature, and motion)[1,2]. Such networks enable the use of applications ranging from remote health monitoring to personalized diagnostics and sports performance optimization with real-time data for medical professionals and improved patient care[3,4].

However, increasing reliance on WBANs generates significant security and privacy challenges[5]. The sensitivity of medical data to attacks such as eavesdropping, data manipulation, and unauthorized access transmitted via wireless channels has been the focus of this research. However, the integration of WBANs into broader applications of IoT ecosystems intensifies these risks because of the commoditization of networked devices by malicious actors[6]. Moreover, WBAN sensor nodes are constrained by limited computational power, memory, and battery life, rendering the implementation of resource-intensive techniques such as RSA and ECC difficult[7,8].

In response, fog computing has emerged as a promising paradigm for addressing these challenges by bringing data processing and decision-making closer to the network edge. Fog nodes reduce latency, supply real-time analytics, and increase security by isolating sensitive data before they enter centralized cloud servers[9]. In addition, adding PUF to WBANs makes tamper resistance and device authentication easier. Using the device's unique physical properties, $PUFs$ create unforgeable identifiers for WBAN nodes to prevent them from being cloned and forged[10].

However, as the security challenges of WBANs, including unauthorized access, data breaches, and high energy consumption, have been induced by existing authentication mechanisms such as high computational overhead,

[1]Department of ECE, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India. [2]Department of ECE, SR University, Warangal, Telangana 506371, India. [3]Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India. [4]Department of Electronics and Communication Engineering, Avanthi Institute of Engineering and Technology, Vizianagaram - 531 162, Cherukupally, Andhra Pradesh, India. ✉email: arunkumar.b@manipal.edu

vulnerability to replay attack, and low resource utilization, the need for an extremely lightweight and resource efficient authentication framework has evidently emerged. As a result, there was a motivation to integrate PUFs and Fog Computing to enhance security whilst reducing computational and communication efficiency, making the proposed solution well-suited for real-world WBAN deployments. Hence, we propose a novel fog-enabled PUF-based lightweight authentication framework for WBANs with limited resource constraints and security requirements. The contributions of this study are as follows.

1. PUF-Based Authentication: Using device-specific physical characteristics to resist tampering and device identification.
2. Fog-Enabled Architecture: Fog nodes perform real-time security management by decentralizing computational tasks.
3. Resource-efficient security: Reduces energy and computational overhead by employing lightweight cryptographic protocols compatible with low-power-constrained WBAN devices.

In contrast to prior WBAN security solutions, the proposed framework uniquely integrates fog computing with PUF-based authentication in a unified architecture to enhance resilience against both cyber and physical threats. The protocol introduces a stateless session key update mechanism using fresh nonces and real-time PUF responses, ensuring perfect forward secrecy and immunity to desynchronization attacks, which are common challenges in traditional PUF systems. Additionally, the system supports priority-based data routing, where normal condition data is directed to the cloud, and emergency data is transmitted immediately to medical personnel and caregivers. These features are further complemented by an offloading strategy, in which fog nodes handle security computations, allowing WBAN devices to preserve battery life and computing resources. These distinctive characteristics make the framework suitable for real-world, latency-sensitive healthcare applications with constrained edge devices.

The remainder of this paper is structured as follows: Section II contains an important literature review, Section III reports on previous work, and the proposed system model. Section IV presents an outline of the proposed framework and Section V presents a security analysis of this framework. Section VI compares the performance efficiency of the proposed scheme, and Section VII concludes the paper.

Related works

WBAN is a wireless technology that can operate in a sensor network in highly sensitive environments, mainly in medical sections, where the treatment of sensitive patient data is essential. These networks are networks of wearables or implantable devices that continuously monitor physiological parameters and transmit this data to healthcare providers on time for decision-making. Although deployed in real-world scenarios, they face numerous security challenges such as impersonation attacks, replay attacks, session hijacking, and data tampering. Owing to the constrained computational resources, limited power supply, and dependence on wireless communication of WBANs, they are very vulnerable to malicious attacks. These security challenges have been documented extensively in previous studies. As an example, the authors in[11] devise a lightweight authentication protocol appropriate for WBANs which strikes the right balance between security and energy efficiency. This protocol protects against lightweight impersonation and replay attacks with cryptographic inexpensiveness for low-power devices. In addition[12], emphasized the growing potential of IoT-enabled vulnerabilities of WBANs and proposed the mitigation of sophisticated attacks through a multi-layered security approach. These studies revealed that the security mechanisms employed in WBANs need to be robust and energy efficient to ensure safe traffic of sensitive data in healthcare and other critical domains.

Although these problems have been addressed, many still need to be resolved. There are some key areas of further research in the form of ensuring that device pairing is secure, defending against physical tampering, and a schema similar to that of SNARC, which aims to balance security, energy efficiency, and scalability. Given their criticality in safety and security applications, these challenges are particularly acute in high-security applications, such as military operations or critical care unit applications.

WBAN security challenges have been successfully addressed by using fog computing as a novel paradigm. Fog computing extends scalability, responsiveness, and efficiency by decentralizing data processing to edge devices that are smaller than WBAN devices. This decentralized approach is desirable, especially in time-sensitive healthcare scenarios where the transmission or processing of data can cause severe consequences. Preprocessing, anomaly detection, and encryption can be performed at fog nodes by reducing the computational burden on WBAN devices and cloud servers. In[13], the authors demonstrated that fog networking can enhance the security and performance of WBANs. In their study, they showed how fog nodes could mediate communications between WBAN devices and cloud servers in several ways, including layering on new means of authentication and encryption. With this approach, communication between resource-constrained WBAN nodes and cloud infrastructure mitigates risks, and real-time data processing is also increased.

However, fog-enabled WBAN frameworks have limitations. High-security applications, such as military operations and critical care settings, pose the danger of physical tampering of fog nodes and WBAN devices[13]. Fog nodes themselves may be targeted by cyberattacks and the entire network can be compromised. Eliminating these challenges necessitates the combination of solid physical security features with a strong authentication and encryption protocol. WBAN node security against physical and cyber threats requires the availability of physically unclonable functions (PUFs). Arrays of inherent manufacturing variant features, called PUFs, are exploited to produce unique, unclonable identifiers for use in device authentication and secure key generation. The effect of this hardware-based security mechanism is that it is not easily tampered with, as in an environment that has a lot of outside interference, which makes the results of this security mechanism more effective.

However, recent studies have demonstrated the security effectiveness of PUFs in WBAN. For instance, in[14], the authors proposed a PUF-based authentication protocol that reduces the physical tampering risk and overall security. However, one aspect of the practical implementation of PUFs in WBANs is their noise resilience, scalability, and integration with other frameworks. PUF reliability is affected by environmental factors such as temperature and aging, and noise-resilient designs are required[15]. In addition, scaling PUF-based solutions for WSAN deployment is an open research problem. Finally, the lightweight nature of WBAN devices requires lightweight cryptographic protocols. Although robust, traditional cryptographic techniques tend to be too computationally intensive for devices with low processing power or short battery life. This gap is addressed using lightweight cryptographic protocols that guarantee the same type of security with minimal resource consumption.

In[17], the authors proposed a hash-based authentication protocol for WBANs with reduced energy consumption, but it was still secure against impersonation and replay attacks. However, lightweight protocols already in existence[18] tend to be largely missing from securing features such as multi-vector attack resistance or advanced persistent threat resistance. This limitation motivates adaptive cryptographic protocols that change the complexity according to the availability of resources and threat levels.

In addition to WBAN-specific security models, several authentication and key agreement protocols developed for related domains such as IoT, cloud computing, and wearable sensor networks are worth noting. For instance[19], proposed a machine learning–resilient and low-latency authentication scheme for AI-driven patient monitoring, while[20] developed a provably secure key management framework tailored for e-healthcare systems. The EAKE-WC protocol[21] offers lightweight authenticated key exchange optimized for wearable computing, and[22] presents a cloud-assisted secure and cost-effective solution for remote health monitoring. These works demonstrate cross-domain applicability, especially where low latency, energy efficiency, and robust authentication are critical. Integrating the design principles of these protocols with WBAN infrastructure may lead to enhanced security outcomes and promote the cross-employment of proven mechanisms across related platforms.

