DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to Visvesvaraya Technological University (VTU), Belagavi,
Approved by AICTE and UGC, Accredited by NAAC with 'A' grade & ISO 9001 – 2015 Certified Institution)
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560 111, India

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING
(Accredited by NBA Tier 1: 2025-2028)

Project Phase- I Report on

[22EC76]

Attribute-Based Cryptographic Access Control Framework for Decentralized Medical IoT Environments

Submitted in partial fulfillment for the award of the Degree of

Bachelor of Engineering
in
Electronics and Communication Engineering

Submitted by

A B Vishvajeeth	1DS22EC001
Malcolm Cephas	1DS22EC118
Shalini Sinha	1DS22EC200

Under the Guidance of
Dr S Thenmozhi
Associate Professor
Department of Electronics and Communication Engineering
DSCE, Bengaluru

VISVESVARAYA TECHNOLOGICAL UNIVERSITYJNANASANGAMA, BELAGAVI-590018, KARNATAKA, INDIA

2025-26

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to Visvesvaraya Technological University (VTU), Belagavi,
Approved by AICTE and UGC, Accredited by NAAC with 'A' grade & ISO 9001 – 2015 Certified Institution)
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560 111, India

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

(Accredited by NBA Tier 1: 2025-2028)

CERTIFICATE

Certified that the project report entitled "Attribute-Based Cryptographic Access Control Framework for Decentralized Medical IoT Environments" carried out by A B Vishvajeeth bearing a USN: 1DS22EC001 a bonafide student of DAYANANDA SAGAR COLLEGE OF ENGINEERING, an autonomous institution affiliated to VTU, Belagavi in partial fulfillment for the award of Degree of Bachelor of Electronic and Communication Engineering during the year 2025-2026. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The Project Phase-I report has been approved as it satisfies the academic requirements with respect to the work prescribed for the said Degree.

Signature of the Guide	Signature of the HoD	Signature of the Principal
Dr S Thenmozhi	Dr. Shobha K.R	Dr. B G Prasad
Associate Professor	Dean IQAC, Prof & Head	Principal
Dept. of ECE, DSCE	Dept. of ECE, DSCE, Bengaluru	DSCE, Bengaluru
Bengaluru		

Name of the Examiners	Signature with date
1.	.....
2.	.....

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to Visvesvaraya Technological University (VTU), Belagavi,
Approved by AICTE and UGC, Accredited by NAAC with 'A' grade & ISO 9001 – 2015 Certified Institution)
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560 111, India

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

(Accredited by NBA Tier 1: 2025-2028)

CERTIFICATE

Certified that the project report entitled "Attribute-Based Cryptographic Access Control Framework for Decentralized Medical IoT Environments" carried out by Malcolm Cephas bearing a USN: 1DS22EC118 a bonafide student of DAYANANDA SAGAR COLLEGE OF ENGINEERING, an autonomous institution affiliated to VTU, Belagavi in partial fulfillment for the award of Degree of Bachelor of Electronic and Communication Engineering during the year 2025-2026. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The Project Phase-I report has been approved as it satisfies the academic requirements with respect to the work prescribed for the said Degree.

Signature of the Guide	Signature of the HoD	Signature of the Principal
Dr S Thenmozhi	Dr. Shobha K.R	Dr. B G Prasad
Associate Professor	Dean IQAC, Prof & Head	Principal
Dept. of ECE, DSCE	Dept. of ECE, DSCE, Bengaluru	DSCE, Bengaluru
Bengaluru		

Name of the Examiners	Signature with date
1.	.....
2.	.....

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to Visvesvaraya Technological University (VTU), Belagavi,
Approved by AICTE and UGC, Accredited by NAAC with 'A' grade & ISO 9001 – 2015 Certified Institution)
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560 111, India

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

(Accredited by NBA Tier 1: 2025-2028)

CERTIFICATE

Certified that the project report entitled "Attribute-Based Cryptographic Access Control Framework for Decentralized Medical IoT Environments" carried out by Shalini Sinha bearing a USN: 1DS22EC200 a bonafide student of DAYANANDA SAGAR COLLEGE OF ENGINEERING, an autonomous institution affiliated to VTU, Belagavi in partial fulfillment for the award of Degree of Bachelor of Electronic and Communication Engineering during the year 2025-2026. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The Project Phase-I report has been approved as it satisfies the academic requirements with respect to the work prescribed for the said Degree.

Signature of the Guide	Signature of the HoD	Signature of the Principal
Dr S Thenmozhi	Dr. Shobha K.R	Dr. B G Prasad
Associate Professor	Dean IQAC, Prof & Head	Principal
Dept. of ECE, DSCE	Dept. of ECE, DSCE, Bengaluru	DSCE, Bengaluru
Bengaluru		

Name of the Examiners	Signature with date
1.	.....
2.	.....

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to Visvesvaraya Technological University (VTU), Belagavi,
Approved by AICTE and UGC, Accredited by NAAC with 'A' grade & ISO 9001 – 2015 Certified Institution)
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560 111, India

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

(Accredited by NBA Tier 1: 2025-2028)

DECLARATION

We, A B Vishvajeeth (1DS22EC001), Malcolm Cephas (1DS22EC118), Shalini Sinha (1DS22EC200), respectively, hereby declare that the project work entitled "Attribute-Based Cryptographic Access Control Framework for Decentralized Medical IoT Environments" has been independently done by us under the guidance of Dr S Thenmozhi , Associate Professor, ECE department and submitted in partial fulfillment of the requirement for the award of the degree of Bachelor of Electronics & Communication Engineering at Dayananda Sagar College of Engineering, an autonomous institution affiliated to VTU, Belagavi during the academic year 2025-2026 for the VII Semester Autonomous Course.

We, the students of VII Semester Major-project group/ batch no. D5 do hereby declare that the entire major-project phase 1 has been done on our own. We further declare that we have not submitted this report either in part or in full to any other university for the award of any degree.

A B Vishvajeeth	1DS22EC001
Malcolm Cephas	1DS22EC118
Shalini Sinha	1DS22EC200

PLACE: Bangalore

DATE:

ACKNOWLEDGEMENT

The satisfaction and euphoria accompanying the successful completion of any task would be incomplete without the mention of people who made it possible under constant guidance and encouragement. We sincerely thank the Management of Dayananda Sagar College of Engineering, Bengaluru.

We express our sincere regards and thanks to **Dr. B G Prasad**, Principal, Dayananda Sagar College of Engineering, Bengaluru. His constant encouragement guidance and valuable support have been an immense help in realizing this project.

We express our sincere regards and thanks to **Dr. Shobha. K.R**, Professor & Head, Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru. Her incessant encouragement guidance and valuable technical support have been an immense help in realizing this project. Her guidance gave us the environment to enhance our knowledge, and skills and to reach the pinnacle with sheer determination, dedication, and hard work.

We would like to express profound gratitude to our guide **Dr. S Thenmozhi**, Associate Professor, Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru who has encouraged us throughout the project. Her moral support enabled us to complete the work successfully.

We express our sincere thanks to Project Coordinator **Dr. S Thenmozhi**, Associate Professor, **Dr. Manasa R**, Assistant Professor of the Department of Electronics and Communication Engineering for their continues support and guidance. We thank all teaching and non-teaching staff of the Department of Electronics and Communication Engineering for their kind and constant support throughout the academic journey.

