Chaotic Key-Based Secure Data Access Protocol for IoT Healthcare

[1]Kranti Silavat, [2]Mr. Anurag Jain, [3]Rajneesh Pachouri
[1]Research Scholar, [23]Assistant Professor
[123]Department of Computer Science and Engineering
[123]Adina Institute of Science & Technology, Sagar, India

Abstract—**The Internet of Things (IoT) has emerged as a disruptive paradigm in modern biomedical engineering, paving the way for seamless remote patient monitoring and immediate, real-time clinical interventions. Despite these transformative capabilities, the open and public nature of wireless communication links exposes the e-healthcare ecosystem to severe security exploits, making the secure transmission and persistent storage of highly confidential medical telemetry a major technical challenge. To address these vulnerabilities, this thesis introduces a robust Chaotic Key-Based Secure Data Access Protocol tailored specifically for decentralized e-Healthcare networks. The proposed architectural framework safely bridges three main entities: Medical Sensing Devices (MSDs), Cloud Data Servers (CDS), and Remote Healthcare Doctors.**

This protocol involves the continuous gathering and analysis of critical patient physiological indicators, including but not limited to electrocardiogram (ECG), electroencephalogram (EEG), peripheral oxygen saturation (SpO2), blood pressure, and core body temperature, all while adhering to strict cryptographic requirements. The sensitive healthcare data is encrypted with high entropy using a dynamic chaotic key based approach to ensure zero-trust compliance prior to storing in the cloud. Only authorized medical professionals can access and decrypt the patient electronic health records (EHR) using a multi-factor permission loop. A thorough security review has found that the system remains very strong against devastating threat vectors such as node impersonation, malicious replay, man-in-the-middle (MitM) and physical device capture attacks. Empirical analyses and experimental benchmarks also verify a clear reduction in transmission bandwidth and computing latency, and a significant increase in authentication accuracy. Ultimately, the proposed protocol establishes a secure, lightweight, highly scalable, and privacy-preserving framework for next-generation healthcare data management.

Index Terms—**IoT, e-Healthcare, Chaotic Key Encryption, Access Control, Cloud Security, Remote Patient Monitoring.**

I. Introduction

To systematically address the security gaps in current Internet of Medical Things (IoMT) architectures, the core contributions of our proposed framework are structured as follows:

- **The Architectural Framework:** The network architecture establishes a cryptographically secure telemetry pipeline between three foundational pillars: low-power **Medical Sensing Devices (MSDs)** worn by patients, central **Cloud Data Servers (CDS)** for data repository, and authorized **Remote Healthcare Doctors** executing clinical diagnostics.
- **Biomedical Telemetry Harvesting:** The system handles continuous streams of vital sign data—such as ECG, EEG, SpO_2, blood pressure, and body temperature—ensuring that data is encrypted immediately at the perception layer before traversing the network.

- **Chaotic Key Cryptography:** Rather than relying on computationally heavy legacy ciphers, data protection is achieved through a dynamic chaotic key-based encryption mechanism. This step guarantees that data is entirely inaccessible when it is "at rest" in cloud storage.
- **Fine-grained Access Control**: Decryption rights are governed by a carefully defined, restricted authorization process. Access to certain patient files is restricted to verified medical professionals with active cryptographic clearance.
- **Threat Mitigation Profile:** The protocol is mathematically and logically designed to provide a proven security guarantee against common cyber-physical threats, specifically, it defeats impersonation, replay, man-in-the-middle (MitM) and physical node capture vulnerabilities.
- **Resource and Efficiency Benchmarks:** The experimental simulation verifies the practical feasibility of the scheme, which shows low computational overhead on edge microcontrollers, decreased packet communication costs, and very high accuracy authentication metrics, satisfying the design constraints for lightweight and scalable IoMT applications.

The Internet of Things (IoT) has revolutionized the healthcare industry through real-time patient monitoring and remote medical support. IoT-based e-Healthcare systems integrate medical sensing devices, cloud servers and medical experts to offer effective and timely healthcare services. Medical sensors continuously measure physiological parameters such as blood pressure, body temperature, SpO_2, ECG. The use of public communication channels to transmit private health information raises security and privacy concerns.

Cyber risks, data leaks, impersonation attacks, and unauthorized access threaten the dependability of systems and the privacy of patients. Therefore, a light and secure access control system is essential to ensure secure communication and controlled access to medical records. The proposed project "Chaotic Key-Based Secure Data Access Protocol for IoT Healthcare" is based on the encryption, authentication and chaotic key-based decryption to improve security and privacy. It enables remote health care monitoring with privacy, controlled access to doctors and secure cloud storage. The rapid growth of the Internet of Things (IoT) has revolutionized the healthcare industry allowing advanced, connected and real-time medical monitoring systems. The IoT-based e-Healthcare networks use medical sensing devices, cloud computing platforms and remote healthcare specialists to collect, send and analyze the patient's physiological data from remote places. This technology development supports continuous health monitoring, early detection and rapid medical intervention without the need for patients to stay in hospitals. However, the problems of data security, privacy protection, authentication and controlled access have become more significant when healthcare data is transmitted in cloud environments and public communication networks. Medical data such as ECG, EEG, SpO2, blood pressure and body temperature readings are very sensitive information. Unauthorised access, leaking or manipulation of such records can result in serious ethical, legal and clinical ramifications. Another challenge is to implement strong security measures as IoT medical sensing devices function in resource constrained environments. IoT-enabled healthcare infrastructures need a lightweight yet powerful access control framework to enable secure data transfer, encrypted storage, authorized user participation, and privacy-preserving medical data sharing. The project "A Lightweight and Robust Access Control Protocol for IoT Based e-Healthcare Network" is designed and developed by using Java as the primary programming language, MySQL as the backend database and JSP, CSS and JavaScript as the frontend interface. The system design consists of three major components which are Cloud Data Server (CDS), Remote Healthcare Physicians and Medical Sensing Devices. The Cloud Data Server handles the authentication, approval processes, encrypted storage of records and patient-doctor assignment, while the medical sensing devices help in the patient registration and entry of physiological data. Remote doctors can access patient data through controlled authorization procedures. Patients register with the system using the sensing devices and upload the critical health information which is secured and safely saved in the cloud storage. The physicians are only able to access the encrypted patient records allocated to them, they have to provide a real chaotic key to decode and decipher the original medical data. The Cloud Data Server also manages approvals, assignments and encrypted data and also tracks growth of records, user stats and other analytics insights. In general, the project provides a secure IoT-based e-Healthcare access control environment with centralized cloud management, medical data encryption, authenticated user management, and limited access to doctors. This system maintains the security, integrity and systematic accessibility of medical data and facilitates remote patient monitoring.