For example, the integration of these protocols with other security frameworks, such as fog computing and PUFs, will provide further security for WBAN. Although fog computing and PUF-based authentication have displayed great potential on individual fronts, their combinations have not been well explored[23]. Decentralized fog computing, in conjunction with hardware-based PUFs, forms a complementary addition that can be used to design robust frameworks for WBAN. Nevertheless, seamless interoperability, resource optimization, and scalability must be addressed to obtain effective integration.

The purpose of this study is to close this gap by proposing a hybrid fog-based and PUF-based lightweight authentication framework for WBANs. The balance between security, scalability, and resource efficiency is achieved through the proposed framework, which addresses the existing limitations in the approaches[23–26]. It offers a multilayer security mechanism to combat both cyber and physical attacks with little overhead by integrating fog computing and PUFs. Furthermore, the framework was optimized for energy consumption to conserve power in the resource-limited context of WBAN devices. This study contributes to the design and implementation of the hybrid framework, evaluation of the framework in real-world scenarios, and comparison of its performance against existing security solutions. These contributions are intended to promote the development of WBAN security and to serve as a basis for future work in the field of WBAN security.

System model, preliminaries and attack model

System model

The adapted system model for the WBAN application is shown in Fig. 1 and consists of several core components such as Cloud Server (CS), Fog Nodes (FN_i), WBAN Controller $(WBAN_j)$ and Monitoring Device (MD_{ij}). The interaction of these elements results in the deployment of secure and efficient communication and monitoring in the WBAN environment.

Cloud server $(\boldsymbol{CS})$ In the WBAN framework, the CS plays the role of a central trusted authority. The system uses services of the CS that need to be used by both $WBAN_j$ and MD_{ij}, and in order to use services of the CS these have to register with it and provide their credentials unique to them. Once registered, the CS generates and distributes the initial security parameters necessary for mutual authentication, along with other parameters, is distributed to the client, to establish communication. The CS is responsible for the overall security of the system including the detection and elimination of malicious activities, a primary repository for health aggregate data generated from the WBAN devices.

Fog node $(\boldsymbol{FN_i})$ FN_i is an intermediate between $WBAN_j$ and MD_{ij}. FN_i is local to $WBAN_j$ and acts to increase system responsiveness and lower latency by performing localized computations and storage. In this framework, we call FN_i a trusted entity, with enough computational power and memory to perform the authentication process and secure communication. In time-sensitive healthcare scenarios, its decentralized role improves the system's efficiency and security.

To prevent FN_i from becoming a single point of failure, the architecture supports redundancy using active-passive or load-balanced fog node deployment. Each fog node is independently preloaded with secure credentials, challenge-response pairs, and session parameters, ensuring continued operation even if another node fails. Additionally, lightweight anomaly detection mechanisms are embedded to detect suspicious behavior or compromise attempts, allowing the system to isolate affected nodes and reroute authentication tasks dynamically. This enhances system robustness against targeted cyberattacks.

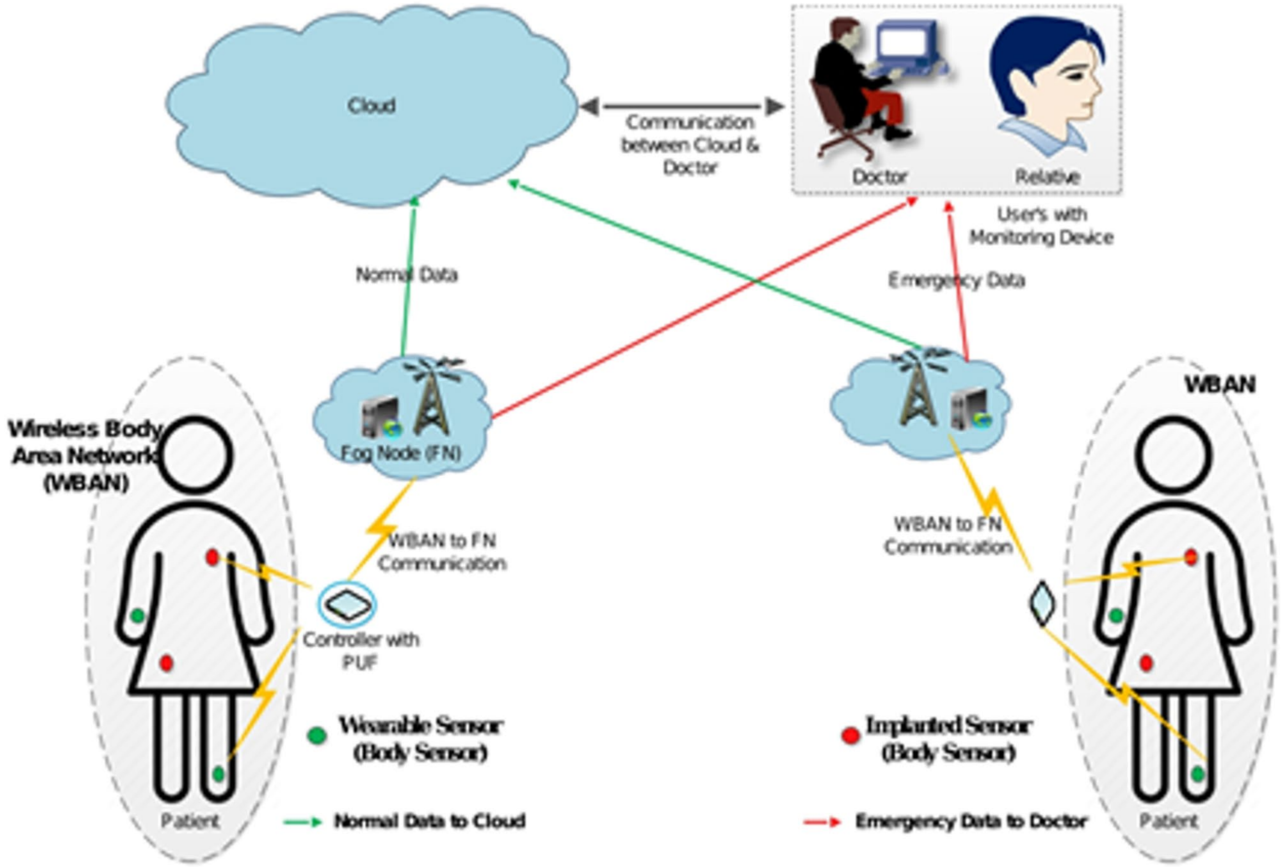

Fig. 1. System model.

WBAN controller ($\boldsymbol{WBAN_j}$) $WBAN_j$ is a body sensor interfaced with a central controller, and is the major node to be integrated within the WBAN system. Physiological data of patients, athletes, elderly persons, etc., are collected by body sensors, and health continues to be monitored by them. This data is consolidated by the $WBAN_j$ while also ensuring secure communication with the monitoring device. During the initial setup, each $WBAN_j$ list at the CS to get the security parameters for authentication. Physically Unclonable Functions ($PUFs$) are used within the controller as a means to provide unique, device-specific identifiers, based on intrinsic hardware variations. These $PUFs$ offer robust hardware-based security, against unauthorized access or tampering attempts. The high level of tamper resistance is ensured by the fact that any attempt to manipulate the $PUFs$ makes them nonfunctional.