A B Vishvajeeth	1DS22EC001
Malcolm Cephas	1DS22EC118
Shalini Sinha	1DS22EC200

ABSTRACT

We present an Attribute-Based Cryptographic Access Control Framework in this project that is intended to be used in Medical IoT (MIoT) scenarios that are decentralized, thus solving the security, compliance, and granularity issues related to the ongoing handling of medical data that are very pressing. The overriding concern is that the attribute-based authorization should not only be facilitated or imposed but also the risks related to key abuse, unauthorized disclosures, and discontinuities arising from medical data that is ever flowing between distributed endpoints should be minimized at the same time. The framework is utilizing Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and a hybrid blockchain–off-chain architecture where the blockchain part provides immutable auditability and authorization of policies via smart contracts, and the off-chain part allows for scalability with regard to processing encrypted medical data. Methodologically, the system consists of user-defined structured attribute assignment, decentralized user key generation, user attribute-based encryption with user-defined access policy embedded in the encryption, verifiable outsourced decryption, and logging that is tamper-resistant. Assessment shows a reduction in client-side computation, the ciphertext will remain constant in size, and confidentiality, integrity, as well as traceability, have been enhanced through the utilization of distributed ledger technology. The final result is a secure and flexible access-control scheme that can be deployed in various heterogeneous nodes across the medical sector to share information that is protected in encrypted form through MIoT devices and clinical systems. Remote diagnostics, interoperable sharing of EHRs, and secure data streams generated by IoMT are some of the potential applications. The future direction includes AI support in dynamic access policies, compatibility across me

Keywords: *Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Medical Internet of Things (MIoT), Blockchain-Based Access Control, Smart Contracts, Verifiable Outsourced Decryption, Distributed Ledger Technology (DLT).*

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Full Form
AA	Attribute Authority
ABE	Attribute-Based Encryption
AC	Access Control / Access Control Server
AES	Advanced Encryption Standard
AI	Artificial Intelligence
APPI	Act on the Protection of Personal Information (Japan)
AR	Augmented Reality
BPM	Beats Per Minute
BT	Blockchain Technology
CBC	Cipher Block Chaining
CID	Content Identifier
CIANA	Confidentiality, Integrity, Availability, Non-Repudiation, Authentication
CKKS	Cheon–Kim–Kim–Song (Homomorphic Encryption Scheme)
CNN	Convolutional Neural Network
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CPU	Central Processing Unit
DAG	Directed Acyclic Graph
DHT	Digital Humidity and Temperature sensor (DHT22)
DL	Deep Learning
DLT	Distributed Ledger Technology
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECG	Electrocardiogram
EHR	Electronic Health Record
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation
GCM	Galois/Counter Mode
HMAC	Hash-Based Message Authentication Code

Abbreviation	Full Form
HIPAA	Health Insurance Portability and Accountability Act
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IoMT	Internet of Medical Things
IoT	Internet of Things
IPFS	InterPlanetary File System
JSON	JavaScript Object Notation
KGC	Key Generation Center
LPWAN	Low-Power Wide Area Network
ML	Machine Learning
MIoT	Medical Internet of Things
MQTT	Message Queuing Telemetry Transport
PBFT	Practical Byzantine Fault Tolerance
PHI	Personal Health Information
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PoW	Proof of Work
PRE	Proxy Re-Encryption
QKD	Quantum Key Distribution
RNN	Recurrent Neural Network
RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithm
TA	Trace Authority
TEEs	Trusted Execution Environments
TPS	Transactions Per Second
WSN	Wireless Sensor Network
WBAN	Wireless Body Area Network
Wi-Fi	Wireless Fidelity
WIoMT	Wearable Internet of Medical Things

Chapter-1

Introduction

1.1 Overview

The Medical Internet of Things (MIoT) has become an essential part of modern healthcare, allowing for uninterrupted patient monitoring, data collection, and remote doctor evaluation, among other things. Such systems are decentralized and, hence, their output consists of Personal Health Information (PHI) and Personally Identifiable Information (PII) that are extremely sensitive and must be protected against unauthorized access, misuse of keys, and privacy violations. The traditional, centralized access-control models have proven to be insufficient for MIoT ecosystems because of the complexity of these systems, their limited scalability, and the impossibility of executing fine-grained, attribute-based permissions in a decentralized network.

To solve these problems, this project introduces an Attribute-Based Cryptographic Access Control Framework that merges Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with a mixed blockchain-off-chain architecture. The blockchain offers decentralized trust, immutable audit logs, and automatic policy application through smart contracts, while the off-chain encrypted storage guarantees scalability and data privacy. This framework not only provides fine-grained authorization but also decentralized key management, verifiable outsourced decryption, and tamper-proof data traceability—all of which contribute to the secure and compliant sharing of medical data between various MIoT devices and healthcare institutions.

1.2 Problem Statement

Despite the fact that Medical IoT (MIoT) systems provide essential health data in real-time from various locations and devices, the current access-control models are still mainly centralized and unable to apply fine-grained, cryptographically verifiable authorization in decentralized settings. Present CP-ABE techniques cover the area of attribute-based access but still experience certain problems. These include the vulnerability to key-abuse, lack of user identification, increase in the size of encrypted data with the complexity of the policy, and high decryption time that is even more than the capability of the restricted IoT nodes. These restrictions indicate a significant

difference between theoretical CP-ABE models and the actual security needs of modern MIoT infrastructures. Moreover, the research indicates a lack of integration of decentralized trusted mechanisms - e.g. blockchain - with CP-ABE to offer unalterable audit logs, verifiable outsourced decryption, and automated policy enforcement. The current frameworks are not able to adapt to the upcoming requirements for data governance regarding confidentiality, traceability, regulated data deletion, and secure interoperability among healthcare networks from multiple institutions. In order to close these gaps, a unified access-control framework that is cryptographically enforced and can control the entire process of issuing keys and decryption, with the added benefit of using blockchain for securing decentralized verification against tampering needs to be addressed.

1.3 Objectives

- Implement a Decentralized, Fine-Grained Access Control Mechanism
- Ensure Cryptographic Accountability and Prevent Key Abuse
- Optimize Performance for Resource-Constrained IoMT Devices

1.4 Motivation

The swift growth of Medical IoT (MIoT) ecosystems has facilitated the exchange of real-time data and the monitoring of health on a continuous basis, but at the same time it has posed challenging issues of security, privacy and compliance that are very complicated. The traditional, centralized access-control models are not capable of securing the sensitive PHI and PII that are moving across various devices with different characteristics, limited resources and different healthcare sectors. Such systems create single points of failure, have a limited capacity for scalability and do not provide a strong support for the fine-grained, attribute-based authorization. Moreover, current ABE schemes produce large ciphertexts, impose high decryption times and do not offer key misuse tracing mechanisms—making them unfit for MIoT. The stringent confidentiality, accountability and verifiable data handling requirements set by global regulations such as GDPR and HIPAA have created a strong demand for a decentralized, cryptographically robust solution. This results in the establishment of an Attribute-Based Cryptographic Access Control Framework that uses CP-ABE, blockchain and off-chain storage to ensure secure, efficient, and compliant medical data sharing in decentralized MIoT settings

Chapter-2

Literature Survey

The literature review provides an overview of the current state of research regarding secure data management in Medical IoT (MIoT) systems and particularly discusses four main areas: attribute-based encryption, blockchain-enabled access control, lightweight cryptography, and decentralized storage. The review also pointed out the pros and cons of different frameworks in the field, which include but are not limited to key abuse, ciphertext expansion, resource constraints, interoperability, and regulatory compliance. Through the critical analysis of these researched works, this part of the thesis not only delineates the major security and performance issues that are still present in decentralized healthcare situations but also prompts the development of a new access-control framework that will be more efficient, traceable, and cryptographically enforced.

