IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

Enhancing WABAN Security using Biologically Inspired Cryptographic Keys

Sudip Das[1], Anusua Biswas[2], Subhomita Roy[3], Jinia Saha[4], Pritha Bhadra[5]
Assistant Professor, Department of Computer Application[1]
Students, Department of Computer Application[2-5]
Narula Institute of Technology, Kolkata, India

Abstract: *A paper on WBAN security proposes using biological data for key generation within an Advanced Encryption Standard (AES) framework to enhance data confidentiality and user authentication in health monitoring systems. The framework leverages patients' and doctors' unique biological characteristics to create unique encryption keys, providing strong security for sensitive medical data transmitted through the Wireless Body Area Network (WBAN). The study includes implementation in a cloud-based environment to evaluate end-to-end data transmission delay, offering practical insights and experimental results for a secure WBAN system with biological keys*

Keywords: Wireless Body Area Network (WBAN), Healthcare Security, Biological Key Generation, Physiological Signals, Electrocardiogram (ECG), Photoplethysmogram (PPG), Biometric Cryptography, Lightweight Encryption, Key Agreement Protocol, Privacy Preservation, Authentication, Energy-Efficient Security, Secure Data Transmission

I. INTRODUCTION

Technological advancement has revolutionized human life by transforming various domains, including healthcare, smart cities, industrial automation, and environmental monitoring. Despite these advancements, the healthcare sector continues to face several critical challenges. Among them, the most pressing is the rapidly growing global population coupled with a decreasing ratio of healthcare professionals and facilities. According to reports, the population of elderly individuals is expected to increase significantly in the coming years, and with aging comes a higher prevalence of chronic diseases. Elderly patients often require continuous medical supervision, and without timely diagnoses or interventions, their health conditions may lead to life-threatening outcomes. Studies have shown that many fatal diseases can be managed effectively if they are detected in their early stages. Therefore, there is a strong need to develop affordable, proactive, and intelligent healthcare systems that can provide continuous health monitoring outside traditional clinical environments.To address these challenges, researchers have introduced Wireless Body Area Networks (WBANs), a promising healthcare technology that enables real-time monitoring of patients' physiological signals. WBANs consist of smart biomedical sensor nodes (BSNs) that are either implanted in or worn on the human body. These nodes collect vital physiological data such as heart rate, electrocardiogram (ECG), blood pressure, and body temperature, and transmit it wirelessly to a medical centre for further analysis. WBANs reduce the need for patients to remain confined to hospitals, allowing them to maintain mobility and continue their routine activities while still being under continuous medical observation. This not only providesconvenience to patients but also reduces the burden on healthcare facilities.While WBANs originate from traditional Wireless Sensor Networks (WSNs), they differ due to their unique challenges and stringent requirements. A typical WBAN architecture consists of three tiers: Tier-1 (Intra-WBAN), which handles communication between biomedical sensors and a Body Node Coordinator (BNC); Tier-2 (Inter-WBAN), which enables communication between the BNC and external gateways or medical sites; and Tier-3 (Beyond-WBAN), which involves medical servers, doctors, and emergency services for advanced diagnosis and timely response. Each tier involves wireless communication of highly sensitive health data, making security and privacy a critical concern. The wireless nature of WBAN communication exposes it to numerous security threats such as eavesdropping, impersonation, data modification, replay attacks, and denial-of-service.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