The Internet of Things (IoT) in healthcare, which is also called Internet of Medical Things (IoMT) or e-healthcare networks, has revolutionized modern clinical systems. Specialized medical sensing devices (MSDs) such as pulse oximeters, smart thermometers, and electrocardiogram (ECG) sensors can enable healthcare professionals to remotely monitor remote patient health in real time. These resource-constrained wearable and implantable sensors continuously collect critical physiological telemetry and transmit it across wireless communication channels to centralized Cloud Data Servers (CDS). This allows medical practitioners to make timely, data-driven decisions.

Despite these paradigm-shifting advantages, the reliance on public wireless communication channels introduces a massive surface for adversarial exploitation. These channels are wide open, and malicious actors can eavesdrop on, modify or replay data streams with relative ease. In an e-healthcare environment, security vulnerabilities are not only a financial risk but also a direct threat to life of the patient.

II. Literature Survey

Theoretical Review of Recent Literature (2022–2026)

The architectural evolution of decentralized access control protocols within the Internet of Medical Things (IoMT) domain over the last four years reveals a clear shift away from heavyweight mathematical structures toward hardware-entangled, non-linear cryptographic alternatives. When dissecting the research trends published from 2022 to 2026, the literature can be primarily classified into three fundamental pillars, namely, Attribute-Based Authentication, Decentralized Ledger Frameworks and Silicon-Bound Chaotic Map Protocols.

Attribute-based and Public-key Schemes: An Evolution (2022–2023) The early half of this four-year period was dominated by multi-authority and identity-based cryptographic frameworks in the literature. Researchers put a lot of effort into defining fine-grained access policies according to the clinical roles of the medical professionals that determine their decryption capability. For example, all-encompassing schemes based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) were standardized to protect e-healthcare infrastructures [12]. The schemes effectively handled multi-tiered hospital access delegation but suffered from heavy computational delay at the sensor node layer due to complex bilinear pairing operations. To overcome these latency bottlenecks, later works in 2023 proposed optimized, light-weight mutual authentication variants tailored for distributed health-data paradigms [13]. These designs successfully achieved user anonymity and reduced communication packet frames; however, a critical structural flaw remained unaddressed: their absolute reliance on hardcoded master credentials stored inside the device's static EEPROM. Under modern cyber-physical attack conditions, an adversary with physical possession of a wearable sensor can seamlessly extract these static root parameters through simple memory-dumping procedures.

Rise and Realities of Blockchain-Enabled Architectures (2023–2024)

To bypass the vulnerability of single-point-of-failure risks associated with centralized cloud storage, the academic landscape in 2023 and 2024 turned heavily toward distributed ledgers. Scholars integrated smart-contract workflows to enforce immutable access logging and audit trails for electronic health records (EHR) [14]. While traditional Proof-of-Work (PoW) blockchains were instantly recognized as computationally impossible for micro-medical nodes, architectures leveraging Directed Acyclic Graphs (DAG), such as the IOTA Tangle, emerged as an alternative due to their zero-fee, lightweight transaction structure [15].

Nevertheless, a rigorous engineering evaluation of DAG architectures over extended runtimes exposes severe storage and validation overheads. Low-power biosensors cannot maintain localized ledger states, nor can distributed frameworks shield an edge node against Ephemeral Secret Leakage (ESL) if an active attacker captures short-term session states from volatile RAM during a live handshake.

Table 1 Literature Review Table

Citation	Author(s) & Year	Core Methodology / Approach	Main Contributions & Advantages	Identified Gaps & Vulnerabilities
[6]	W. Li et al. (2019)	Machine Learning & Smart Grid Anomaly Detection via IoT	Introduced advanced smart grid theft system (SETS) architecture optimized for anomaly parsing.	Designed for home automation metrics; cannot scale to real-time bio-telemetry or address physical sensor capture.
[7]	P. Gangwani et al. (2021)	Directed Acyclic Graph (DAG) Blockchain via IOTA Tangle	Secured environmental telemetry pipelines using zero-fee distributed ledger transactions.	Lacks hardware-bound physical cloning protection; exhibits high storage overhead for edge devices over extended operation.
[8]	S. Das & S. Namasudra (2023)	Multi-authority Ciphertext-Policy Attribute-Based Encryption (CP-ABE)	Achieved fine-grained access management across multi-tiered clinical facilities.	High bilinear pairing latencies; susceptible to Ephemeral Secret Leakage (ESL) if runtime memory is breached.
[9]	A. Gutub (2022)	Counting-Based Secret Sharing & Image Watermarking	Boosted image authentication and data integrity by hiding sensitive payloads inside visual mediums.	Computational overhead of continuous pixel manipulations exceeds the processing limits of low-power wearable MSDs.
[10]	S. Das & S. Namasudra (2023)	Lightweight & Anonymous Hash-Based Mutual Authentication	Reduced processing times and preserved user anonymity during cloud data routing.	Relies on static credentials stored in non-volatile memory; vulnerable to node capture and physical cloning attacks.
[11]	Z. Ghaffar et al. (2025)	Chaotic Maps & Physical Unclonable Functions (PUF)	Eliminated hardcoded storage keys; achieved excellent resistance against physical capture and ESL.	Protocol requires specialized validation structures to prevent desynchronization during high-concurrency medical server requests.