Table 2.1: Literature Review on ABE, Blockchain, MioT, and Decentralized Storage

Reference Number	Key Points	Objectives	Technologies Used	Research Gaps
[1]	Through wearable technology, smart devices, and cloud-based data sharing for real-time monitoring, the Internet of Things (IoT) is revolutionizing the healthcare industry. To guarantee safe and dependable IoT use, experts call for more robust security measures, and the US, EU, and WHO create eHealth regulations.	Diagnosing and Finding Health issues before it becomes an issue Medicine has been reactive all this time, try to make it proactive Remote vital tracking by experts (doctors)	Cloud Computing, Grid Computing, Big Data, Networks, Ambient Intelligence, AR, Wearables	Standardization and Interoperability Architectural and Platform Issues Resource Constraints and Low-Power Protocols Security and Data Protection Operational, Financial, and Safety Challenges Environmental and Health Impacts
[2]	Covers advances in wearables, sensors, blockchain, edge-AI, and cryptography in healthcare, stressing regulatory compliance, patient-centric design, and the	Predicting and Preventing sickness before symptoms, Making healthcare proactive from reactive, Easier accessibility in	Network of medical devices, AI analysis, Decision Making, Remote Diagnosis, Edge AI, Big Data, Blockchain	Data Security Patient Privacy System Reliability

	role of ML in diagnosis and monitoring.	medicine to everyone		
[3]	Highlights need for stronger security, protocol interoperability, and patient-centric usability. Reviews biosensors, cloud/fog-edge computing, and cryptographic standards. Barriers include regulatory hurdles, fragmented standards, and lack of user-focused designs.	Real Time Health Diagnosis, Smart Hospital Systems, Higher Quality of Life, Detecting Anomalies	Nano Tech, Pill sized sensors, Real time Medicine ,Wearables, Lightweight Cryptography, Decision Making	Hardware Hurdles (sensors in the body) Privacy concerns Different players and standardization Security Risks Communication and Networking Challenges
[4]	Framework integrates multiple sensors, cloud computation, and ML-based analytics for prediction. Ensures data security and scalability, tested for various patient-centric use cases and real-time remote access	Secure and real time patient monitoring; Accurately track people and services; Collect, share, monitor, store, and analyse data	Wearable Sensors, Cloud and Big Data Support, Wide Body Area Network (WBAN), RFID Wi-Fi, ZigBee, BLE, LPWAN	Security and Privacy, Quality of Service , (Performance, Stability, Cost),Energy Constraints ,Computational Load
[5]	Uses AES+RSA (not CP-ABE) for faster, less resource-intense cryptography; smart contracts for patient consent, revocation, and emergency delegation; and full audit trail on a public blockchain for all operations, with plans to migrate to a consortium chain for cost scalability.	Creating a Health Record with the following properties, Confidentiality, Access Control, Integrity, Emergency Access, Interoperability, Decentralisation	Blockchain, Inter Planetary File System, Smart Contacts, Encryption Techniques, RSA, AES, SHA 256	Cost Challenge, Future Mitigation, Improved Security, Emergency, Accessibility
[6]	Reviews key protocols (ZigBee, BLE, LoRa WAN) and advocates for CIANA (Confidentiality, Integrity, Availability, Non-repudiation, Authentication) emphasis. Calls for lightweight security, device-level measures, and continuous adaptation of	review the current state of security and privacy in IoMT. Examine, classify, and characterize security techniques and solutions. Review and discuss attack use cases,	Implantable Devices, Wearable Devices, Ambient Devices, Stationary Devices, Blockchain (MedSBA, BAKMP-IoMT, Health-Chain), SSA, ABE, Biometrics, ECC,	Time Complexity, Energy Consumption, Resource Complexity, Need for ML approaches, Security in Network Layer, Anomaly Detection, Access Control

	IDS/IPS for health environments	challenges, and future directions. Minimal Human Intervention	ECDSA, Deep Learning, Hybrid PCA-GWO +DNN, Deep Belief Network	
[7]	Permissioned blockchains (like Hyperledger) are more efficient than Ethereum for health data. AI-driven methods enhance contract security/fraud detection. Key challenges are quantum security, regulatory compliance, interoperability, scalability, and energy use.	Enhanced Data Security; Privacy Protection; Improved Interoperability; Efficiency and Transparency; Patient Autonomy and Data Control;	Distributed Networks (P2P, IPFS), Decentralized Blockchain, PoW, BFT, RAFT, ABE, Cryptography, FHIR Chain, HIPAA, GDPR, FHIR	Scalability, Regulatory Compliance, Interoperability ,Transaction Costs, Quantum Attacks, Need for Quantum Resilient Architecture
[8]	Most frameworks target technological not organizational risk. ML and blockchain are vital for intrusion detection and privacy. There is a critical need for updated, comprehensive risk management databases, and none of the reviewed frameworks fully integrate security measures.	Review progress in developing IoMT risk assessment and management frameworks Check if these frameworks focus on technological security design and measures Determine whether they also assess organizational security practices.	Machine Learning, Deep Learning, Blockchain, Digital Twins, IoMT, Attacks	No assessment of organizational measures, Need for comprehensive frameworks, Design of general risk management database for IoMT, Framework for overall IS security level
[9]	This paper reviews IoMT cybersecurity, noting major risks like unpatched systems, unencrypted data, and weak authentication in devices such as pacemakers and infusion pumps. It suggests network segmentation to limit breaches and recommends using AI and machine learning for early threat detection.	Address and discuss core cybersecurity problems Examine a variety of solutions Investigate and detail specific mitigation strategies	Network Segmentation, HIPAA, GDPR, Machine Learning, AI, IoMT, Blockchain	No New Solutions. Outdated Technology. Did Not Build Any New Tool, Suggested Only The Existing Ones. HIPPA Law Is Too General, Gap In Creating Specific Standards And Regulations. Sensitive Information.

[10]	The framework stores AES-encrypted medical images in IPFS, while the blockchain records their hashes and access rules through smart contracts. Edge nodes perform key generation and encryption using ECC to reduce delay. For secure data exchange between hospitals, keys are shared via ECDH.	Achieving Low Latency Higher Throughput Improved Security and Data Integrity Reduced Storage Costs	Blockchain, IPFS, Edge Computing, ECC, AES, RTOS, SHA 256, HIPFS PID,HID	Substantial Computational Requirements. Potential Edge Node Overload. Limited Real-World Validation. Machine Learning Integration.
[11]	The paper outlines a three-layer WIoMT architecture (Perception, Network, Application) and identifies key risks such as unsecured networks, unencrypted data, and missing updates. Regression analysis showed security and privacy as the strongest predictor of WIoMT adoption, with users most concerned about unauthorized data access and network insecurity	Analyse factors influencing user trust and adoption Identify key security and privacy risks Evaluate the predictive impact of technical factors	WIoMT, EHR, RFID, Portable Medical Apps, Wi-Fi, Bluetooth, PKI, Qualtrics	Study limited to Australian users. Survey model explains only 54% variance. Self-reported survey may bias results.
[12]	The framework stores encrypted IoT data off-chain in IPFS, with Hyperledger Fabric managing metadata and access policies. It applies CP-ABE for access control, a game-theoretic model for data pricing, and CKKS homomorphic encryption for secure data analysis. Tests achieved 64.5 TPS write and 515.3 TPS read throughput.	Adapt "End Edge Cloud" Collaboration Data Confidentiality Fine Grained Access Control	Blockchain, IPFS, ABE, Homo-morphic Encryption, KGC, CPABE	Limited Device Recourses Untrustworthy Network Environment Highly Sensitive User Privacy Serious Data Silos
[13]	Core systems include WSNs, RFID tracking, and IoT-based data acquisition. Blockchain enhances data integrity and privacy via distributed ledgers and smart contracts. AI, ML, DL, and CNNs enable automated diagnosis, while 5G provides low latency and	Trace IoT research in healthcare since its emergence. Identify which countries or world regions contribute most to the development of IoT research in healthcare. Identify	RFID, Actuators, Sensors, Mobile Phones, OSI model, ML, DL, CNN, Big Data, Edge Computing	Security and Privacy (Critical Issues) Trust and Acceptance Interoperability, Scalability, Mobility Data Storage, Ownership, Control Barriers to Wide Scale Implementation