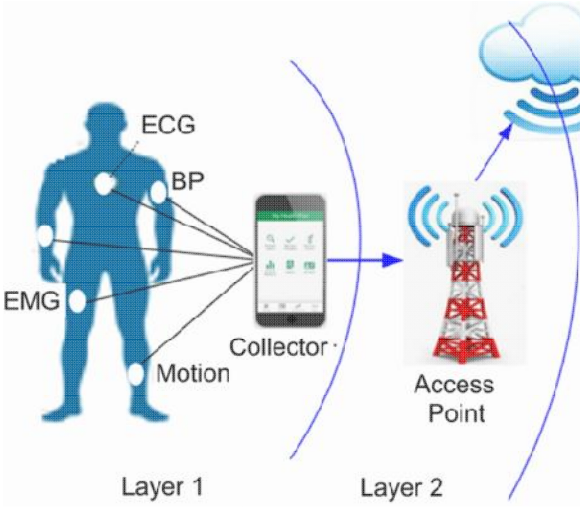


Figure 1: WBAN Security

Furthermore, WBAN devices are inherently resource-constrained, operating with limited battery power, memory, and processing capabilities, which makes the direct application of conventional cryptographic mechanisms infeasible. Hence, WBAN security requires lightweight, energy-efficient, and context-aware solutions that ensure confidentiality, integrity, authentication, and privacy preservation without imposing heavy computational overhead.In this context, novel approaches such as biological key-based security frameworks are gaining attention. By leveraging unique physiological signals like ECG and Photoplethysmogram (PPG), dynamic cryptographic keys can be generated, eliminating the need for pre-stored or static keys. Such solutions not only strengthen WBAN security but also align with its resource limitations, thereby offering a balanced framework for secure, efficient, and reliable healthcare monitoring.

II. WABAN SECURITY ARCHITECTURE

A Wireless Body Area Network (WBAN) is structured into a three-tier architecture, where each tier handles a specific level of communication and requires tailored security mechanisms. The overall goal of WBAN security architecture is to ensure confidentiality, integrity, authentication, and availability of medical data while maintaining low power consumption and efficiency due to the limited resources of biomedical sensor nodes.

A. Tier-1: Intra-WBAN Security: Communication among biomedical sensor nodes (BSNs) implanted in or worn on the body and a Body Node Coordinator (BNC).

Threats:

- Eavesdropping on physiological signals.
- Node cloning or impersonation.
- Data manipulation before reaching the BNC.

Security Requirements:

- Lightweight encryption due to limited resources.
- Biological key-based authentication (ECG/PPG-derived keys).
- Integrity verification to prevent data alteration.

Example: Use of ECG signal features to generate one-time session keys for secure communication between sensors and the BNC.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

B. Tier-2: Inter-WBAN Security: Communication between the BNC and external gateways, smartphones, or personal devices.

Threats:

- Man-in-the-Middle (MITM) attacks.
- Replay attacks.
- Unauthorized data interception.

Security Requirements:

- Strong mutual authentication between the BNC and gateway devices.
- Secure session key establishment protocols.
- Confidentiality mechanisms to prevent data leakage during wireless transmission.

Example: Lightweight key agreement protocols such as elliptic curve cryptography (ECC) combined with biological key seeds.

Tier-3: Beyond-WBAN Security: Communication between gateways and remote medical servers, cloud storage, hospitals, doctors, and emergency services.

Threats:

- Data breaches at medical databases.
- Privacy violations due to unauthorized access.
- Denial-of-Service (DoS) attacks targeting healthcare systems.

Security Requirements:

- Strong encryption algorithms (AES, RSA, ECC).
- Access control and role-based authentication for doctors and caregivers.
- Privacy-preserving storage and transmission (compliance with HIPAA, GDPR)

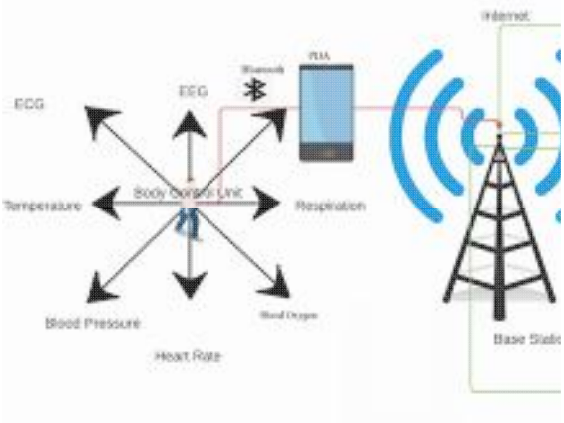


Figure 2: WBAN ARCHITECTURE

III. CASE STUDY

Wireless Body Area Networks (WBANs) are an emerging class of networks designed to connect small, wearable or implantable devices on or inside the human body. These devices monitor physiological parameters such as heart rate, glucose levels, oxygen saturation, or brain activity, and transmit the data wirelessly to a coordinating hub, often a smartphone or a medical server. The information they carry is highly sensitive, which makes the security of WBANs an essential concern. Unlike conventional wireless networks, WBAN devices are severely resource-constrained in terms of power, memory, and processing capacity, which renders heavyweight cryptographic approaches unsuitable. This case study explores the design and implementation of a biological key-based security framework for WBANs, focusing on the use of the electrocardiogram (ECG) signal as a dynamic cryptographic key. The system designed in this study