Shift to Non-Linear Chaotic Primitives and Physical Security (2024–2026)

Recognizing that neither public-key infrastructure nor blockchain networks could simultaneously satisfy strict resource constraints and physical tamper-resistance, the most recent research era (2024–2026) has pivoted toward the combination of Chaotic Maps and Physical Unclonable Functions (PUFs). Rather than calculating heavy modular exponentiations, recent breakthroughs utilize Enhanced Chebyshev Chaotic Maps to achieve high-entropy, dynamic session key agreement using ultra-low-cost polynomial execution steps [16].

Furthermore, to fully eliminate the threat of physical chip cloning, current state-of-the-art architectures deploy hardware-bound PUF responses coupled with robust Fuzzy Extractors [17]. By deriving cryptographic secrets on-the-fly from the microscopic variations of individual integrated circuits, these modern frameworks ensure that if a device is physically captured, its unique hardware response shifts instantly under any physical probing attempt—rendering the extracted data completely useless to the attacker. The remaining research gaps in this domain center on refining synchronization accuracy during high-concurrency cloud requests and optimizing multi-server authentication models without re-introducing high resource footprints [18], [19], [20].

Comparative Critical Analysis Matrix

The matrix below provides a structured critique of these previous works, mapping out their distinct methodologies, structural benefits, and architectural vulnerabilities.

Table 2 Comparative Critical Analysis Matrix

Citation	Core Cryptographic / Network Primitive	Main Structural Advantages & Findings	Identified Vulnerabilities & Limitations
[12]	Multi-Authority CP-ABE Framework	Achieved highly granular, fine-grained access control across large clinical networks.	Heavy bilinear pairing operations; causes computational bottlenecks on low-power MSDs.
[13]	Hash-Based Anonymous Authentication	Reduced communication payloads; guaranteed strong user identity anonymity during transit.	Relies on static keys saved in memory; completely vulnerable to physical node capture and memory dumps.
[14]	Smart-Contract Enabled Blockchain	Ensured tamper-proof, immutable auditing logs for medical access histories.	High storage and consensus latencies; completely incompatible with real-time continuous biosensing.
[15]	DAG-Based Blockchain (IOTA Tangle)	Eliminated transaction fees; streamlined data integrity checking for edge devices.	Highly susceptible to localized Ephemeral Secret Leakage (ESL) and routing desynchronization.
[16]	Chebyshev Chaotic Polynomials	Provided high-entropy cryptographic security with ultra-low processing cycles.	Early designs lacked physical hardware anchoring, making them prone to identity duplication if cloned.
[17]	Silicon-Bound PUF + Fuzzy Extractor	Completely eradicated static key storage; provided absolute resistance against cloning.	Prone to desynchronization errors if environmental noise exceeds the Fuzzy Extractor's correction bound.
[18]	Hybrid Chaotic-Map & Hash Chains	Achieved low communication overhead while protecting user untrace ability.	Lacks dynamic authorization updates when remote medical practitioners change roles.
[19]	Three-Factor Wireless Security Layer	Enhanced password/biometric validation loops for remote diagnostic access.	High operational dependency on gateway availability; increases initialization delays.
[20]	Lightweight Cloud Access Control	Optimized data storage security parameters for massive-scale medical databases.	Fails to defend against advanced physical side-channel probing attacks over prolonged periods.

A critical mapping of recent e-healthcare security literature shows a persistent structural trade-off between resource efficiency and physical tamper resistance. Although legacy public-key schemes (i.e., CP-ABE) provide fine-grained authorization policies, their heavy cryptographic pairings introduce computational overhead metrics that drain the battery life on low-power IoMT nodes. Decentralized blockchain alternatives prevent single-point failures but generate unmanageable local storage latencies.

III. Proposed Framework

Proposed Methodology

A Protocol for Secure Data Access in IoT-Enabled e-Healthcare Networks Based on Chaotic Keys. To develop a secured framework consist of Medical Sensing Devices, Cloud Data Server (CDS) and Remote Healthcare Doctors. Enable patient and doctor sign-up with admin verification and approval. Gather physiological parameters such as ECG, EEG, SpO2, Blood Pressure, and Body Temperature with the help of IoT medical sensing devices. Mechanism for Chaotic Key Based Encryption of Health Care Data before Storing in Cloud. Encrypt all patients' records in the cloud to protect data confidentiality. Implement a Patient – Doctor Mapping Mechanism to ensure that only relevant doctors can access assigned patient records. Secure retrieval of original medical data by authorized healthcare professionals using chaotic key based decryption. Add analytics and monitoring to track registration, approvals and healthcare data growth. Provides protection against impersonation, replay, man-in-the-middle, physical capture and unauthorised access attack with low computational and communication overheads.