	high reliability for body sensor networks and remote surgery.	the most impactful scholars and publications in IoT research in healthcare		
[14]	Addresses key security issues such as key abuse, privacy, and computation limits. The framework uses five entities for secure data sharing, with anonymous IDs for privacy, outsourced decryption, and fixed-size ciphertext to reduce storage.	To provide key abuse prevention and traceability. To reduce the user's computational burden. To enhance cloud storage efficiency	CP-ABE, IoMT, Cloud Computing, Cryptography Key Exchange, Access Structure	Cloud Storage Efficiency. Encryption/ Decryption Efficiency
[15]	Focussing on global privacy regulations such as GPDR, HIPAA, CCPA, PIPEDA, APPI and LGPD. Analysed regulatory conflicts with blockchain immutability. Proposing hybrid structure combining hash registries with encrypted medical data storage. Smart contracts help dynamic consent and policy compliance. Cryptography techniques ensure integrity, confidentiality	analyse and compare major international personal data protection and healthcare regulatory guidelines	GPDR (Europe), HIPAA (USA), CCPA(USA), PIPEDA(Cannada), Privacy Act 1988(Australia), APPI(Japan), AAMCEP(Japan	Extend Global Understanding. Proof of Concept Work. Validate/Implement BT in real scenarios.
[16]	This paper proposes a blockchain–IPFS hybrid framework to secure PHI and PII in smart healthcare systems and ensure GDPR compliance. It uses blockchain for immutability and traceability and integrates with Hyperledger for encryption, record management, and ownership verification.	Propose a GDPR-Compliant Framework. Implement Secure Off-Chain Storage. Enable Secure Data Sharing	Blockchain, IPFS, Smart Contacts, GDPR	Integrating Mobile API for Patient Traceability. Including Emergency Service Scenarios

[17]	a comprehensive technical survey of the Biomedical IoT (Bio-IoT) ecosystem. Systematically maps and categorizes the constituent technologies, including biosensors, multi-layer communication protocols (like BLE, 6LoWPAN, MQTT), and key architectural standards such as FHIR and IEEE 802.15.6 .	expand on the current protocols and architectures of medical IoT. Most relevant protocols and technologies specifically for medical IoT as well as the challenges	IoT, Healthcare IoT, wireless communication, wearable technology, Raspberry Pi, Arduino WSNs, 5G, LTE, ZigBee, 6LoWPAN , IPv6,biosensors, transducers	Slow Adoption Rate Regulatory Issues High barrier for entry
[18]	introduces a new cryptographic primitive (OC-BTCP-ABE) that features compulsory black-box traceability, making it impossible for adversaries to distinguish a normal ciphertext from a tracing ciphertext .	Proposing a new CP-ABE scheme that simultaneously achieves Black-Box Traceability and Computational Outsourcing Capabilities. Significantly improving the tracing efficiency. Achieving high computational efficiency and practicality	Compulsory Black-Box Traceable CP-ABE with Outsourcing of Computation, CP-ABE, Cryptographic Access Control, Black-box traceability, KeyGen algorithm, Elliptic curve group	Inefficient Decryption for Resource-Constrained Devices Quantum Threats Assessment
[19]	identifies the most critical security risks in healthcare as the lack of device visibility and the proliferation of unpatchable legacy systems .	Protect patient safety and privacy Maintaining availability of patient care services	Medical Devices, Smart beds, Virtual care telemetry, HVAC systems, Legacy workstations	Healthcare being a top target for attacks Lack of visibility and inventory capabilities
[20]	provides a simulation-based performance analysis comparing various encryption techniques for healthcare IoT. It models the trade-offs between robust algorithms (AES, ECC) and lightweight ciphers (Speck, PRESENT) , and also discusses the role of hardware-based security like TEEs and HSMs in protecting device keys.	Investigate specific security needs and risks linked with Internet of Things (IoT) devices Provide a comprehensive analysis of sophisticated encryption methods	AES, ECC, QKD, Multi Party Computing, HSM, Speck and Simon Block Cipher	Lack of standardized security protocols Difficulty in ensuring interoperability necessity for continuous research and development in encryption methods and security solutions

[21]	Provides a simulation-based analysis of encryption methods for healthcare IoT, comparing strong algorithms (AES, ECC) with lightweight ciphers (Speck, PRESENT) and discussing hardware security options like TEEs and HSMs for key protection.	Investigate specific security needs and risks linked with Internet of Things (IoT) devices Provide a comprehensive analysis of sophisticated encryption methods	AES, ECC, QKD, Multi Party Computing, HSM, Speck and Simon Block Cipher	Lack of standardized security protocols Difficulty in ensuring interoperability necessity for continuous research and development in encryption methods and security solutions
[22]	same as the above. Provides a comparative case. study on the encryption and performance factors.	Explore lightweight encryption methods tailored for IoT healthcare applications and evaluate their effectiveness. Conduct a detailed comparison of lightweight encryption methods. Identify future research directions necessary to address emerging challenges in IoT healthcare systems	AES-128, SIMON/SPECK, SKINNY, PICCOLO, Crypto Core, CLEFIA, RC6, KATAN, SPONGENT, LED.	Quantum-Resistant Encryption Energy Efficiency Context-Aware Security
[23]	A security architecture combining private blockchain, Proxy Re-Encryption, and ABE, enabling patients to delegate data access to doctors through proxy-transformed ciphertext without exposing private keys.	Propose an architecture that integrates private blockchain and Proxy Re-Encryption . Ensure tamper-proof record-keeping using blockchain while enabling fine-grained access control through PRE	Blockchain, Proxy Re-Encryption (PRE), Smart Contracts, IoT devices , ABE	Further optimization is needed to minimize energy consumption and computational costs for resource-limited IoT devices focus on enhancing interoperability with other healthcare systems

[24]	This paper proposes and benchmarks a practical security framework for IoMT systems that integrates AES-256 for data confidentiality and HMAC hashing to ensure data integrity and authenticity . Its performance analysis on a medical dataset confirms the framework adds robust security with a negligible computational overhead, demonstrating its real-world feasibility.	Suggest a comprehensive security framework to provide the confidentiality, integrity, and authenticity of data transmission .Demonstrate the implementation and feasibility of a security model to protect the multifarious healthcare architecture	AES-256 encryption, HMAC (Hash-based Message Authentication Code) hashing, SHA-256 (HMAC-SHA256), Diffie-Hellman key exchange method, PyCrpytodome framework	Validation and Resilience continuous need for enhancement approach to minimize latency for real-time applications

[1] Internet of Things for Health Care: A Comprehensive Survey. Discuss about various IoT healthcare architectures and applications emphasizing challenges like interoperability, energy efficiency, and security/privacy. Highlights the critical need for standardization and robust, scalable solutions for safe healthcare IoT deployment.

[2] A Survey on Transforming Healthcare with IoMT: Reviews IoMT devices/platforms enabling continuous and proactive healthcare monitoring and decision-making and identifies research gaps in interoperability, system security, and validating large-scale real-world implementations.