Monitoring device ($\boldsymbol{MD_{ij}}$) Doctors, medical professionals, relatives or any authorised individual uses the MD_{ij} to monitor data collected by the $WBAN_j$. MD_{ij} in the proposed scheme continuously links to the $WBAN_j$ which will provide real-time observation and analysis of the wearer's health. CS provide the basic secure parameters which are needed to utilize secure communication between MD_{ij} and $WBAN_j$. MD_{ij} talks to $WBAN_j$ via these secure channels to retrieve data in a way that it guarantees the integrity and confidentiality of the sensitive information. Additionally, MD_{ij} also plays a critical important role in the transfer of device ownership. It performs handover authentication process in order to allow only allowed people to enter the system. For a confidential and secure transition of sensitive health data, this functionality is required. Monitoring Device provides a secure and efficient oversight mechanism within the framework of WBAN by fulfilling these responsibilities.

Scalability and device adaptability The proposed protocol is scalable and supports dynamic changes in the number of WBAN devices. Each $WBAN_j$ independently initiates the authentication process using its unique identity and freshly generated session parameters. The protocol does not rely on global state synchronization, enabling seamless onboarding of new WBANs or removal of existing ones without affecting other active sessions. The session-specific use of nonces and timestamps ensures isolation and statelessness, which allows the system to accommodate fluctuating WBAN device counts efficiently.

Physically unclonable function ($\boldsymbol{PUF}$)

The PUF is a microelectronic system that is designed to process the challenge (C) and provide the response (R). The PUF produces an output denoted R that is an outcome of the PUF function, which takes the value C as its input.

Consequently, the PUF generates an output that differs from that of other systems with similar physical structures and inputs. Therefore, interference with the structural output of electronic devices is an effective way to protect their physical integrity, especially if they are located in remote areas. However, noise is a major flaw in the responsive action of the PUF. A reverse fuzzy extractor method has been successfully applied in eliminating noise from PUF response with relatively low computation complexity[27].

Attack model

The potential threats to the system under consideration were thoroughly investigated and meticulously analyzed for each specified attack scenario.

Physical intrusion attack An adversary having physical access to $WBAN_j$ would attempt unauthorized access to tamper or steal the sensitive data, or devices. To overcome this, $WBAN_j$ employ tamper-evident security through PUFs. Safeguarding sensitive health data, any unauthorized attempt to access or manipulate the PUF makes the device non-functional.

Eavesdropping attack In wireless communications between $WBAN_j$ and MD_{ij}, an interception by an adversary is an attempt to get hold of authentication credentials or sensitive health data. A secure, encrypted communication channel specified with parameters provided by the CS is proposed using; Confidentiality and preventing unauthorized interception.

Man-in-the-middle attack An adversary may impersonate devices, or change data during transmission in an attempt to intercept and modify communication between $WBAN_j$ and MD_{ij}. Besides PUF-based unique identifiers, the mutual authentication mechanism provides that only legitimate entities can participate in the communication. Additionally, no attempts to modify or falsify data are allowed, providing integrity taken with the data.

Resource-exhaustion attack An adversary might be able to increase performance over $WBAN_j$ computational and communication resources to degrees in which performance is degraded or services are denied. The system continues operating even with attacks, through the development of lightweight cryptographic protocols that guarantee functionality and the optimization of resource allocation mechanisms to minimize its energy consumption.

Dolev-Yao attack model In the Dolev-Yao model an adversary is allowed to eavesdrop, intercept, modify, fabricate, and retransmit messages. Specifically designed to confront these advanced threats through robust encryption, secure key-exchange protocols, and PUF-based authentication mechanisms, the proposed scheme attempts to counter these issues. These measures enable the WBAN system to remain confidential, well-known, and authentic, even in a severely insecure environment.

Proposed scheme

The proposed approach consists of three main stages: system initialization, user registration, and subsequent authentication.

System initialization

Master key generation To secure communication and authentication amongst different entities in the system, the Cloud Server (CS) generates master secrets. The aforementioned master secrets are s_{CS} (the master key for Cloud Server), s_{FN_i} (shared key for Fog Nodes) and s_{WBAN_j} (the key associated with WBAN Controllers only). These keys comprise the basis of security in the system, from which they create secure channels and trusted interactions among the components.

$\boldsymbol{PUF}$ challenge-response pair ($\boldsymbol{CRP}$) registration For CRP registration, each device $(WBAN_j,\ MD_{ij})$ has to perform a one-time secure registration with CS in a physically secure and trusted setup (e.g., certified hospital environment or factory provisioning). Each of these challenges (C) are then applied to the PUF resulting in unique responses $R_{PUF} = PUF\,(C)$ for challenges in this process. Then the $(C,\ R_{PUF})$ challenge-response pairs are securely transmitted to the CS.

To prevent eavesdropping or tampering during this transfer, CRPs are encrypted using an ephemeral session key derived as $K_{Session}^{Initial} = H(R_{PUF} \parallel s_{CS})$, or transferred via a trusted, offline method. The CS stores these CRPs for future authentication.

Preloading parameters The CS preloads essential security parameters into the devices, including CRP subsets and device-specific keys. These parameters are protected during preloading using either physical security controls or cryptographic encryption, ensuring confidentiality and integrity before deployment.

Secure parameter distribution CS distribute initialization keys and corresponding $CRPs$ with Fog Nodes (FN_i) in a secure manner. Specifically, CS shares $\left\{C_{FN_i},\ R_{PUF_{FN_i}},\ s_{FN_i}\right\} \to FN_i$ either during a trusted offline provisioning phase or via a secure, authenticated encryption channel. This ensures confidentiality, integrity, and protection against CRP exposure during the distribution process, enabling decentralized and tamper-resistant authentication.

System entity registration
The Entity Registration phase ensures that $WBAN_j$ and MD_{ij} securely register with CS to establish their identity and receive initial parameters for authentication.

WBAN controller ($WBAN_j$) registration

Step 1: $WBAN_j$generates its unique identifier UID_{WBAN_j} and secret m_{WBAN_j}.

Step 2: Compute the PUF Response as $R_{PUF_{WBAN_j}} = PUF\left(C_{WBAN_j}\right)$, and calculate the Hash value as $M_{WBAN_j} = H\left(UID_{WBAN_j} \parallel m_{WBAN_j}\right)$.

Step 3: Send the Registration Request $\left\{UID_{WBAN_j},\ M_{WBAN_j},\ R_{PUF_{WBAN_j}},\ C_{WBAN_j}\right\}$ to CS.

Step 4: CS verifies M_{WBAN_j} and registers $WBAN_j$. Assigns the following parameters: $\alpha_{\,WBAN_j} = H\left(UID_{WBAN_j} \parallel s_{WBAN_j}\right)$, $K_{Session}^{Initial} = H\left(R_{PUF_{WBAN_j}} \parallel s_{CS}\right)$.

Monitoring device (MD_{ij}) registration

Step 1: MD_{ij} generates Identity and Secret key as follows, Unique identifier $\left(UID_{MD_{ij}}\right)$, Password $\left(PW_{MD_{ij}}\right)$ and Random nonce $\left(N_{MD_{ij}}\right)$.

Step 2: Compute the Temporary Identifiers as $TID_{MD_{ij}} = H\left(UID_{MD_{ij}} \parallel N_{MD_{ij}}\right)$, $TPW_{MD_{ij}} = H\left(TID_{MD_{ij}} \parallel PW_{MD_{ij}}\right)$.

Step 3: Send the Registration Request $\left\{TID_{MD_{ij}},\ UID_{MD_{ij}},\ C_{MD_{ij}}\right\}$ to CS.

Step 4: CS verifies $TID_{MD_{ij}}$ and registers MD_{ij}. Assigns the following parameters: $\alpha_{\,MD_{ij}} = H\left(TID_{MD_{ij}} \parallel s_{FN_i}\right)$, $\delta_{\,MD_{ij}} = PUF\left(C_{MD_{ij}}\right) \oplus TPW_{MD_{ij}}$, $K_{Session}^{Initial} = H\left(R_{PUF_{MD_{ij}}} \parallel s_{CS}\right)$.

Authentication scheme

The authentication scheme ensures session-key uniqueness, forward secrecy, and secure communication while preventing session-key reuse. It incorporates provisions for dynamic parameters, session identifiers, and device-specific keys to ensure secure and efficient operation. The notation used in the proposed method is listed in Table 1.