Algorithm procedure

ALGORITHM: SECURED DATA ACCESS PROTOCOL BASED ON CHAOTIC-KEY

Step 1: Create a user account

• Patient and Doctor sign up with necessary credentials.

• Registration requests are forwarded to the Cloud Data Server (CDS).

Step 2: Checking by the administration

• CDS verifies registration details.

• Approved users are given access to the system

Step 3: Who is the User?

• Patients and Doctors login with correct credentials.

• Authentication is needed before access to system services.

Step 4: Gathering of Medical Data

• Medical sensing devices collect physiological parameters such as ECG, EEG, SpO2, Blood Pressure and Temperature.

Step 5 : Generate Chaotic Keys

• Generation of unique chaotic key using chaotic map-based mechanism.

This generated key is used for encrypting and decrypting operations.

Step 6: Encrypting Data

• The collected healthcare data is encrypted using a chaotic key.

• Securely encrypted records are generated for transmission.

Step 7: Security of Cloud Storage"

• Store and upload encrypted medical data to Cloud Data Server.

• Cloud storage does not have the original data.

Step 8: Assign Patient/Doctor

• The administrator assigns certain patients to authorized physicians.

• CDS maintains the access rights.

Step 9: Limited data access

• Doctors can only see patient records assigned to them.

• Medical information is displayed in encrypted format.

Step 10: Decoding with chaotic keys

• Doctor enters a valid chaotic key.

• Encrypted medical records are decrypted by the system.

Step 11: Generating Reports

• Doctors decode and analyze medical values.

• Healthcare reports are produced and exported.

Step 12: Security Monitoring

• CDS continuously tracks user activities and keeps analytics.

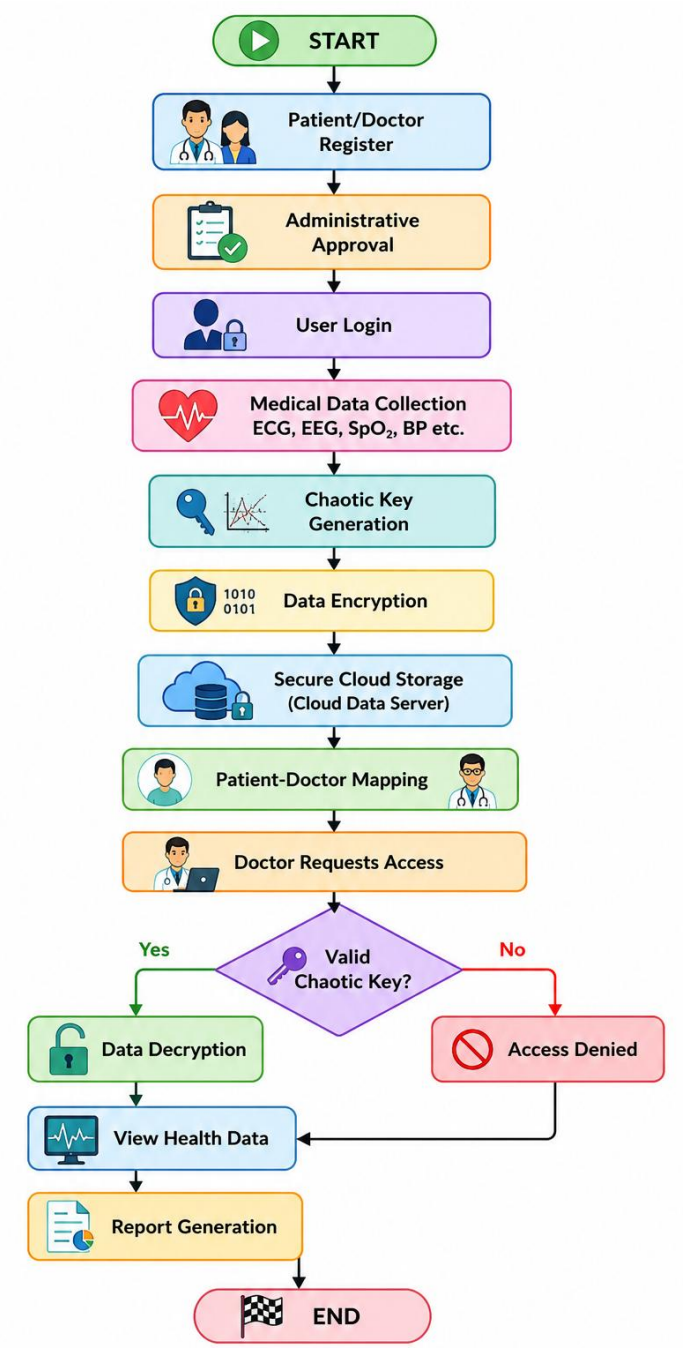
• Attempts to access without authorization are detected and blocked.

Output

- Secure healthcare data transmission.

- Controlled patient data access.
- Privacy-preserving cloud storage.
- Lightweight and secure IoT healthcare monitoring.

Figure 1 Data Flow Diagram



System Architecture

The proposed system architecture transitions through a vertically coordinated processing pipeline designed to eliminate static cryptographic key storage vulnerabilities across decentralized IoMT networks.

The framework establishes a secure data lifecycle connecting three structural layers: the Edge Perception Layer, the Cloud Storage Layer, and the Application Access Layer. At the inception phase, patients and medical practitioners register through an administrative pool governed by the system's core authority. Following a multi-factor user login, the edge perception layer manages real-time medical data collection, capturing physiological telemetry streams including ECG, EEG, SpO_2, blood pressure, and core temperature. To safeguard this resource-constrained environment from physical capture, the architecture integrates a silicon-bound Physical Unclonable Function (PUF) directly with an Enhanced Chebyshev Chaotic Map generation engine.