[3] Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges covers the topics of Maps biomedical IoT layers, including biosensors and edge-cloud computing, with AI-based analytics for personalized medicine and discusses unresolved issues such as data privacy, regulatory compliance, and scaling barriers.

[4] IoT-Based Healthcare-Monitoring System for Quality of Life surveys wearable and ambient sensor systems for vital tracking and health monitoring in chronic and elderly patients. It also emphasizes that user security, privacy, and ease-of-use are paramount for sustained improvements in quality of life.

[5] Med-Block: Secure Health Record System Using Blockchain and IPFS proposes a blockchain and IPFS hybrid for secure, tamper-proof EHR storage with smart contracts managing access and

consent. It also notes scalability and cost challenges, proposing permissioned chains to enhance practical deployment.

[6] Security and Privacy Management in Internet of Medical Things surveys cyber threats targeting IoMT layers and reviews adaptive security solutions tailored to resource-constrained devices and urges lightweight, context-aware intrusion detection and access control for medical IoT environments.

[7] Smart Contracts, Blockchain and Health Policies analyzes blockchain smart contracts automating health policy enforcement and patient data control it also highlights challenges in scalability, regulatory alignment, and evolving quantum-security threats.

[8] Internet of Medical Things Security Frameworks researches most IoMT security models lack organizational risk measures, focusing mainly on technical defenses and recommends a comprehensive risk management framework integrating organizational, technical, and procedural controls.

[9] Internet of Things (IoT): Cybersecurity Risks in Healthcare involves the details of cybersecurity issues from legacy devices, weak encryption, and unpatched systems in healthcare IoT and proposes network segmentation, stronger authentication, and encryption to mitigate prevalent risks.

[10] Zero-Trust Medical Image Sharing Using Blockchain and IPFS designs a decentralized, zero-trust medical image sharing framework combining AES encryption, blockchain, and ECC key management and demonstrates secure, scalable data sharing with low latency but notes edge node computational load concerns.

[11] Security Risks and User Perception towards Adopting Wearable IoMT reports that privacy and security concerns significantly impact willingness to adopt wearable health devices and highlights the importance of addressing unauthorized access and network security fears among users.

[12] Blockchain-Based Secure Data Transaction and Privacy Scheme proposes end-edge-cloud architecture with Hyperledger and IPFS using CP-ABE and homomorphic encryption for data

privacy and achieves fine-grained access control and high throughput but acknowledges IoT device constraints.

[13] IoT in Healthcare: Taking Stock and Moving Forward reviews healthcare IoT technologies and applications, underlining barriers including security, privacy, trust, and interoperability and advises for addressing technological and social challenges to enable broad adoption.

[14] CP-ABE-Based Medical Data Sharing proposes ciphertext-policy attribute-based encryption for secure medical data sharing with key abuse prevention and incorporates outsourcing of decryption to reduce patient device load while maintaining strong security.

[15] Reflections about Blockchain in Health Data Sharing examines conflicts between health data privacy laws and blockchain immutability and suggests hybrid approaches where encrypted data are off-chain and blockchains store hashes and consent records.

[16] GDPR Compliant Data Storage and Sharing in Smart Healthcare presents blockchain and IPFS-based framework for GDPR-compliant health data storage and dynamic consent management and notes ongoing challenges such as mobile integration and emergency access scenarios.

[17] Biomedical IoT: Enabling Technologies and Architectural Elements classifies key biomedical IoT protocols and standards and identifies adoption slowdowns due to regulation and costs and emphasizes layered architectures from sensing to application.

[18] Compulsory Black-Box Traceable CP-ABE with Outsourcing introduces a CP-ABE with black-box traceability and outsourced decryption to prevent key misuse and reduce device load and researches for an approach promising yet resource-heavy for very constrained IoT devices.

[19] ARMIS Report on Medical and IoT Device Security highlights lack of asset visibility and legacy unpatchable systems as chief risks for healthcare cybersecurity and recommends continuous monitoring, agentless device discovery, and network segmentation to enhance protection.

[20] Advanced Encryption Techniques in Healthcare IoT simulates trade-offs between strong and lightweight ciphers, emphasizing energy, latency, and security balance and calls for standardized encryption profiles adapted to diverse healthcare IoT constraints.

[21]Encryption Analysis for Healthcare IoT compares encryption algorithms and hardware protections, reaffirming the need to match algorithms to device context and threat level.

[22]Lightweight Encryption Methods for IoT-Based Healthcare reviews a suite of lightweight block ciphers suitable for constrained medical devices and discusses future quantum-resilient needs.

[23] Blockchain and Proxy Re-Encryption for Medical IoT Records proposes private blockchain integrated with proxy re-encryption to allow patient-controlled access delegation without key exposure and notes the need for further optimization to reduce energy and computation overhead.

[24] AES-256 Encryption and HMAC Hashing in IoT Smart Healthcare demonstrates an AES-256 and HMAC-SHA256 framework for IoMT data confidentiality and integrity with minimal performance impact and recommends further validation in real-time and large-scale scenarios to bolster resilience.

The project proposed is aims at eliminating critical security and performance issues in the protection of medical data, by bringing mechanisms that ensure accountability, efficiency, and adherence to regulations. It stops the most important misuse from happening through identity embedding that can be traced, thus dealing with the accountability in the traditional ABE schemes. The whole setup allows for decryption which is a significant support to resource-strapped IoMT devices, resulting in a local computational load reduction without exposing secret keys. Trust is further fortified amongst the healthcare networks since blockchain smart contracts enforce policies that are unalterable and create audit logs that are impervious to tampering. These innovations are in direct response to the issues of GDPR/HIPAA compliance, the need for data to be traceable, and the high computational cost associated with the use of existing cryptographic methods. Thus, the solution would be a lot more applicable in the case of the real-world deployments of IoMT.

Chapter-3

Problem Analysis and Design

3.1 Analysis

This section identifies the functional needs, performance expectations, hardware/software requirements, and operational constraints associated with designing a decentralized cryptographic access-control framework for Medical IoT (MIoT) environments.

Requirement Analysis

A. Functional Requirements:
   a. Attribute-Based Access Control:
      i. Implement CP-ABE for detailed and policy-controlled access based on encryption of the data that has been encrypted according to the specified attributes.
      ii. Facilitate the activities of user attribute assignment, key generation, and policy embedding.
   b. Decentralized Trust Management:
      i. Make use of blockchain technology for enforcement of policies that cannot be altered, execution of smart contracts, and auditing of access logs.
      ii. Facilitate the verification of access events in a decentralized manner.
   c. Encrypted Medical Data Handling:
      i. Obtain encrypted PHI/PII and IoMT data using symmetric encryption prior to off-chain storage.
      ii. IPFS will be the storage place for encrypted payloads and on-chain will be registered the content hashes.
   d. Key Abuse Prevention & Traceability:
      i. Ensure that interested users employ internal operations under secret situations to refrain from overwriting actual events.
   e. Verifiable Outsourced Decryption:
      i. Transfer substantially taxing cryptographic tasks to an Access Control (AC) server.
      ii. In the case of computations done by third parties, offer proof of their accuracy that is verifiable.
   f. Secure Data Sharing Across Entities:
      i. Allow patients, doctors, and healthcare institutions to share encrypted data using re-encryption or policy-based access.
   g. Device-to-Cloud Secure Communication

i. Support secure data upload from IoMT devices to IPFS via the user/gateway.
ii. Ensure end-to-end encryption.