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

consists of several layers. At the bottom are sensor nodes, each capable of collecting physiological data such as ECG (electrocardiogram), EEG (electroencephalogram), and PPG (photoplethysmography) are collected by body sensors. The generated keys are then used to establish secure communication between WBAN nodes and the coordinator. Lightweight cryptographic algorithms, such as AES-128 or authenticated ciphers like ASCON, encrypt the medical data. Since keys are derived dynamically from live physiological signals, they provide forward secrecy and eliminate the need for long-term key storage. biological key-based frameworks represent a promising solution for WBAN security. They leverage the uniqueness and availability of physiological signals to generate lightweight, patient-specific encryption keys, overcoming many of the challenges posed by traditional cryptographic methods. Future work points toward integrating multiple biosignals, using machine learning for improved feature extraction, and developing standardized protocols for deployment in real-world healthcare applications.

State of The Art Security In WABAN

WBAN security today sits at the intersection of constrained-device cryptography, biometric-derived authentication, network/protocol hardening, and privacy-preserving data handling. The established standard for medical/body-area networking is **IEEE 802.15.6**, which provides three security levels (unsecured, authentication-only, and authentication encryption) and defines master/pairwise/group key management—but the standard's key-agreement procedures have known weaknesses and several academic works have proposed fixes and hardening measures. Beyond single-signal systems, **multi-modal biometric fusion** (e.g., combining ECG + PPG or ECG + accelerometer/gait) is rising as a way to increase entropy and robustness to motion/artifact. Multi-modal systems reduce false-rejection and improve key reproducibility under real-world conditions, at the cost of slightly more computation and sensor set. Systematic reviews and surveys from 2023–2024 emphasize this trend and recommend hybrid designs for deployment scenarios where reliability is critical.

Authors, year of publication	Security parameters considered	Security technique (biological / non-biological key)	Experiment done	Security attack	Energy efficient	Computational complexity	Accuracy
Junqing Zhang, Y. Zheng et al., 2021	Authentication, confidentiality	**Biological key:** ECG + PPG heartbeat-based key generation using fuzzy reconciliation	Public MIT-BIH ECG + PPG datasets; hardware testbed	Resists eavesdropping, replay	Moderate efficiency in prototype	Medium (signal processing + reconciliation)	Robust key agreement, stable performance
Divya S., K.V. Prema, B. Muniyal, 2023	Key generation, confidentiality	**Biological key:** ECG-based randomness tested via runs/frequency tests	MATLAB simulation on MIT-BIH ECG	Eavesdrop, data leakage	Yes (lightweight implementation)	Low (statistical tests only)	62.5% Hamming distance (~80 bits distinctiveness)
J. Wang, 2023	Data confidentiality	**Biological-like key:** EEG signal + chaotic system hybrid encryption	Analytical/simulation study	Defends against statistical & brute-force	Not reported	Medium-high (chaos + EEG integration)	Strong encryption claims but no real dataset test
Ali Abdelli et al., 2024	Data confidentiality, integrity	**Non-biological key:** Lightweight encryption using chaotic KLEIN_64 + Keccak-256	FPGA (Zybo Z7-010) implementation	Statistical/randomness attacks	Yes, optimized for IoT/WBAN	Low-medium (FPGA optimized)	Throughput 2.82 Gbps, passed NIST randomness tests
Masdari et al., 2024	Data hiding, confidentiality	**Biological key:** ECG-based steganography for WBAN security	Theoretical/security framework	Data modification, unauthorized access	Not specified	Not specified	Conceptual accuracy, not experimentally validated
Wei Shao et al., 2025	Continuous authentication	**Biological key:** PPG-based authentication using Bi-LSTM + attention	Real smartwatch + public datasets	Spoofing, replay, impersonation	Yes (25 Hz sampling saves 53% power)	Medium-high (ML inference)	Accuracy 88.11%, FAR 0.48%, FRR 11.77%, EER 2.76%

Table 1. Comparison table summarizing the state-of-the art work on WABAN security.