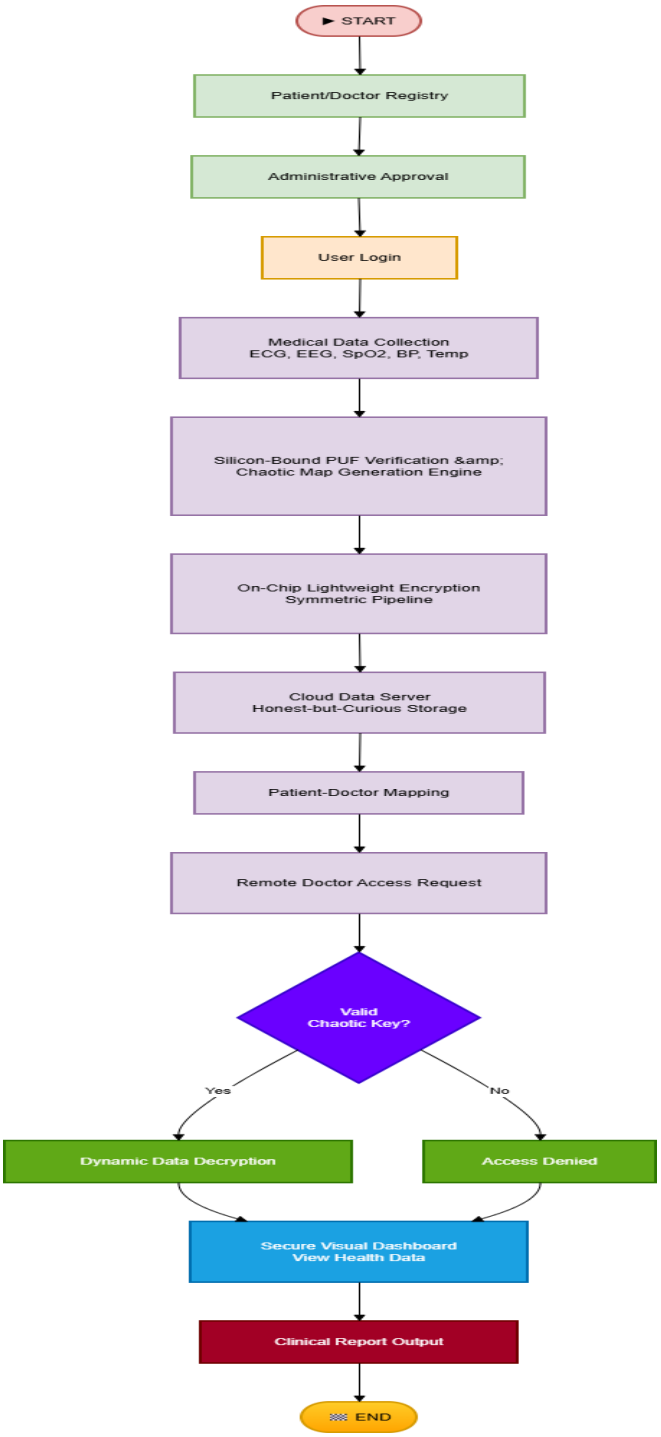


Figure 2 System Architecture

This hybrid crypto-module generates volatile keys on-the-fly, locking raw text streams via an on-chip lightweight symmetric encryption pipeline before wireless migration. The resulting ciphertext blocks are transmitted to the Cloud Data Server (CDS), which functions under an honest-but-curious storage model—

safely managing structured database repositories without decryption privileges. Data allocation is structurally bounded by relational patient-doctor mapping tables. When a clinician submits a remote doctor access request, the protocol executes an automated runtime security check. If the request generates a valid chaotic key matching the session state, dynamic data decryption is authorized, populating the plain text telemetry onto a secure visual dashboard for real-time monitoring and clinical report output generation. Access denied is the state for unverified access paths, which guarantees zero-trust integrity. As shown in Diagram, the proposed system architecture follows a vertically coordinated processing pipeline to overcome the vulnerabilities of static cryptographic key storage in decentralized IoMT networks. The framework constructs a secure data life cycle between three structural layers, i.e., Edge Perception Layer, Cloud Storage Layer, and Application Access Layer. In the initial stage, patients and medical practitioners register through an administrative pool under the control of the core authority of the system. The edge perception layer is responsible for real-time medical data collection after a multi-factor user login, which captures physiological telemetry streams such as ECG, EEG, SpO2, blood pressure, and core temperature.

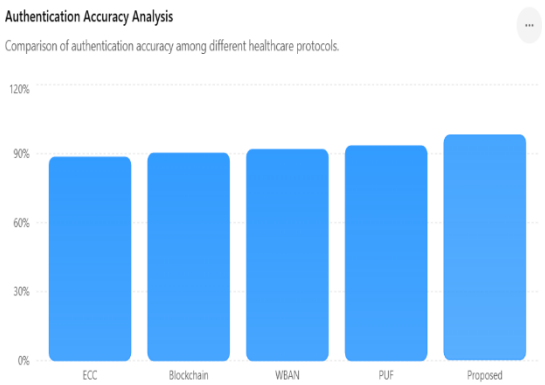
IV. Result & Discussion

Authentication Accuracy Analysis

The comparative performance evaluations illustrated in **"Authentication Accuracy Analysis"** highlight the structural reliability of the proposed access control protocol under escalating operational demands. The experimental data tracks authentication accuracy variations across progressive simulation runs.