B. Non-Functional Requirements
   a. Security & Privacy
      i. Confidentiality: Data encryption while not in use and during the transmission.
      ii. Integrity: Verification based on hashing and non-repudiation of the blockchain.
      iii. Accountability: Key misuse detection with complete traceability.
   b. Performance & Efficiency
      i. Constant size of ciphertext no matter how complex the access policy is.
      ii. Decryption overhead is decreased for IoMT devices with limited processing power.
      iii. Outsourced decryption is verifiable and requires little time for producing proofs.
   c. Reliability & Availability
      i. Decentralized storage and blockchain consensus eliminate a single point of failure.
      ii. Powerful functioning even when there are delays in the network or failures of nodes.
   d. Scalability
      i. Play the support role in ensuring expanding user controls as well as individual rights compliance.
      ii. On behalf of the medical networks, ETRIPS would help to disenfranchise the control of this medical documentation.
   e. Compliance Requirements
      i. Must accommodate GDPR doctrines such as “Privacy by Design” and “Right to Erasure.”
      ii. Compatibility with HIPAA, CCPA, and other international health care regulations.
   f. Usability
      i. Seamless user interaction for doctors, patients, and administrators.
      ii. Automated consent and authorization via smart contracts.

C. Hardware Requirements:
   a. IoMT Devices / Sensors
      i. Heart rate sensor (MAX30102)
      ii. ECG module (AD8232)
      iii. Temperature/Humidity sensor (DHT22)
   b. Microcontroller Platform

i. Arduino Uno R4 WiFi (for data collection & transmission)

c. Networking Hardware
   i. Wi-Fi router or hotspot for data transfer to backend
d. Storage Node
   i. IPFS local node or cloud-hosted IPFS gateway
e. Computer / Server Hardware
   i. System running Hyperledger Fabric blockchain network
   ii. AC server for outsourced decryption
   iii. TA and AA servers for key issuance and traceability

D. Software Requirements:
   a. Programming Languages
      i. Python / Go (Smart contracts & backend development)
      ii. JavaScript / Node.js (IPFS and REST API integration)
      iii. C/C++ (Microcontroller-side programming)
   b. Platforms & Frameworks
      i. Hyperledger Fabric (permissioned blockchain)
      ii. IPFS (distributed storage)
      iii. OpenSSL / Crypto libraries (ABE, ECC, SHA-256)
      iv. CP-ABE library (Waters, Bethencourt, or custom implementation)
   c. Microcontroller Tools
      i. Arduino IDE
   d. Testing & Evaluation Tools
      i. Hyperledger Caliper (benchmarking)
      ii. Postman / MQTT interface (device-to-server testing)

E. Constraints
   a. Device Constraints
      i. Low processing power & memory of IoMT nodes.
      ii. Limited battery capacity for wearable/portable sensors.
   b. Network Constraints
      i. Variable latency in decentralized blockchain networks.
      ii. Bandwidth limitations for real-time medical data.
   c. Storage Constraints
      i. On-chain storage must remain minimal—only hashes & metadata.
      ii. IPFS node availability affects data retrievability.
   d. Security Constraints
      i. Must protect against collusion attacks, insider threats, and key misuse.
      ii. Smart contract vulnerabilities must be minimized.
   e. Regulatory Constraints
      i. Data deletion requirements under GDPR (Right to be Forgotten).
      ii. Compliance with healthcare regulations (HIPAA, CCPA, APPI, etc.).

f. Cost & Infrastructure Constraints
   i. Running multiple blockchain nodes increases operational cost.
   ii. IPFS and blockchain hosting require stable server resources.

3.2 Block Diagram

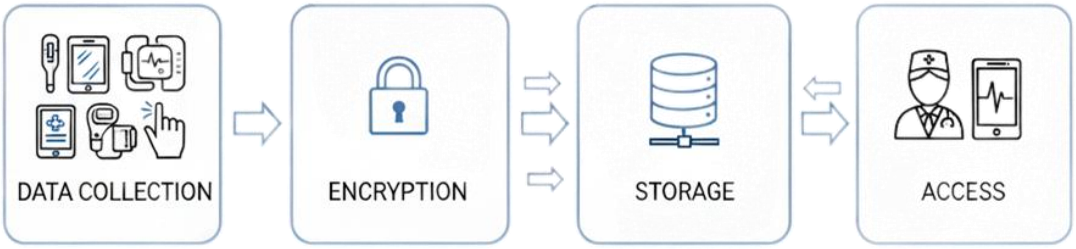

Fig.3.1 Block Diagram of the Proposed Methodology

- Data Collection: Various Internet of Medical Things (IoMT) devices, like wearables and sensors, constantly gather sensitive physiological data, producing raw Protected Health Information (PHI) and Personally Identifiable Information (PII). Encryption: The collected data undergoes encryption right at the device, using a hybrid approach: Symmetric key encryption ensures the payload remains confidential and efficient. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) embeds fine-grained attribute-based access control into the ciphertext, enforcing flexible, policy-driven data access. No unencrypted health data ever leaves the edge device, greatly improving privacy.
- Storage: The encrypted data is stored on off-chain distributed storage (e.g., IPFS nodes). Content identifiers (hashes), access policies, and transaction logs are immutably recorded on a permissioned blockchain for integrity, auditability, and traceability. This system ensures even if off-chain data is compromised, all references and access remain secure and tamper-proof.
- Regulatory, security controls: The use of blockchain and distributed storage ensures compliance with standards such as HIPAA/GDPR and enables robust auditing, tamper-proof data retention, and proof of origin.
- Access by authorized users: Only healthcare professionals with the right attribute credentials (e.g., clearance, specialization) can decrypt and access patient records, as enforced by the CP-ABE policy. Optional outsourced decryption reduces computation on local devices and supports efficient access.
- End-to-End Secure Data Lifecycle: The full data pipeline emphasizes decentralized control, cryptographically enforced privacy, tamper-resistance, and tightly regulated access from initial sensing to final data consumption.

Chapter-4

Methodology

The entire methodological framework is shown in this chapter, which was used for the design, implementation, and validation of the proposed Attribute-Based Cryptographic Access Control Framework for Decentralized Medical IoT (MIoT) Environments. The methodology elaborates on the system architecture, operational workflow, cryptographic processes, and evaluation strategy that are going to be carried out in Phase II. The aim is to outline the procedure for the establishment of each subsystem and their combination into a working end-to-end security solution in detail.