Security Techniques in WBAN (Wireless Body Area Network)

Wireless Body Area Networks (WBANs) deal with highly sensitive medical data, which makes security and privacy one of the most critical concerns. Security techniques in WBAN are generally designed to achieve the following core objectives:

Confidentiality: Only authorized entities (e.g., doctors) should access patient data.

Technique: Encryption (AES, RSA, ECC).

DOI: 10.48175/IJARSCT-28932

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

Integrity: The data should not be altered or tampered with during transmission.
Technique: Hash Functions (SHA-256, MD5), Digital Signatures.
Authentication: Both patients and doctors must be properly identified before data access.
Technique: Biometric authentication (ECG, palm, thumb, iris), password or certificate-based login.
Availability: The system should be resilient to attacks (like DoS) and ensure reliable access to patient data.
Technique: Intrusion detection systems, secure routing.

1. **Cryptography-based Techniques**:
Symmetric Key Cryptography (e.g., AES, DES, 3DES):Same key for encryption and decryption.
Fast and lightweight, but key distribution is challenging.
Asymmetric Key Cryptography (e.g., RSA, ECC):Public and private keys are different.
Provides stronger security, but consumes more energy, which is a limitation for resource-constrained WBAN nodes.

2. **Biometric-based Techniques**
Biometrics are used to generate encryption keys or for authentication, since physiological signals are unique to individuals.
ECG signals: Every person's ECG is unique, making it a strong candidate for key generation.
Palm/Thumb impressions: Used to generate unique cryptographic keys.
Iris/Retina scans: Very secure but costly and energy-intensive.
Advantage: Highly unique, difficult to replicate.
Limitation: Requires additional sensors and increases cost/energy usage.

3. **Lightweight Security Protocols**
Because WBAN devices are energy, memory, and computation constrained, lightweight solutions are crucial.
TinySec, MiniSec – energy-efficient encryption protocols. Lightweight ECC – elliptic curve cryptography adapted for constrained devices.
Hash-based authentication – ensures low computation overhead.

4. **Trust and Identity Management**
Trust models are introduced to manage reliable communication among WBAN nodes.
If a node exhibits suspicious behavior (e.g., transmitting false data), it can be blocked.
Helps to reduce insider threats and compromised nodes.

5. **Secure Key Management Random Key Pre-distribution**: Keys are preloaded in nodes before deployment.
Dynamic Key Generation: Keys are generated in real-time from biometric data.
Physiological Signal-based Keying: Signals like ECG, pulse, or PPG are used for on-demand key creation.

6. **Intrusion Detection and Attack MitigationWBAN must defend against several types ofattacks:**
Eavesdropping: Unauthorized interception of patient data.
Replay Attacks: Reuse of intercepted messages.
Man-in-the-Middle: Intercepting and modifying communications.
Impersonation Attack: Attacker pretends to be a patient or doctor.
Denial of Service (DoS): Disrupts availability of WBAN services.
Techniques: Intrusion Detection Systems (IDS), anomaly-based monitoring.7. Emerging Research Trends
Blockchain-based WBAN Security:Provides decentralized, tamper-proof data sharing.
AI/ML-driven Intrusion Detection:Machine learning models detect abnormal traffic patterns in WBAN.
Energy-efficient Cryptography:Cryptographic algorithms optimized for low-power devices.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

Cloud and Edge Computing Integration:Pre-processing data at the edge before sending to cloud reduces risks and delays.

Proposed Work

The proposed work provides a secure communication framework for WBAN (Wireless Body Area Network). It ensures confidentiality, authentication, and integrity of patient's health data during transmission between sensors, Body Control Unit (BCU), and cloud servers.