Step 1: Request Initialization by MD_{ij} by generating a fresh nonce $N_{MD_{ij}}$ and a timestamp TS_i. Next, it computes the following, $R_{MD_{ij}} = PUF\left(C_{WBAN_j}\right) \oplus H\left(TID_{MD_{ij}} \parallel N_{MD_{ij}}\right)$, $SID = H\left(N_{MD_{ij}} \parallel N_{WBAN_j} \parallel TS_i\right)$. Finally, it Sends the following request to $WBAN_j$ via the Fog Node (FN_i): $M_{request} = \left\{UID_{MD_{ij}},\ R_{MD_{ij}},\ SID,\ TS_i\right\}$ to $WBAN_j$.

Notation	Description
$UID_{MD_{ij}}$	Unique ID of Monitoring Device MD_{ij}
UID_{WBAN_j}	Unique ID of WBAN Controller $WBAN_j$
$N_{MD_{ij}}$ and N_{WBAN_j}	Dynamic nonces generated by MD_{ij} and $WBAN_j$, respectively
TS_i	Timestamp for freshness verification
SID	Session Identifier
$K_{Session}$	Current session key
$K_{Session}^{Prev}$	Previous session key
$R_{MD_{ij}}$ and R_{WBAN_j}	PUF-based responses from MD_{ij} and $WBAN_j$
MAC	Message Authentication Code
$H(x)$	Cryptographic hash function

Table 1. Notations and description.

Step 2: $WBAN_j$ receives $M_{request}$ and validates the TS_i by ensuring $|TS_j - TS_i| \leq \triangle T$ to prevent replay attacks and also it verifies the SID by ensuring $SID = H\left(N_{MD_{ij}} \parallel N_{WBAN_j} \parallel TS_i\right)$. Next, it computes, $R'_{MD_{ij}} = PUF\left(C_{WBAN_j}\right) \oplus H\left(TID_{MD_{ij}} \parallel N_{MD_{ij}}\right)$. If $R'_{MD_{ij}} = R_{MD_{ij}}$, then MD_{ij} is authenticated. Further, it generates a fresh nonce N_{WBAN_j}, response $R_{WBAN_j} = PUF\left(C_{WBAN_j}\right) \oplus H(UID_{WBAN_j} \parallel N_{WBAN_j})$ and sends the following response to MD_{ij}: $M_{response} = \left\{UID_{WBAN_j},\ R_{WBAN_j},\ SID,\ N_{WBAN_j}\right\}$

Step 3 MD_{ij} verifies $R'_{WBAN_j} = PUF\left(C_{WBAN_j}\right) \oplus H(UID_{WBAN_j} \parallel N_{WBAN_j})$. If $R'_{WBAN_j} = R_{WBAN_j}$, then $WBAN_j$ is authenticated. Next, both MD_{ij} and $WBAN_j$ compute the session key as $K_{Session} = H\left(R_{MD_{ij}} \parallel R_{WBAN_j} \parallel K_{Session}^{Prev} \parallel SID\right)$, ensuring it incorporates fresh parameters and the previous session key for uniqueness.

Step 4: During communication, the request, response, and verification of messages are structured as follows: Each message includes SID and a Message Authentication Code, $MAC = H(K_{Session} \parallel M)$, where M is the message content. The transmitted request is: $M_{transmitted} = \{M,\ MAC,\ SID\}$. The response message includes an updated SID' and its MAC: $MAC = H(K_{Session} \parallel M_{response})$, The transmitted response is: $R_{transmitted} = \{M_{response},\ MAC',\ SID'\}$. For verification, the receiver ensures: $SID = H\left(N_{MD_{ij}} \parallel N_{WBAN_j} \parallel TS_i\right)$, and $MAC = H(K_{Session} \parallel M)$.

Step 5: Session key update mechanisms are as follows: Both MD_{ij} and $WBAN_j$ generate new nonces $N'_{MD_{ij}}$ and N'_{WBAN_j} and compute the New Session Identifier as $SID' = H\left(N'_{MD_{ij}} \parallel N'_{WBAN_j} \parallel TS'_i\right)$. Next, it updates the Session Key as $K_{Session}^{New} = H\left(R'_{MD_{ij}} \parallel R'_{WBAN_j} \parallel SID' \parallel K_{Session}^{Prev}\right)$. Finally, both devices do the continuity verification by ensuring the following: $K_{Session}^{New} = H\left(R'_{MD_{ij}} \parallel R'_{WBAN_j} \parallel SID' \parallel K_{Session}^{Prev}\right)$.

Security analysis

This section evaluates the security effectiveness of the proposed approach by conducting both formal and informal analyses to address the various security risks.

Formal security analysis

The suggested approach is evaluated by Burrows, Abadi, and Needham (BAN) logic to assess its security properties.

The postulates of the BAN logic is given as follows.

Message-meaning rule (R_1) : $\frac{P|\equiv P \underset{\leftrightarrow}{K} Q, P \lhd \{X\}_K}{P|\equiv Q|\sim X}$

$$\text{Nonce} - \text{verification rule } (R_2)\ :\ \frac{P|\equiv\ \#(X),\ P|\equiv\ Q|\sim\ (X)}{P|\equiv\ Q|\equiv\ X}$$

Jurisdiction rule (R_3) : $\frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$

Freshness rule (R_4) : $\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$

Belief rule (R_6) : $\frac{P|\equiv Q|\equiv (X,Y)}{P|\equiv Q|\equiv (X)}$

The following are the preliminary security assumptions for the suggested approach.

Let $WBAN_j$ be the WBAN Controller, and MD_{ij} the Monitoring Device.

Assumptions • $WBAN_j$ and MD_{ij} share $K_{Session}$, derived securely through the protocol.

- Nonces N_{WBAN_j} and $N_{MD_{ij}}$ are fresh and random.
- SID is fresh and unique to each session.
- $WBAN_j$ and MD_{ij} believe that each other has jurisdiction over the session key.

Logical beliefs:

- $WBAN_j|\equiv\ \#N_{WBAN_j}$: $WBAN_j$ believes that the nonce N_{WBAN_j} is fresh.
- $MD_{ij}|\equiv\ \#N_{MD_{ij}}$: MD_{ij} believes that the nonce $N_{MD_{ij}}$ is fresh.
- $MD_{ij}|\equiv\ \#SID$: MD_{ij} believes that the session identifier SID is fresh.
- $WBAN_j|\equiv\ \#SID$: $WBAN_j$ believes that the session identifier SID is fresh.
- $WBAN_j|\equiv\ WBAN_j \underset{\longleftrightarrow}{K_{Session}} MD_{ij}$: $WBAN_j$ believes that it securely shares the session key $K_{Session}$ with MD_{ij}.
- $MD_{ij}|\equiv\ MD_{ij} \underset{\longleftrightarrow}{K_{Session}} WBAN_j$: MD_{ij} believes that it securely shares the session key $K_{Session}$ with $WBAN_j$.

To show how the suggested approach is secure enough, you would need to comply with at least these specific requirements,

G_1: **Mutual authentication**.

- $WBAN_j| \equiv \ MD_{ij}| \equiv \ WBAN_j \underset{\longleftrightarrow}{K_{Session}} MD_{ij}$: $WBAN_j$ believes that MD_{ij} shares the session key $K_{Session}$.
- $MD_{ij}| \equiv \ WBAN_j| \equiv \ WBAN_j \underset{\longleftrightarrow}{K_{Session}} MD_{ij}$: MD_{ij} believes that $WBAN_j$ shares the session key $K_{Session}$.

G_2: **Key secrecy**.

- $WBAN_j| \equiv \ WBAN_j \underset{\longleftrightarrow}{K_{Session}} MD_{ij}$: $WBAN_j$ believes that the session key $K_{Session}$ is securely shared with MD_{ij}.
- $MD_{ij}| \equiv \ MD_{ij} \underset{\longleftrightarrow}{K_{Session}} WBAN_j$: MD_{ij} believes that the session key $K_{Session}$ is securely shared with $WBAN_j$.