4.1 Flow diagram

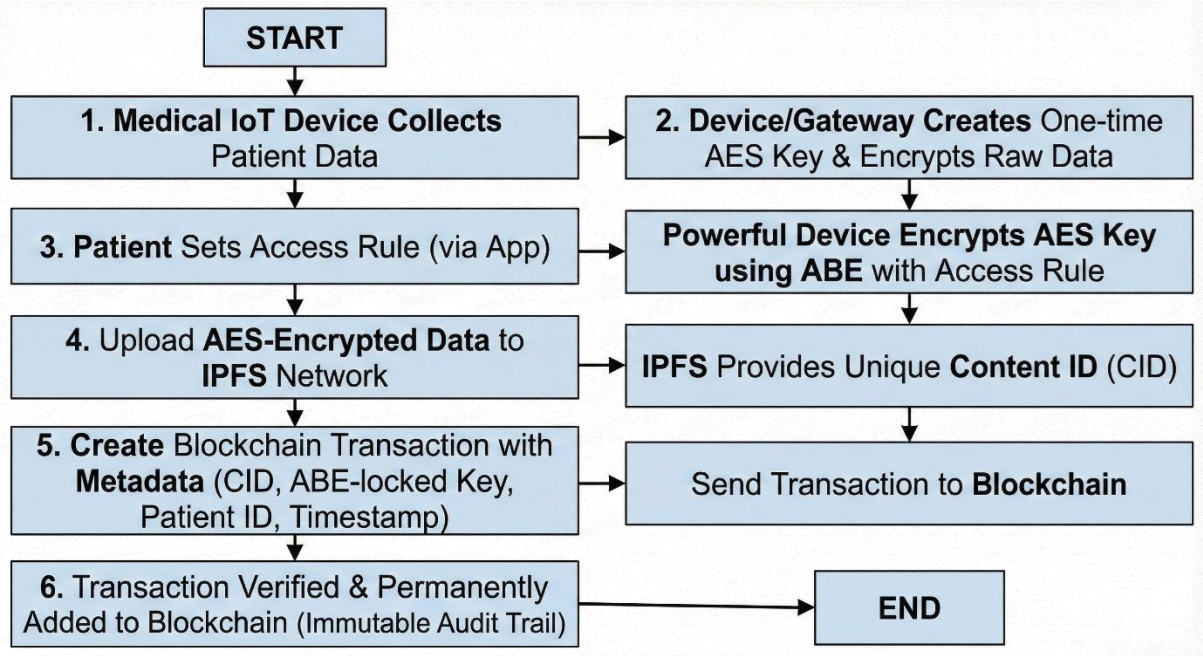

Fig.4.1 Flow diagram of the Proposed Methodology

Figure 4.1 illustrates the complete secure data-handling workflow of the proposed MIoT access-control system. The whole process begins with the capture of raw data by a medical IoT device from a patient, followed by immediate one-time AES session key encryption at the edge generated by the medical device or a nearby gateway. The patient or an authorized controller then specifies the access policy through an app once the data has been made secure. Using ABE, a more powerful device, such as a smartphone or edge node, subsequently encrypts the AES key based on the access policy, permitting only those with the right attributes to decrypt it. The AES-encrypted data is dispatched to the IPFS network, which assigns a CID that permanently links to the stored file as its reference. Next, a lightweight blockchain transaction containing only the CID, the ABE-encrypted AES key, and other crucial metadata such as patient ID and timestamp is produced. After being verified by the blockchain network, this becomes part of an immutable audit trail. In summary, Fig. 4.1 elaborates on the ways in which AES encryption, ABE, IPFS, and blockchain technology collaborate to offer a secure, transparent, and decentralized medical data management solution in MIoT environments.

4.2 System Architecture

The framework of the system includes these components:

- IoMT Device Layer: Gathers the primary physiological data through sensors.
- Gateway/Edge Layer: Encrypts the data via AES and executes ABE key wrapping.
- Attribute Authority (AA): Provides the secret keys based on the attributes.
- Trace Authority (TA): Inserts concealed identity markers for the detection of key abuse.
- Access Control (AC) Server: Conducts decryption of ABE on the outsourced data and issues the proofs of verifiability.
- Blockchain Network: Holds the metadata (CID, encrypted keys, timestamps).
- IPFS Storage: Keeps the medical data encrypted and off-chain.

4.3 Methodology Steps

Step 1: IoMT Data Collection Module

The initial step in acquiring data is to connect the MAX30102, AD8232, and DHT22 sensors to the Arduino Uno R4 WiFi, which facilitates non-stop monitoring of patient vitals in real-time. The microcontroller, through its digitizing and processing functions, draws the output of the sensor, whether analog or digital, and turns him/her into structured physiological values. Then,. These readings are sent through a wire together in one common format, that is a JSON packet, for uniform processing downstream. After formatting, the data is securely sent to the gateway or mobile device through the use of light protocols like MQTT or HTTP, thus assuring efficient and reliable delivery into the larger MIoT security pipeline.

Step 2: Symmetric Encryption (AES Module)

The structured sensor data is sent to the gateway where it is immediately subjected to the symmetric encryption process ensuring confidentiality before the data actually leaves the device. A one-time AES-256 session key is created with a cryptographically secure random generator, and the raw PHI/PII is encrypted with either CBC or GCM mode depending on the requirement for integrity. This process turns the plaintext readings into irreversible ciphertext which cannot be deciphered without the corresponding key. Encryption latency and CPU load in the process are also measured to confirm that the method is suitable for low-power IoMT environments. The execution of AES at the edge guarantees that the framework provides a protection for sensitive medical data even in untrusted networks or storage nodes.

Step 3: Attribute-Based Encryption (CP-ABE Module)

Currently, the technology is employing Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in a way that the AES session key is encrypted under a highly detailed access policy which specifies who is entitled to decrypt the medical data. A trustworthy gateway or edge node makes a Boolean policy (e.g., Doctor AND Cardiology OR EmergencyStaff) and incorporates it straight

into the CP-ABE encryption workflow. Secret keys are provided by the Attribute Authority (AA), whereas the Trace Authority (TA) includes non-extractable identity markers during key generation that facilitate forensic tracing of leaked keys. The CP-ABE module, depending on the choice of a Python library or a Waters/Bethencourt-based scheme, is utilizing bilinear pairings on the elliptic curves to impose policy-driven decryption. Only the individuals whose attributes fulfill the policy can obtain the AES key, and the embedded trace markers offer a robust cryptographic accountability against key misuse.

Step 4: Off-Chain Storage (IPFS Integration)

The medical data that has been encrypted is afterwards uploaded to the IPFS off-chain storage layer, which is a distributed, content-addressable system that does not depend on central servers. A local or cloud node of IPFS is set up to be part of the peer-to-peer network, which guarantees redundancy and fault-tolerant availability. Once the file encrypted with AES is uploaded, the IPFS automatically divides it into chunks, applies Merkle-DAG hashing, and creates a unique Content Identifier (CID) which is based only on the ciphertext hash. Any change in the data results in a different CID thus providing verification of integrity. This CID is stored for future access and serves as a permanent link to the encrypted file. Performance tests evaluate upload and retrieval latency, as well as CID matching. By this means, the IPFS provides large-scale, tamper-proof storage while at the same time ensuring that no sensitive medical data is ever directly placed on the blockchain.

Step 5: Blockchain Layer (Metadata Recording + Smart Contracts)

The blockchain layer operates on a private Hyperledger Fabric network with a separate channel specifically for medical data, thus providing limited and secure access for healthcare stakeholders only with required permissions. In the process of putting the AES-encrypted data on IPFS, the gateway makes a blockchain transaction that involves nothing but metadata: CID, the CP-ABE–encrypted AES key, a pseudonymized patient ID, and a secure timestamp. A Fabric smart contract takes care of this metadata by applying schema validation, performing authorization

checks, and making a tamper-proof record before a ledger entry is committed. Transaction is uniformly replicated across peers using consensus protocols like Raft or PBFT. The storage of only hashes instead of medical data guarantees the system's privacy and at the same time it has an immutable audit trail for forensic analysis. The conducting of controlled tests confirms the correct handling of metadata, enforcement of policies, and integrity of the ledger. Therefore, the blockchain layer provides non-repudiation, verifiable provenance, and traceability aligned with regulation without scalability issues associated with full on-chain storage.

Step 6: Access Control Server (Outsourced Decryption)

The AC server, during the outsourced decryption phase, performs the heavy pairing and exponentiation operations necessary for CP-ABE, thereby lessening the computational burden on the resource-limited IoMT devices. Upon a user's access request, the AC server gets the ABE-encrypted AES key from the blockchain metadata, carries out the heavy decryption steps, and produces a cryptographic correctness proof to authenticate the computation. It subsequently sends to the user both the partially decrypted key and the proof, who then only needs to conduct a lightweight final step to get the AES key. This method dramatically enhances the performance while simultaneously providing strong security guarantees..