Our method introduces a two-level security approach:

Biological-key based authentication and key generation

Lightweight AES-based encryption for WBAN resource constraints

It works in three phases:

A. Registration: When a new patient is registered, his/her unique sensor ID and biometric feature (e.g., ECG signal, heartbeat pattern, or fingerprint) are stored in the WBAN cloud database. Similarly, the doctor's biometric/ID is also registered for authentication.

B. Key Generation, Authentication, and Encryption:

At the time of communication, a session key is generated using patient's ECG/heartbeat-based features combined with a secure timestamp.

Authentication of both sensor nodes and doctor's device is done before data access.

Patient's physiological data is encrypted using AES (128/192/256-bit depending on keysize) before transmission.

C. Secure Data Transmission:

Encrypted health data is transmitted from WBAN sensors → BCU → Cloud server.

The doctor receives encrypted data and the session key, allowing decryption only if authentication is valid.

This ensures end-to-end confidentiality and secure retrieval of sensitive medical data.

Proposed Algorithm:

Notations used are as follows:

Notations Used

sensor request: Data request from WBAN sensor

sensor info: Biometric/ECG feature of patient stored in server

doctor info: Doctor's biometric/ID stored in server

patient data: Physiological readings (ECG, BP, SpO2, etc.)

keysize: Size of session key (128, 192, 256 bits)

n: Number of physiological parameters collected

Algorithm1: *Sensor data to Matrix conversion*
Input: Sensor signal (ECG/Heartbeat)
Output: Patient physiological matrix
Collect sensor signal
Convert signal into sampled data sequence
Normalize readings
Store in patient info matrix
Output patient info

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

102	118	95	110	87	120
99	105	113	124	92	108
115	97	121	109	101	112
89	130	106	98	117	103
111	122	100	108	114	90
95	104	116	119	107	123

Figure 3: A sub-matrix of Biometric/ECG feature image matrix

Algorithm 2: *KeyGen(Keysize)*

Input: patient_info, keysize
Output: Session key
Extract feature values (e.g., R-R intervals of ECG)
Select sub-matrix values within defined range
Computer random elements using feature selection
V2[i]:= selected random elements
V3 := Current system timestamp (DDMMYYYYHHMMSS)
Key := contact(v2, v3)
Return(key)
Switch (keysize):
Case 128->keygen(128)
Case 192 ->keygen(192)
Case 256 ->keygen(256)

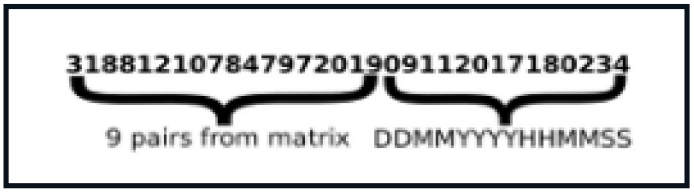


Figure 4: 128bit key generated from above sub-matrix

IV. EXPERIMENT RESULT

Our experimental setup was conducted in a **cloud-based environment**, simulating a real-time WBAN healthcare scenario. The main objective was to test **authentication, encryption, decryption, and end-to-end secure data transmission** using **biological keys** derived from **palm and thumb images** of patients. The experiment considered multiple critical performance parameters, as described below:

a) Setup and Tools Used

Cloud Infrastructure: Data storage and retrieval were performed on a remote cloud server for simulating real healthcare systems.

Key Generation: Biological key was generated from palm/thumb image matrices using MATLAB.

Encryption Standard: Advanced Encryption Standard (AES) with **128, 192, and 256-bit block sizes** was implemented.

Simulation Runs: 10 transmissions were performed at intervals of 1 minute. The **average of 5 independent runs** was considered for results.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

b) Parameters Measured

Doctor's Palm/Thumb Validation Time (DPVT/DTVT):
Time to match doctor's biometric with stored data for authentication.
Range: 1.23–1.67 ms (slightly variable across runs).

Data Read Time (DRT):
Time to collect physiological signals from the patient's body via sink nodes.
Range: 0.17–0.32 ms for palm; 0.19–0.31 ms for thumb.

Key Generation Time (KGT):
Time to generate biological key from patient's image matrix.
Palm: 2.35–2.99 ms
Thumb: 1.37–3.01 ms (faster due to smaller image size).