G_3: **Freshness of $\boldsymbol{K_{Session}}$.**

- $WBAN_j| \equiv \ \#\left(K_{Session}\right)$: $WBAN_j$ believes that the session key $K_{Session}$ is fresh.
- $MD_{ij}| \equiv \ \#\left(K_{Session}\right)$: MD_{ij} believes that the session key $K_{Session}$ is fresh.

The following steps are used to obtain the anonymous authentication (among $WBAN_j$ and MD_{ij} using the above criteria assisted with assumptions).

Protocol idealized messages Let $WBAN_j$ be the WBAN Controller, and MD_{ij} the Monitoring Device.

The idealized protocol steps are expressed as follows:

M1: MD_{ij} to $WBAN_j$: $\left\{UID_{MD_{ij}},\ R_{MD_{ij}},\ SID,\ TS_i\right\}$, where $R_{MD_{ij}} = PUF\left(C_{WBAN_j}\right) \oplus H\left(TID_{MD_{ij}} \parallel \ N_{MD_{ij}}\right)$,and $SID = H\left(N_{MD_{ij}} \parallel \ N_{WBAN_j} \parallel \ TS_i\right)$.

M2: $WBAN_j$ **to** MD_{ij}: $\left\{UID_{WBAN_j},\ R_{WBAN_j},\ SID,\ N_{WBAN_j}\right\}$, where $R_{WBAN_j} = PUF\left(C_{WBAN_j}\right) \oplus H(UID_{WBAN_j} \parallel \ N_{WBAN_j})$.

Step 1: $\boldsymbol{MD_{ij}}$ **sends M1 to** $\boldsymbol{WBAN_j}$:

1. $WBAN_j$ computes $R'_{MD_{ij}} = PUF\left(C_{WBAN_j}\right) \oplus H\left(TID_{MD_{ij}} \parallel \ N_{MD_{ij}}\right)$.
2. If $R'_{MD_{ij}} = R_{MD_{ij}} \rightarrow \ WBAN_j \lhd R_{MD_{ij}}$ and infers: $WBAN_j| \equiv \ MD_{ij}| \sim R_{MD_{ij}}$ (message meaning rule R1).
3. Since $WBAN_j| \equiv \ \#N_{MD_{ij}} \rightarrow$ By Nonce Verification Rule (R2): $WBAN_j| \equiv \ MD_{ij}| \equiv \ R_{MD_{ij}}$.
4. SID check: $SID = H\left(N_{MD_{ij}} \parallel \ N_{WBAN_j} \parallel \ TS_i\right)$, Since SID binds both nonces and timestamp: $WBAN_j| \equiv \ \#SID$.

Step 2: $\boldsymbol{WBAN_j}$ **sends M2 to** $\boldsymbol{MD_{ij}}$.

1. MD_{ij} receives $\left\{UID_{WBAN_j},\ R_{WBAN_j},\ SID,\ N_{WBAN_j}\right\}$, computes $R'_{WBAN_j} = PUF\left(C_{WBAN_j}\right) \oplus H(UID_{WBAN_j} \parallel \ N_{WBAN_j})$.
2. If $R'_{WBAN_j} = R_{WBAN_j} \rightarrow \ MD_{ij}| \equiv \ WBAN_j| \sim R_{WBAN_j}$.
3. $MD_{ij}| \equiv \ \#N_{WBAN_j} \rightarrow$ By Nonce Verification Rule (R2): $MD_{ij}| \equiv \ WBAN_j| \equiv \ R_{WBAN_j}$.
4. Both agree on SID → shared session context.

Step 3: Session key agreement.

1. Both MD_{ij} and $WBAN_j$ computes $K_{Session} = H\left(R_{MD_{ij}} \parallel \ R_{WBAN_j} \parallel \ K_{Session}^{Prev} \parallel \ SID\right)$.
2. Since both MD_{ij} and $WBAN_j$ believe that $R_{MD_{ij}},\ R_{WBAN_j}$ values and SID are fresh:

   - $MD_{ij}| \equiv \ \#\left(K_{Session}\right)$
   - $WBAN_j| \equiv \ \#\left(K_{Session}\right)$

By Jurisdiction Rule (R3):

- $MD_{ij}| \equiv \ WBAN_j \Rightarrow \ K_{Session}$, and $MD_{ij}| \equiv \ WBAN_j| \equiv \ K_{Session} \rightarrow \ MD_{ij}| \equiv \ K_{Session}$.
- Similarly, $WBAN_j| \equiv \ MD_{ij}| \equiv \ K_{Session}$.

$WBAN_j$ and MD_{ij} achieve mutual authentication. Both entities believe that $K_{Session}$ is securely shared and authenticated. Further, $K_{Session}$ is securely derived and shared exclusively between $WBAN_j$ and MD_{ij}. The use of fresh nonces $\left\{N_{WBAN_j},\ N_{MD_{ij}}\right\}$ and unique session identifiers (SID) ensures that $K_{Session}$ remains fresh and unique for every session.

Informal security analysis

Mutual authentication Certain values of cryptographic verification are used in the flow of the proposed protocol to accomplish the $WBAN_j$ and MD_{ij} authentication. Each of the entities checks the identity of the counterpart through challenge-response values generated by the $PUFs$. By using dynamic nonces $N_{WBAN_j},\ N_{MD_{ij}}$, and unique SID, the protocol ensures that only authorized entities can engage in safe communications, making it easy to achieve mutual authentication.

Replay attack resistance Replay attacks are prevented by using time-bound session-specific tokens (TS_i) and distal nonce $\left(N_{WBAN_j},\ N_{MD_{ij}}\right)$ for every communication cycle. To ensure freshness, the receiver validates the timestamp by checking whether $|TS_j - TS_i| \leq \Delta T$, where TS_j is the local time and ΔT is a predefined threshold that accommodates network latency, processing delays, and possible clock drift in wireless environments. In case an adversary (Λ) tries to resume an eavesdropped session, the timestamps or the nonces is checked and found invalid and thus, the session is denied. This dynamic approach eliminates any possibility of the system being undermined by old or duplicate messages.

Impersonation attack resistance The proposed scheme helps to avoid impersonation attacks because the responses and cryptographic keys are generated from the PUF of a device. An adversary (Λ) who wants to impersonate either $WBAN_j$ or MD_{ij} would require open access to secret keys $\left(s_{WBAN_j},\ s_{MD_{ij}}\right)$ and unique responses $\left(R_{WBAN_j},\ R_{MD_{ij}}\right)$ which are safely stored out of reach of the adversary. But, the inclusion of the cryptographic parameters for instance hashed challenge-response pair makes it possible to thwart any impersonation.

Session key secrecy Session keys ($K_{Session}$), are also dynamic and are computed based on other parameters such as nonces $\left(N_{WBAN_j},\ N_{MD_{ij}}\right)$, PUFresponse and session ID (SID) for each communication session. In an additional level of security, all subsequent session keys derived from the current master key will not be affected in any way should an opponent get hold of an earlier session key. It ensures forward secrecy so that at the end of each session no means can be traced to subsequent sessions.

User anonymity $TID_{MD_{ij}}$ preserving user anonymity through the dynamically updated pseudonymous identifiers. These identifiers are refreshed between each session avoiding an adversary (Λ) from linking communication sessions to specific users. Hence, in the proposed scheme, the secret information remains hidden, even when transmitted over a public channel.

Forward secrecy The suggested scheme achieves forward secrecy, in which a new session key $K_{Session}$ is established for each session, and is dependent on fresh inputs such as nonces $\left(N_{WBAN_j},\ N_{MD_{ij}}\right)$ and PUF responses $\left(R_{WBAN_j},\ R_{MD_{ij}}\right)$. If long-term keys (resp. credentials) are ever compromised past session keys cannot be reconstructed and retroactive attacks are shielded against communication past while keys have remained valid. It guarantees a very high level of data confidentiality that does not change over time.