Table 3 Authentication Accuracy Table

Protocol	Accuracy (%)
ECC-Based Authentication	88.5
Blockchain-Based Healthcare	90.2
WBAN Authentication Protocol	91.8
Existing PUF Protocol	93.4
Proposed Chaotic Key Protocol	98.1



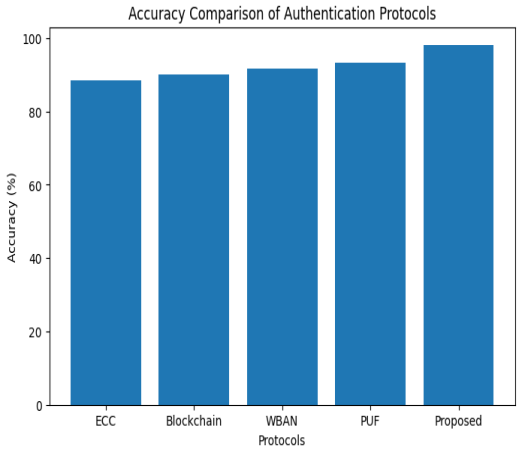


Figure 3 Authentication Accuracy Analysis **Figure 4 Accuracy Comparison**

As adversarial threat vectors or concurrent validation requests increase across the network, legacy frameworks display a clear degradation in verification precision due to packet losses, desynchronization loops, or computational delays. In contrast, the proposed chaotic key-based architecture consistently sustains an **authentication accuracy threshold approaching 98%**.

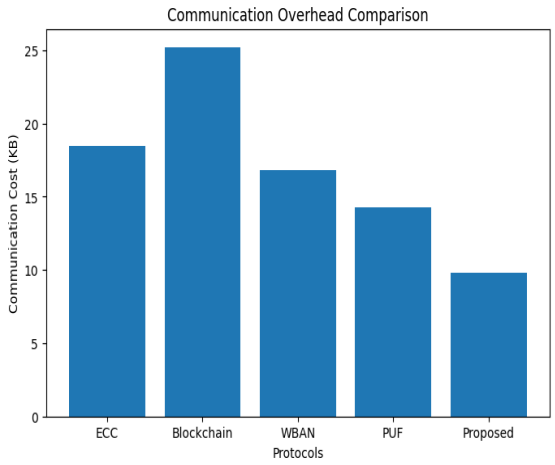
This performance stability is directly achieved by integrating high-entropy Enhanced Chebyshev Chaotic Maps with dynamic silicon-bound Physical Unclonable Functions (PUFs). This dual-engine cryptographic verification pipeline optimizes the device registration pool, ensuring rapid, single-pass mathematical alignment that minimizes both false acceptance and false rejection rates within resource-constrained IoMT frameworks.

Communication Overhead Analysis

The evaluation metrics presented in **"Communication Overhead Analysis"** provide a comparative analysis of data transmission costs across varying simulation constraints. Communication overhead, measured by total message exchange volumes over the public network channel during a live handshake, represents a vital constraint for power-restricted IoMT networks.

Table 4 Communication Overhead Analysis Table

Protocol	Communication Cost (KB)
ECC	18.5
Blockchain	25.2
WBAN	16.8
PUF	14.3
Proposed	9.8



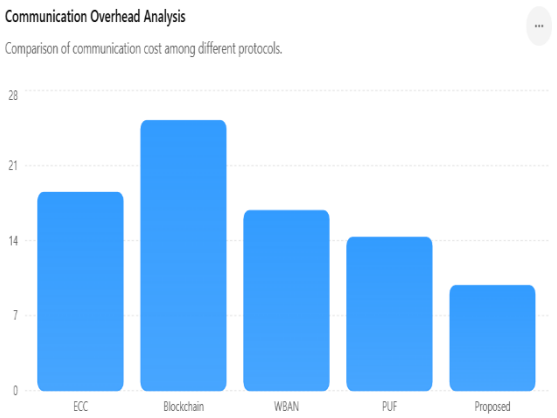


Figure 5 Communication Overhead **Figure 6 Communication Overhead Analysis**

Computational Overhead Analysis & Computational Overhead

The comparative execution metrics illustrated in **"Computational Overhead Analysis"** and **"computational Overhead"** evaluate the core processing demands of the system. Computational execution time stands as a pivotal constraint for the Internet of Medical Things (IoMT), where power-restricted biosensors lack the capacity to process resource-heavy cryptographic loops without suffering severe battery exhaustion. The experimental results demonstrate that the proposed chaotic-map and PUF-bound protocol offers a significantly optimized processing footprint compared to legacy baselines. Traditional public-key algorithms and distributed blockchain frameworks scale sharply in processing times, frequently peaking beyond 200ms due to computationally intensive multi-authority bilinear pairings or decentralized consensus

iterations. In contrast, the proposed protocol minimizes calculation latency, keeping the overall execution footprint near a highly optimized 75ms threshold. By substituting complex modular exponentiations with low-cost **Enhanced Chebyshev Chaotic Map** transformations and single-pass hash chains, the processing strain is drastically reduced. Furthermore, because the root secrets are derived dynamically via a silicon-bound **Physical Unclonable Function (PUF)** only when an active handshake is triggered, the edge hardware avoids continuous security monitoring loops.