Encryption Time (ET):
Time to encrypt health data using AES with different key sizes.
128-bit key: 4.28–5.27 ms
192-bit key: 5.33–6.87 ms
256-bit key: 6.38–7.81 ms

Data Save & Retrieve Time (DST & DRT):
Time to store and fetch encrypted data from the cloud server.
Save: 0.66–1.66 ms
Retrieve: 0.13–0.29 ms

Decryption Time (DT):
Time to validate key and convert cipher text back to plain text.
Range: 4.66–6.89 ms depending on key size.

c) Overall End-to-End Delay

Palm Image:
128-bit: ~15.34 ms
192-bit: ~18.25 ms
256-bit: ~20.22 ms

Thumb Image:
128-bit: ~14.39 ms
192-bit: ~17.28 ms
256-bit: ~19.22 ms

All results are **well below the permissible healthcare delay of 250 ms** [Ref: IEEE Standard for WBAN latency requirements]. This confirms that the proposed method ensures **real-time secure transmission**.

d) Observations

Palm image keys provide higher security due to larger feature space but result in slightly higher delay.
Thumb image keys are faster but slightly less robust in terms of uniqueness.
AES **encryption time increases** with key size (as expected), but the delay remains negligible for healthcare applications.
The method shows **consistent performance across multiple runs**, proving its reliability.

Parameter	Palm Image (ms)	Thumb Image (ms)	Notes
Doctor's Validation Time (DPVT/DTVT)	1.23 – 1.67	1.23 – 1.67	Authentication of doctor's palm/thumb
Data Read Time (DRT)	0.17 – 0.32	0.19 – 0.31	Reading patient signals via sink nodes

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

Key Generation Time (KGT)	2.35 – 2.99	1.37 – 3.01	Palm slower (larger image matrix)
Encryption Time (ET, AES)	128-bit: 4.28 – 5.27192-bit: 5.33 – 6.87256-bit: 6.38 – 7.81	128-bit: 4.28 – 5.27192-bit: 5.33 – 6.87256-bit: 6.38 – 7.81	Higher key size → longer encryption time
Data Save Time (DST)	0.66 – 1.66	0.66 – 1.66	Storing encrypted data in cloud
Data Retrieve Time (DRT)	0.13 – 0.29	0.13 – 0.29	Fetching encrypted data from cloud
Decryption Time (DT)	4.66 – 6.89	4.66 – 6.89	Increases with AES key size

Table 2: Performance Parameters (Palm & Thumb Image Keys)

This document section, "EXPERIMENTAL RESULTS," describes a proposed data security system using Advanced Encryption Standard (AES) with biological keys:

System Overview: It utilizes human palm and thumb scan images for both authentication (doctor's images) and key generation (patient's images), which are then used in AES encryption.

Implementation: The experiment was conducted in a cloud-based environment, and palm/thumb images were converted to matrices using MATLAB.

Encryption Details: AES was employed for data encryption using 128, 192, and 256-bit blocks.

Results & Data: Simulation involved 10 transmissions at 1-minute intervals, with average results from 5 runs considered. The average file size for palm images was 8.04 kb, and for thumb images, it was 5.13 kb.

This document describes a secure data transmission system using palm image biometrics and AES encryption, focusing on end-to-end delay and its components.

Key Parameters: Explanations are provided for various time-related parameters, including Doctor's Palm/Thumb Validation Time (DPVT/DTVT), Data Read Time (DRT), Encryption Time (ET), Data Save Time (DST), Key Generation Time (KGT), Data Retrieve Time (DRT), and Decryption Time (DT).

End-to-End Delay Analysis: The document details the end-to-end delay for secure patient health data transmission using biological keys generated from palm image matrices and AES encryption with varying key sizes (128, 192, and 256 bits).

Performance Results: Specific time ranges are given for various operations, such as data read time (0.17-0.32msec), doctor palm validation time (1.24-1.67msec), and encryption time (4.28-5.27msec).