Resistance to physical attacks Inherent resistance to physical attacks is achieved by using $PUFs$. If the adversary (Λ) can tamper the device to extract cryptographic parameters, then the PUF would be nonfunctional and the stored data useless. Also, $PUFs$ possess additional tamper detection mechanisms that notify the system if there is a probable breakage.

Insider attack resistance Even though an insider registers as a legitimate user, they cannot recover the session keys of other users as PUF responses and cryptographic credentials are unique to a device. Sensitivity of parameters, which can be sensitive inputs like $\alpha_{MD_{ij}} = H\left(TID_{MD_{ij}} \parallel s_{FN_i}\right)$, depends on inputs that must be securely distributed and are inaccessible to unauthorized entities.

Resistance to temporary secret key leakage The protocol resists temporary secret key leakage because the computation of session keys involves independent unique parameters like nonces $\left(N_{WBAN_j},\ N_{MD_{ij}}\right)$, PUF responses $\left(R_{WBAN_j},\ R_{MD_{ij}}\right)$, and cryptographic keys. Although Λ gets at least some data (such as a partial nonce), without complete knowledge of all necessary data, an adversary is not able to deduce the session key.

Resistance to cloning attacks Device-specific $PUFs$ guarantee that no two devices have the same challenge-response behaviour. Cloning of devices is prevented by this, as duplication of a PUF is computationally infeasible. In the domain of $PUFs$, any attempt to mimic a genuine device would inevitably fail because PUF responses are unique and unpredictable.

Resistance to desynchronization attacks The proposed authentication scheme resists desynchronization attacks by design, as it avoids storing or updating any state-dependent variables across sessions. Each authentication instance independently uses fresh nonces $N_{MD_{ij}}$ and N_{WBAN_j} along with a timestamp TS_i to derive the session identifier $SID = H\left(N_{MD_{ij}} \parallel N_{WBAN_j} \parallel TS_i\right)$. The PUF-based responses $R_{MD_{ij}} = PUF\left(C_{WBAN_j}\right) \oplus H\left(TID_{MD_{ij}} \parallel N_{MD_{ij}}\right)$ and $R_{WBAN_j} = PUF\left(C_{WBAN_j}\right) \oplus H(UID_{WBAN_j} \parallel N_{WBAN_j})$ are computed afresh for each session and not reused. The session key $K_{Session} = H\left(R_{MD_{ij}} \parallel R_{WBAN_j} \parallel K_{Session}^{Prev} \parallel SID\right)$ is also derived dynamically without requiring synchronization of counters or helper data. As all parameters are freshly generated and not dependent on previous session success, failed or dropped sessions do not cause state mismatch, thus ensuring desynchronization resistance.

Performance analysis

In this section, we analyze the performance efficiency of the proposed approach by examining parameters such as the computational overhead, communication overhead, and security attributes.

Computational overhead

To analyze the computational overhead of the proposed scheme, the time consumed by the important cryptographic operations such as the hash function (T_H), PUF (T_{PUF}), reverse fuzzy extractor (T_F), scalar multiplication (T_M) and symmetric cryptography (T_S) of the suggested protocols are considered in this section. The proposed approach is evaluated using Ubuntu 14.04 VMware with an Intel Core i5-8265U processor and an 8-GB RAM system. The simulation work was carried out using the JCE library Pbc-05.14 and the computational overhead of different cryptographic operations, such as T_H, T_{PUF}, T_F, T_M, and T_S are calculated as 0.011 ms $(millisecond)$, 0.12 ms, 2.53 ms, 2.6 ms, and 0.041 ms respectively. Table 2 lists the computational overhead of various methods, and it ensures that the suggested approach consumes only 3.024 ms to establish a session key, whereas other related existing approaches[23–26], consume 8.47 ms, 8.04 ms, 5.77 ms, and 15.79 ms as a communication overhead.

It is important to note that the performance evaluation was conducted on a system with Intel Core i5-8265U processor and 8 GB RAM running Ubuntu 14.04, selected to represent a constrained computing environment typical of edge or wearable WBAN devices. While this configuration helps simulate real-world resource limitations, we acknowledge that results may vary on modern edge computing platforms with advanced processors (e.g., ARM Cortex-A76, Intel i7/i9, or Raspberry Pi 5-level SoCs). Performance profiling on such contemporary hardware platforms will be considered in our future work to generalize the findings across broader deployment scenarios.

Figure 2 compares the computational overhead of the proposed approach with those of other existing competitive schemes[23–26] and ensures the efficiency of the proposed approach.

Communication overhead

We analyze the total number of messages exchanged as well as the size of the data transmitted in the session establishment phase of the proposed authentication scheme to evaluate the communication overhead. Calculating all parts of the transmitted messages, including identifiers, nonces, hashed values, and challenge-response pairs. The scheme consists of four message exchanges among system entities during authentication and session key establishment. The total size of the first message (M1) sent from the WBAN Controller to a Fog Node is 64 bytes including a unique identifier16 bytes, a nonce of 16 bytes, and a hashed value of 32 bytes. The second message (M2) that the Monitoring Device sends to the Fog Node contains a Unique Identifier of 16 bytes, a nonce of 16 bytes, and a hash of 32 bytes, for a total of 64 bytes. The third message (M3) sent from the Fog Node to the WBAN Controller is a challenge-response pair of 16 bytes, a hashed value of 32 bytes, and a total size of 48 bytes. The Fog Node also sends a message (M4) to the Monitoring Device with 48 bytes, which contains a challenge-response pair of 16 bytes and a hashed value of 32 bytes, for a total of 48 bytes.

The total communication overhead of the proposed scheme is the sum of the following message sizes: 64 + 64 + 48 + 48 = 224 bytes. In a resource-constrained WBAN environment, this efficient design reduces data transmission while keeping robust authentication and session key establishment process[28]. Table 3 lists the communication overhead of various methods.

A proposed scheme is shown to exhibit the lowest communication overhead among compared methods while preserving robust security features. This scheme provides a highly efficient communication protocol by reducing the size and number of transmitted parameters. This efficiency makes this protocol especially attractive for WBAN environments with resource constraints, where there is a need to minimize bandwidth and energy consumption. Figure 3 compares the communication overhead of the proposed scheme with other competitive schemes and shows that the proposed scheme outperformed other independent schemes in terms of reduced data transmission.

Security attributes

The security attributes of the proposed approach were evaluated and compared with other related schemes[23–26] to ensure its performance efficiency. Table 4 compares the security attributes of the proposed approach and related schemes.

The data in Table 4 demonstrate that the examined technique safeguards against unauthorised user device, replay, user anonymity, forward secrecy, and physical attacks. Conversely, schemes[23,25] lack support for security aspects such as impersonation attacks and insider attacks. Similarly, the method in[24] lacked protection against

Methods	$WBAN_j$	FN_i	MD_{ij}	Total
[24]	$2T_S + 8T_H + T_F$	$5T_S + 11T_H + T_F$	$2T_S + 6T_H + T_F + 2T_{PUF}$	$9T_S + 25T_H + 3T_F + 2T_{PUF} = 8.474ms$
[25]	$14T_H + 2T_F + T_{PUF}$	$8T_H$	$8T_H + T_F$	$30T_H + 3T_F + T_{PUF} = 8.04ms$
[26]	$T_S + 10T_H + T_F$	$4T_S + 9T_H$	$3T_S + 5T_H + T_F + T_{PUF}$	$8T_S + 24T_H + 2T_F + T_{PUF} = 5.772ms$
[27]	$3T_M + 6T_H$	$T_M + 6T_H$	$2T_M + 6T_H$	$6T_M + 18T_H = 15.798ms$
Suggested scheme	$15T_H$	$12T_H$	$7T_H + T_F + T_{PUF}$	$34T_H + T_F + T_{PUF} = 3.024ms$

Table 2. Computational overhead of various schemes.