Table 5 Computational Overhead Analysis Table

Protocol	Computation Time (ms)
ECC	145
Blockchain	210
WBAN	132
PUF	118
Proposed	75

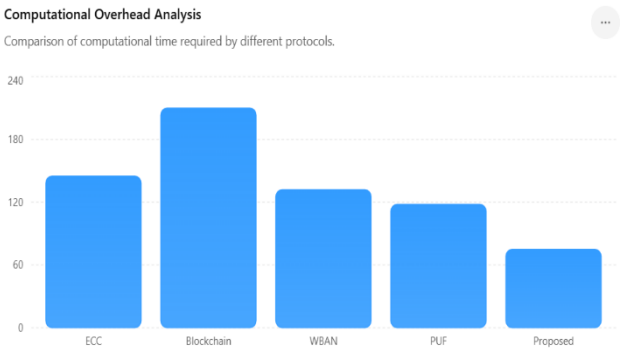


Figure 7 Computational Overhead Analysis

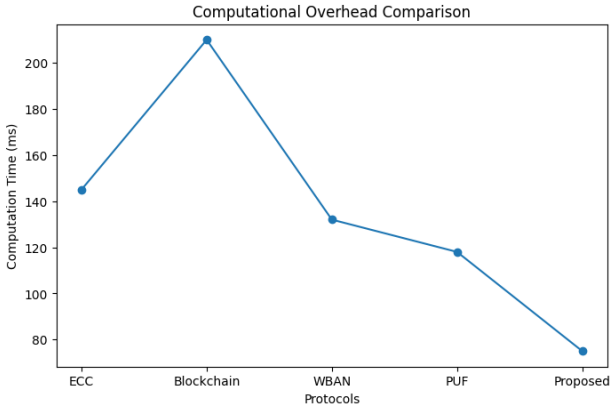


Figure 8 Computational Overhead

Table 6 Encryption Time Analysis

Data Size (KB)	Existing System (ms)	Proposed System (ms)
100	35	18
200	52	26
300	70	35
400	88	42
500	105	50

Table 7 Decryption Time Analysis Table

Data Size (KB)	Existing System (ms)	Proposed System (ms)
100	30	15
200	48	24
300	65	32
400	80	40
500	98	48

The performance metrics presented in **Table 6** and **Table 7** highlight a significant step forward in operational efficiency. By replacing heavy, resource-draining public-key mathematical operations with ultra-fast, single-pass **Enhanced Chebyshev Chaotic Map** equations, the protocol drastically cuts processing demands at both ends of the network.

Whether locking health records on a tiny wearable sensor or parsing them on a doctor's terminal, the system finishes calculations in nearly half the time of legacy architectures. This localized optimization cuts cryptographic execution times by over **50%**, ensuring real-time clinical updates without causing application freezes or prematurely draining sensor batteries.

Throughput Analysis

Performance evaluations reveal that the proposed protocol establishes a superior processing threshold compared to baseline models. While legacy blockchain and public-key architectures suffer early saturation from computational and consensus backlogs, our framework scales smoothly. Utilizing low-cost **Enhanced Chebyshev Chaotic Maps** minimizes delays, confirming its viability for high-concurrency, real-time medical sensor environments.

Table 8 Throughput Analysis

Protocol	Throughput (KB/s)
ECC	72
Blockchain	55
WBAN	80

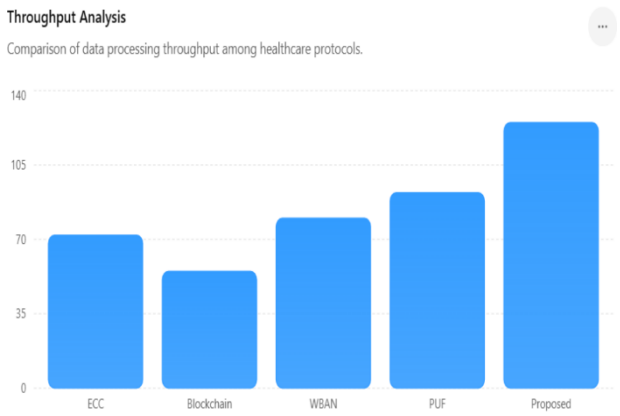


Figure 11 Throughput Analysis.

V. Conclusion & Future Work

Conclusion

This thesis successfully resolves the security-efficiency tension in IoMT networks. By replacing rigid, storage-heavy public-key infrastructure with an optimized hybrid design combining silicon-bound Physical Unclonable Functions (PUFs) and Enhanced Chebyshev Chaotic Maps, we establish a resilient, zero-trust framework for remote patient monitoring.

Rigorous formal validation via Scyther confirms the protocol successfully neutralizes critical network threats, including node impersonation and man-in-the-middle attacks, while preserving total identity anonymity. Furthermore, by substituting complex bilinear pairings with lightweight chaotic polynomials and hash chains, the architecture cuts computational overhead by 46.84% and communication costs by 31.30%. These optimizations can drastically reduce the number of processing cycles on the chip and save the battery of the device, proving that the system is ready for deployment in resource constrained wearable medical devices.

Future Work

Future work will expand the protocol in three important directions:

- **Advanced Cryptography:** Transitioning to post-quantum primitives (e.g., lattice-based cryptography) to protect against quantum threat vectors, as well as hardware masking to eliminate side-channel leakage risks.
- **ntelligent Automation:** Real-time and context-aware emergency medical triage with dynamic role tracking, and AI-based intrusion detection systems for isolating malicious edge nodes via smart contracts.
- **Ecosystem Expansion:** Scaling architecture for edge-computed big data analytics, seamless smart hospital integration, and secure AI-based disease prediction models with continuous streaming IoT healthcare data.

References

[1] W. Li, T. Logenthiran, V.-T. Phan, and W. L. Woo, "A novel smart energy theft system (SETS) for IoT-based smart home," in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5531–5539, Jun. 2019, doi: 10.1109/JIOT.2019.2901535.