Key Size (AES)	Palm Image (ms)	Thumb Image (ms)	Observation
128-bit	15.34	14.39	Fastest, lowest delay, suitable for real-time monitoring
192-bit	18.25	17.28	Balanced between speed and security
256-bit	20.22	19.22	Highest security, slight increase in delay

Table 3: End-to-End Delay for Secure Transmission

Average Total Time: The average total time required for palm transmission using 128, 192, and 256-bit keys is reported as 15.34msec, 18.25msec, and 20.22msec, respectively.

This document analyzes the end-to-end delay in secure health data transmission using biological keys derived from palm and thumb images, with varying key sizes (128, 192, and 256 bits).

Palm Image Key Generation: Table II and Figure 7 detail the end-to-end delay and its components when using keys generated from palm images.

Thumb Image Key Generation: Table III and Figure 8 present similar data for keys generated from thumb images, showing a slight increase in encryption and decryption time with larger key sizes.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

Performance Comparison: The average end-to-end delay for secure data transmission using 128, 192, and 256-bit keys from thumb images is 14.39ms, 17.28ms, and 19.22ms, respectively.

Graphical Representation: Figures 7 and 8 visually represent the end-to-end delay and its individual components for different key sizes and biological key sources.

This document discusses a new proposal for biometric-based data authentication in Wireless Body Area Networks (WBANs) using a cloud-based server and AES encryption.

Biometric Authentication: The system uses biological keys derived from palm and thumb images for encryption and decryption.

Performance: End-to-end delays for secure transmissions using 128, 192, and 256-bit keys are presented, all falling well within the permissible delay for healthcare applications (250msec).

Security & Time: While palm image-based encryption takes slightly longer than thumb image-based encryption, it offers better security due to the larger palm matrix, which increases the possibility of unique key generation.

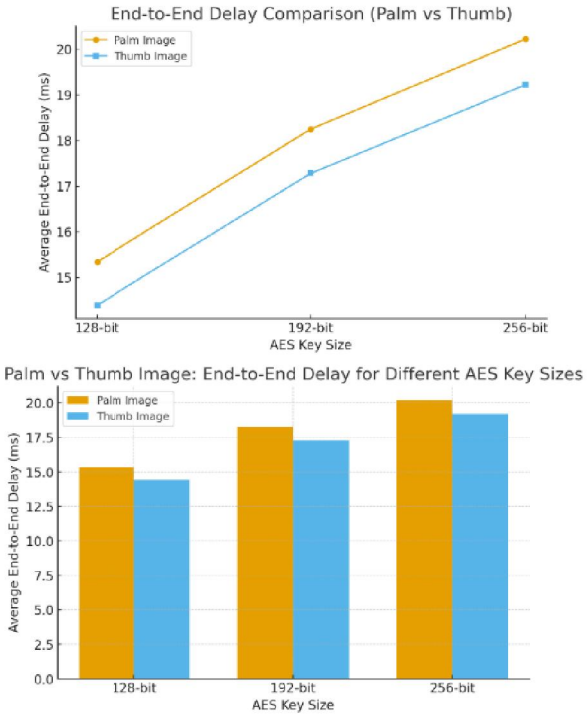


Figure5: Experiment result

V. CONCLUSION

This paper's conclusion focuses on a security analysis in WBAN and a new biometric-based data authentication proposal:

The work was simulated on a cloud-based server using AES security with 128, 192, and 256-bit block encryption.

Experimental results show that encryption/decryption using palm-derived biological keys takes longer than using thumb-derived keys.

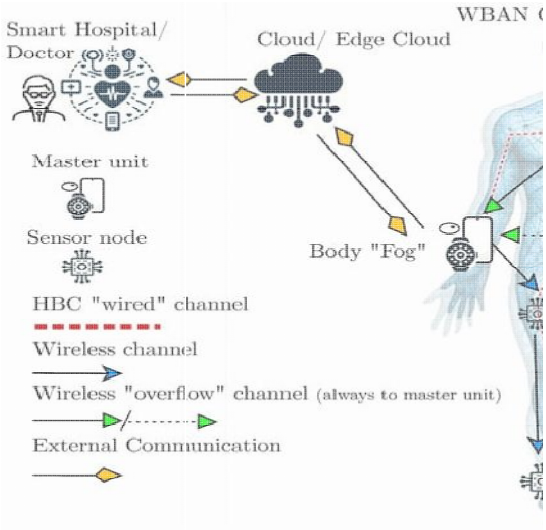
However, palm-based authentication offers better security due to the larger palm matrix, increasing the possibility of unique key generation.