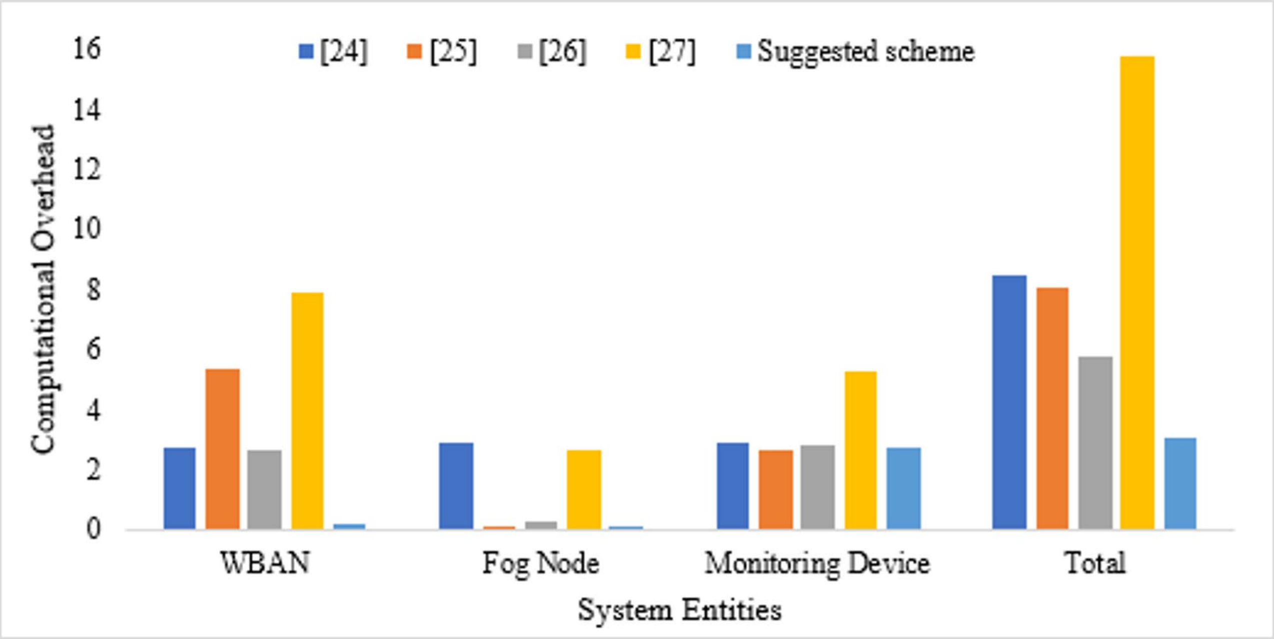

Fig. 2. Computational overhead of various methods.

Methods	No. of messages	Overhead (bytes)
[24]	4	356
[25]	5	360
[26]	6	456
[27]	4	372
Suggested scheme	4	224

Table 3. Communication overhead of various schemes.

impersonation attacks. The[26] scheme also lacks security features such as authentication, impersonation attacks, and temporary secret key leakage attacks. Conversely, the proposed strategy encompasses all the security attributes delineated in Table 4.

Storage overhead

The storage requirements for each entity in the proposed system are as follows: All registered devices need to have $CRPs$ stored in the CS. It takes $16 \times 2 = 3216 \times 2 = 32$ bytes for $CRPs$ each device. It also has to store the master keys of other entities in the system: s_{CS}, s_{FN_i} and s_{WBAN_j}, for a total of $3 \times 16 = 48$ bytes$3 \times 16 = 48$bytes. Additionally, it keeps track of the $UIDs$ of all devices, consuming 16 bytes per device. The total storage requirement for the CS is $32 + 48 + 16 = 96$ bytes.

For Fog Node, it must store the $CRPs$ $16 \times 2 = 32$ bytes, shared key 16 bytes, and $UIDs$ refrigerate joined contraptions as 16 bytes. The total fog node storage requirement is 64 bytes. The WBAN Controller must store the $CRPs$ $16 \times 2 = 32$ bytes, The WBAN specific key 16 bytes, and the Nonces and Temporary Identifiers $2 \times 16 + 32 = 64$ bytes. In total, the WBAN controller must store $32 + 16 + 64 = 112$ bytes. The monitoring device must store the monitoring device key 16 bytes, Nonces, and Temporary Identifiers $2 \times 16 + 32 = 64$ bytes. In total, the monitoring device must store $16 + 64 + 16 = 96$ bytes.

Conclusion

In this paper, a physically secure and fog-capable lightweight authentication scheme for WBANs is presented. WBAN environments introduce specific challenges that the proposed framework addresses by combining the decentralised processing power of fog computing with the hardware-based security of PUFs. As shown by the proposed scheme, the reduction in the computational overhead is 64.33%, whereas the reduction in the communication overhead grid is 29.58% compared to the existing state-of-the-art WBAN devices. Results from the security analysis show that the proposed framework is robust against a variety of attack vectors, such as impersonation, replay, insider, and tampering. The scheme also accommodates key security properties, including mutual authentication, user anonymity, forward secrecy, and compromise resilience to temporary secret key leakages. Storage overhead analysis shows the context in which cryptographic parameters are stored by different

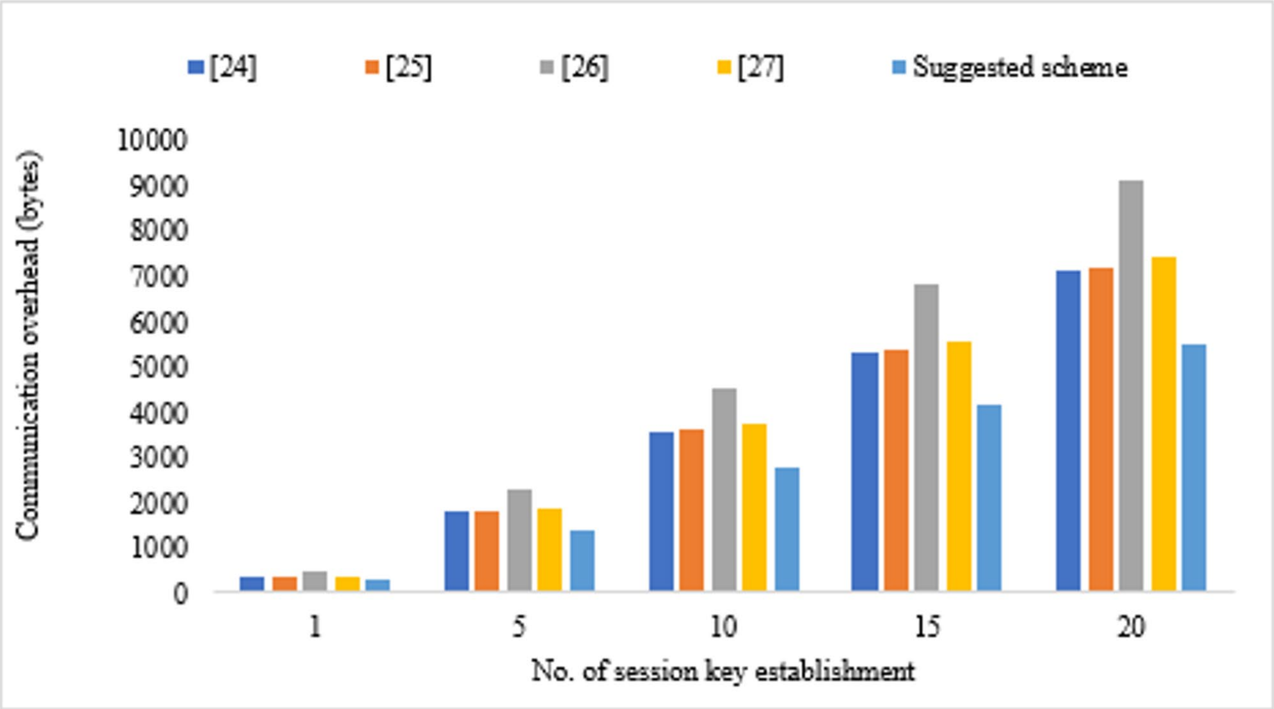

Fig. 3. Communication overhead of various schemes.