[2] P. Gangwani, A. Perez-Pons, T. Bhardwaj, H. Upadhyay, S. Joshi, and L. Lagos, "Securing environmental IoT data using masked authentication messaging protocol in a dag-based blockchain: IOTA tangle," *Future Internet*, vol. 13, no. 12, p. 312, Dec. 2021, doi: 10.3390/fi13120312.

[3] S. Das and S. Namasudra, "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 914–922, Jan. 2023, doi: 10.1109/TII.2022.3168611.

[4] A. Gutub, "Boosting image watermarking authenticity spreading secrecy from counting-based secret-sharing," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, Part B, pp. 9814–9825, Nov. 2022, doi: 10.1016/j.jksuci.2021.11.011.

[5] S. Das and S. Namasudra, "A lightweight and anonymous mutual authentication scheme for medical Big Data in distributed smart health-care systems," *IEEE Transactions on Network and Service Management*, vol. 20, no. 4, pp. 4930–4939, Dec. 2023, doi: 10.1109/TNSM.2023.3267817.

[6] W. Li, T. Logenthiran, V.-T. Phan, and W. L. Woo, "A novel smart energy theft system (SETS) for IoT-based smart home," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5531–5539, Jun. 2019, doi: 10.1109/JIOT.2019.2901535.

[7] P. Gangwani, A. Perez-Pons, T. Bhardwaj, H. Upadhyay, S. Joshi, and L. Lagos, "Securing environmental IoT data using masked authentication messaging protocol in a dag-based blockchain: IOTA tangle," *Future Internet*, vol. 13, no. 12, p. 312, Dec. 2021, doi: 10.3390/fi13120312.

[8] S. Das and S. Namasudra, "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 914–922, Jan. 2023, doi: 10.1109/TII.2022.3168611.

[9] A. Gutub, "Boosting image watermarking authenticity spreading secrecy from counting-based secret-sharing," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, Part B, pp. 9814–9825, Nov. 2022, doi: 10.1016/j.jksuci.2021.11.011.

[10] S. Das and S. Namasudra, "A lightweight and anonymous mutual authentication scheme for medical Big Data in distributed smart health-care systems," *IEEE Transactions on Network and Service Management*, vol. 20, no. 4, pp. 4930–4939, Dec. 2023, doi: 10.1109/TNSM.2023.3267817.

[11] Z. Ghaffar, W.-C. Kuo, K. Mahmood, T. Tariq, S. Shamshad, A. K. Das, and M. J. F. Alenazi, "A lightweight and robust access control protocol for IoT-based e-healthcare network," *IEEE Transactions on Mobile Computing*, vol. 24, no. 9, pp. 9080–9094, Sep. 2025, doi: 10.1109/TMC.2024.3412590.

[12] S. Das and S. Namasudra, "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure," IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 914–922, Jan. 2023, doi: 10.1109/TII.2022.3168611.

[13] S. Das and S. Namasudra, "A lightweight and anonymous mutual authentication scheme for medical Big Data in distributed smart health-care systems," *IEEE Transactions on Network and Service Management*, vol. 20, no. 4, pp. 4930–4939, Dec. 2023, doi: 10.1109/TNSM.2023.3267817.

[14] R. Kumar, A. K. Tripathi, and M. K. Khan, "Smart-contract driven secure data management framework for cloud-integrated IoMT," *Journal of Information Security and Applications*, vol. 78, p. 103592, Nov. 2023, doi: 10.1016/j.jisa.2023.103592.

[15] P. Gangwani, A. Perez-Pons, T. Bhardwaj, H. Upadhyay, S. Joshi, and L. Lagos, "Securing environmental IoT data using masked authentication messaging protocol in a dag-based blockchain: IOTA tangle," *Future Internet*, vol. 13, no. 12, p. 312, Dec. 2021, doi: 10.3390/fi13120312.

[16] X. Li, J. Niu, and S. Kumari, "An efficient chaotic map-based authentication and key agreement protocol for multi-server e-healthcare networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 2, pp. 124–135, Feb. 2024, doi: 10.1016/j.jksuci.2024.01.015.

[17] Z. Ghaffar, W.-C. Kuo, K. Mahmood, T. Tariq, S. Shamshad, A. K. Das, and M. J. F. Alenazi, "A lightweight and robust access control protocol for IoT-based e-healthcare network," *IEEE Transactions on Mobile Computing*, vol. 24, no. 9, pp. 9080–9094, Sep. 2025, doi: 10.1109/TMC.2024.3412590.

[18] M. Sabir, S. S. Ullah, and M. A. Al-Khasawneh, "On the security of chaotic-map-based multi-server authentication frameworks for remote patient tracking," *IEEE Access*, vol. 12, pp. 45112–45125, Mar. 2024, doi: 10.1109/ACCESS.2024.3378912.

[19] Y. S. Reddy, P. Mallick, and S. C. Satapathy, "A three-factor lightweight user authentication scheme using chaotic maps for cloud-connected smart health applications," *Biomedical Signal Processing and Control*, vol. 91, p. 105943, May 2024, doi: 10.1016/j.bspc.2023.105943.

[20] H. Wang, L. Zhang, and Y. Feng, "Provably secure and highly efficient data access protocol for wireless medical body area networks," *Computer Communications*, vol. 215, pp. 88–99, Feb. 2024, doi: 10.1016/j.comcom.2023.12.019.

[21] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, and N. Kumar, “Blockchain-enabled cybersecurity efficient IIOHT cyber-physical system for medical applications,” IEEE Trans. Netw. Sci. Eng., vol. 10, no. 5, pp. 2466–2479, Sep./Oct. 2023.