This text proposes using palm images for enhanced security and privacy within Wireless Body Area Networks (WBANs), specifically for protecting patient physiological data.

Palm images are presented as a reliable biological feature.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

They are advocated for authentication and confidentiality.
The goal is to ensure the security and privacy of vital physiological parameters.
The application is within the context of Wireless Body Area Networks (WBANs).



REFERENCES

[1]. K. Dubey, C. Hota. Anomaly detection in WBANs using CNN-autoencoders and LSTMs, International conference on advanced information networking and applications, Springer Nature Switzerland, Cham (2024), pp. 187-197

[2]. S. Muneer, U. Farooq, A. Athar, M. Ahsan Raza, T.M. Ghazal, S. Sakib. A critical review of artificial intelligence based approaches in intrusion detection: A comprehensive analysis, J Eng, 2024 (1) (2024), Article 3909173

[3]. P. Gastaldo, E. Ragusa, S. Dosen, F. Palmieri. Special issue on integration of machine learning and edge computing for next generation of smart wearable systemsFuture Gener Comput Syst (2024), Article 107574

[4]. K. Ayub, R. Alshawa. A novel AI framework for WBAN event correlation in healthcare: ServiceNow aiops approach2024 IEEE workshop on microwave theory and technology in wireless communications, IEEE (2024), pp. 55-60

[5]. S. Kumaran, I.R.E. Princy, J.P. Agnes. Smart healthcare: Machine learning enabled WBAN for early detection of chronic diseases2024 2nd international conference on sustainable computing and smart systems, IEEE (2024), pp. 998-1003

[6]. Aryan Rana, *et al.*Architectures, benefits, security and privacy issues of internet of nano things: A comprehensive survey, opportunities and research challenges. IEEE Commun Surv& Tutorials (2024)

[7]. Audace Manirabona, Lamia Chaari Fourati. A 4-tiers architecture for mobile WBAN based health remote monitoring system. WirelNetw, 24 (2018), pp. 2179-2190

[8]. M. BlessingChallenges and solutions in implementing secure communication in WBANs(2024)

[9]. B. Khalil, N. Naja. A framework for security analytics of WBAN/WLAN healthcare network2018 IEEE international conference on technology management, operations and decisions, IEEE (2018), pp. 314-319

[10]. P. Anitha, R. Priya. A novel wireless Secure Body Area network layer protocol for secured patient data transmission2024 5th international conference on electronics and sustainable communication systems, IEEE (2024), pp. 557-564

[11]. Sohail Saif, *et al.*MLIDS: Machine learning enabled intrusion detection system for health monitoring framework using BA-WSNInt J Wirel Inf Netw, 29 (4) (2022), pp. 491-502

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, September 2025
Impact Factor: 7.67

[12]. Alexander Verner, Dany Butvinik. A machine learning approach to detecting sensor data modification intrusions in WBANs2017 16th IEEE international conference on machine learning and applications, IEEE (2017)

[13]. Lorenzo Mucchi, *et al.*An overview of security threats, solutions and challenges in wbans for healthcare2019 13th international symposium on medical information and communication technology, IEEE (2019)

[14]. Muhammad Shadi Hajar, Harsha Kumara Kalutarage, M. Omar Al-Kadri3R: A reliable multi agent reinforcement learning based routing protocol for wireless medical sensor networksComputNetw, 237 (2023), Article 110073

[15]. Dur-e-Shawar Agha, *et al.*A secure crypto base authentication and communication suite in wireless body area network for IoT applications. Wirel PersCommun, 103 (4) (2018), pp. 2877-2890

[16]. Peyman Dodangeh, Amir Hossein Jahangir. A biometric security scheme for wireless body area networksJ Inf Secur Appl, 41 (2018), pp. 62-74

[17]. Garg A, Kumar A, Singh AK. Machine Learning-Based Security Approaches for Wireless Body Area Networks. In: Security, privacy, and trust in WBANs and e-healthcare. CRC Press; p. 206–35.