Security attributes	[24]	[25]	[26]	[27]	Suggested scheme
Authentication	*Yes*	*Yes*	*Yes*	*No*	*Yes*
Unauthorized User Device Attack	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Impersonation Attack	*No*	*No*	*No*	*No*	*Yes*
Replay Attack	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
User Anonymity	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Forward Secrecy Attack	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Temporary Secret Key Leakage Attack	*Yes*	*Yes*	*Yes*	*No*	*Yes*
Insider Attack	*No*	*Yes*	*No*	*Yes*	*Yes*
Physical Attack	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Table 4. Security attributes of various schemes.

actors, such that security is traded for resource efficiency. It provides a scalable, energy-efficient, and secure framework for WBANs using integration of lightweight cryptographic protocols, fog-enabled architecture, and PUF-based authentication. The results presented in this work provide a solid foundation for future research to further improve the scalability and adaptability of WBANs operating in a fog-enabled IoT ecosystem.

Data availability

The dataset underlying this study is publicly available on Figshare at 10.6084/m9.figshare.28540859.

Received: 26 May 2025; Accepted: 14 August 2025
Published online: 21 August 2025

References

1. Bhatti, D. S. et al. A survey on wireless wearable body area networks: A perspective of technology and economy. *Sensors* **22** (20), 7722 (2022).
2. Humayun, M., Jhanjhi, N. Z., Hamid, B. & Ahmed, G. Emerging smart logistics and transportation using IoT and blockchain. *IEEE Internet Things Magazine*. **3** (2), 58–62 (2020).
3. Dinarvand, N. & Barati, H. An efficient and secure RFID authentication protocol using elliptic curve cryptography, Wireless Networks, vol. 25, no. 1, pp. 415–428, Jan. (2019).
4. Ashok, K. & Gopikrishnan, S. Statistical analysis of remote health monitoring based IoT security models & deployments from a pragmatic perspective. *IEEE Access*. **11**, 2621–2651 (2023).

5. Singh, N. & Das, A. K. TFAS: two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor. *J. Supercomputing*. **80** (1), 865–914 (2024).
6. Ataei Nezhad, M., Barati, H. & Barati, A. An authentication-based secure data aggregation method in Internet of Things, Journal of Grid Computing, vol. 20, no. 3, p. 29, Sep. (2022).
7. Subramani, J. et al. Blockchain-enabled secure data collection scheme for fog-based WBAN. *IEEE Access*. **12** (2024).
8. Mirsaraei, A. G., Barati, A. & Barati, H. A secure three-factor authentication scheme for IoT environments. *J. Parallel Distrib. Comput.* **169**, 87–105 (2022).
9. Al-Meer, A. & Al-Kuwari, S. Physical unclonable functions (PUF) for IoT devices. *ACM Comput. Surveys*. **55** (14s), 1–31 (2023).
10. Zargar, G. R., Barati, H. & Barati, A. An authentication mechanism based on blockchain for IoT environment. *Cluster Comput.* **27** (9), 13239–13255 (2024).
11. Singh, M. B., Taunk, N., Mall, N. K. & Pratap, A. Criticality and utility-aware fog computing system for remote health monitoring. *IEEE Trans. Serv. Comput.* **16** (3), 1738–1749 (2022).
12. Khajehzadeh, L., Barati, H. & Barati, A. A lightweight authentication and authorization method in IoT-based medical care. *Multimedia Tools Appl.* **1**, 1–40 (2024).
13. Yıldırım, E., Cicioğlu, M. & Çalhan, A. Fog-cloud architecture-driven internet of medical things framework for healthcare monitoring. *Med. Biol. Eng. Comput.* **61** (5), 1133–1147 (2023).
14. Wang, W. et al. Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. *IEEE Internet Things J.* **9** (11), 8883–8891 (2021).
15. Priya, J. C., Praveen, R., Nivitha, K. & Sudhakar, T. Improved blockchain-based user authentication protocol with ring signature for internet of medical things. Peer-to-Peer networking and applications. May **13**:1–20. (2024).
16. Chbaik, N., Khiat, A., Bahnasse, A. & Ouajji, H. Blockchain-assisted IoT wireless framework for equipment monitoring in smart supply chain: a focus on temperature and humidity sensing. IEEE Access. Aug 23. (2024).
17. Zhang, J. & Dong, C. Secure and lightweight data aggregation scheme for anonymous multi-receivers in WBAN. *IEEE Trans. Netw. Sci. Eng.* **10** (1), 81–91 (2022).
18. Delgado-Vargas, K., A, Gallegos-Garcia, G. & Escamilla-Ambrosio, P. J. Cryptographic protocol with keyless sensors authentication for WBAN in healthcare applications. *Appl. Sci.* **13** (3), 1675 (2023).
19. Ghaffar, Z. et al. A machine learning attack resilient and low-latency authentication scheme for AI-driven patient health monitoring system. *IEEE Commun. Stand. Magazine*. **8** (3), 36–42 (2024).
20. Saleem, M. A. et al. Provably secure authenticated key-management mechanism for e-healthcare environment. *IEEE Internet Things J.*, **12**(2025). Early Access.
21. Ghaffar, Z. et al. Security analysis on 'EAKE-WC: Authenticated key exchange protocol for wearable computing', in Proc. 2023 Int. Conf. on Intelligent Computing and Its Emerging Applications (ICICEA), Kuala Lumpur, Malaysia, Dec. pp. 148–153. (2023).
22. Mahmood, K. et al. Cloud-assisted secure and cost-effective authenticated solution for remote wearable health monitoring system. *IEEE Trans. Netw. Sci. Eng.* **10** (5), 2710–2718 (2022).
23. Liu, Z., Guo, C. & Wang, B. 'A physically secure, lightweight three- 1102 factor and anonymous user authentication protocol for iot'. *IEEE Access*. **8**, 195914–195928 (2020). 1103.
24. Chen, Y. & Chen, J. "An efficient mutual authentication and key agree- 1105 ment scheme without password for wireless sensor networks," J. Super- 1106 Comput., vol. 77, no. 12, pp. 13653–13675, Dec. (2021).
25. Xia, Y. et al. "PUF- 1108 assisted lightweight group authentication and key agreement protocol in 1109 smart home," Wireless Commun. Mobile Comput., vol. pp. 1–15, 1110 Mar. 2022. (2022).
26. Zou, S., Cao, Q., Wang, C., Huang, Z. & Xu, G. "A robust two1060 factor user authentication scheme-based ECC for smart home in 1061 IoT," IEEE Syst. J., vol. 16, no. 3, pp. 4938–4949, Sep. doi: 1062 (2022). https://doi.org/10.1109/JSYST.2021.3127438
27. Al-Meer, A. & Al-Kuwari, S. Physical unclonable functions (PUF) for IoT devices, ACM Computing Surveys, vol. 55, no. 14s, pp. 1–31, (2023).
28. Jegadeesan, S., Obaidat, M. S., Vijayakumar, P. & Azees, M. SEAT: secure and energy efficient anonymous authentication with trajectory privacy-preserving scheme for marine traffic management. *IEEE Trans. Green. Commun. Netw.* **6** (2), 815–824. https://doi.org/10.1109/TGCN.2021.3126618 (June 2022).

Author contributions

JS- Conceptualization, Formal analysis, Supervision, Resources, Validation, Writing – original draft, Writing – review & editingAR- Investigation, Resources, Formal analysis, Writing – original draft, Writing – review & editingAB- Supervision, Validation, Investigation, Writing – original draft, Writing – review & editingGAR- Supervision, Validation, InvestigationAll authors reviewed the manuscript.

Funding

Open access funding provided by Manipal Academy of Higher Education, Manipal

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to A.B.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.