Step 7: User Application for Data Access

During the last step, the authorized healthcare user gets the protected medical record back by first downloading the encrypted data from IPFS using its CID and then getting the blockchain metadata—such as the ABE-encrypted AES key and the timestamp. The user device receives the partial decryption output and correctness proof from the AC server and then verifies the proof to make sure the outsourced CP-ABE computation was performed accurately. The user then uses their CP-ABE secret key to carry out the final lightweight step of recovering the AES session key. The application then uses this key to decrypt the medical data and reconstruct the sensor readings for secure display. This process guarantees that only correctly authorized users can access sensitive health information, thus confidentiality and integrity are kept throughout the MIoT data flow.

Step 8: System Testing and Evaluation

Table 4.1 Testing and Evaluation Metrics for each step

Test Category	**Metrics**
AES Module	Latency, throughput
CP-ABE	Keygen time, encryption time, decryption time
Outsourced Decryption	Reduction in client workload
IPFS	Upload and retrieval time, CID consistency
Blockchain	Transaction latency, throughput, block creation time
Access Control	Policy enforcement accuracy
Security Tests	Unauthorized access attempts, key leak simulation

Table 4.1 provides a concise overview of the main testing categories and metrics that were utilized to assess the performance, security, and correctness of the suggested MIoT access-control framework. The AES module is evaluated with respect to latency and throughput, where the best performance is characterized by less than 5 ms for encryption latency and very high throughput, which is good for real-time medical data streams. The CP-ABE component is tested through the measurement of key-generation, encryption, and decryption times, targeting less than 50 ms for key generation, less than 40 ms for encryption, and less than 80 ms for decryption. This ensures that the attribute-based policies do not add considerable overhead. The outsourced decryption part of the system measures the workload reduction for the client, which is ideally achieved by 60–80% lower computation duration than local CP-ABE decryption, thus, it becomes a viable solution for low-power IoMT devices.

The performance of IPFS is measured by upload and retrieval times, where the ideal values are below 200 ms and CID consistency has to be 100% reproducible, which assures trustworthy off-chain storage. The blockchain layer is subjected to testing for transaction latency (less than 1 second), throughput (more than 100 transactions per second), and block creation time (less than 2 seconds), thus, confirming the logging of metadata in real-time. Access control precision is determined by checking whether only the users with the attributes satisfying the policy are able to decrypt the data, with the expected precision of 100%. Moreover, security tests consist of unauthorized access attempts and simulated key-leak situations, where ideal results indicate no successful decryptions of unauthorized parties and successful detection of leaked keys using the traceability approach. The system's efficiency, robustness, and adherence to secure MIoT data-flow requirements are all validated by these metrics combined.

Chapter-5

Work Done so Far

From our initial testing and prototyping we were able to get the following results

Sensor Quality checks:

In order to guarantee the reliability of the physiological data that were collected, the three modules MAX30102, AD8232, and DHT22 underwent a number of quality checks for their outputs done by sensors. Such checks examine the stability of the signals, the levels of noise, the consistency of the sampling, and the accuracy of the response when the sensor is in normal operation. It is necessary to evaluate the performance of the sensors before the readings are integrated into the MIoT security pipeline since poor-quality signals can affect not only medical interpretation but also cryptographic processing.

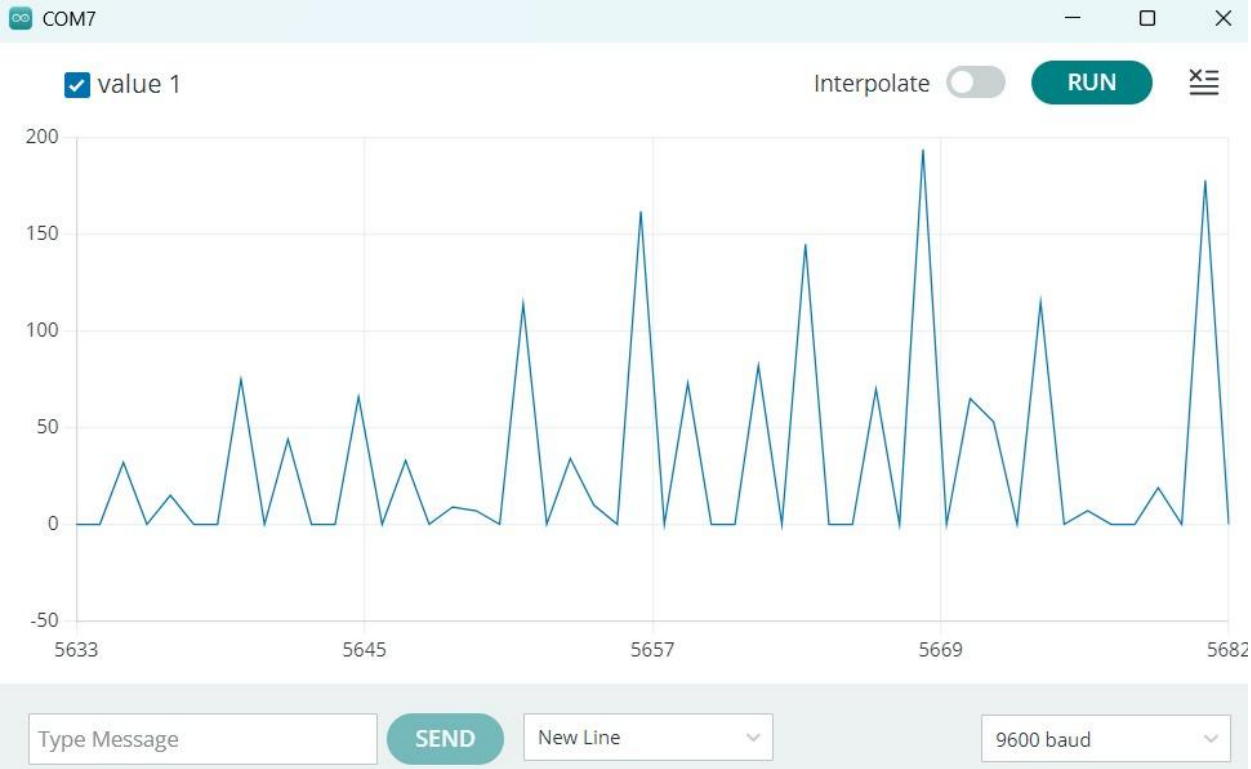

Fig 5.1: Plot of ECG graph when tested on ourselves

Fig 5.1 shows the ECG graph that was plotted on the serial monitor of Arduino IDE when the ECG electrodes were hooked up to our body, the ideal value ranging around 50 to 75 and the spiking values appearing when we frantically waved our hands around

Table 5.1: Initial Test Value from MAX30102 Sensor

IR=501	Avg BPM=74.66
IR=496	Avg BPM=74.66
IR=497	Avg BPM=74.66
IR=505	Avg BPM=74.66
IR=1482	Avg BPM=74.66
IR=92020	Avg BPM=76.48
IR=93772	Avg BPM=76.48
IR=93736	Avg BPM=76.81
IR=92389	Avg BPM=76.81
IR=87012	Avg BPM=76.81

Table 5.1 shows the infrared (IR) intensity values taken from the MAX30102 sensor and also the average heart rate (BPM) calculated. The weakest IR readings (approximately 496 to 505) stand for the normal signal reflections which are usually seen when the finger is placed firmly on the sensor resulting in an average BPM of 74.66 which denotes heart activity at the baseline level very well. As the IR values get higher (like mid-range 1482 and even higher magnitudes 92,000–93,000) the sensor perceives the signal reflections as stronger ones which might be due to better finger contact, motion artifacts, or variations of perfusion. This has been the case with the IR intensities being a little up to the BPM value of 76.48–76.81. The BPM values are, however, still stable and nature-like, hence, it can be said that the heart-rate algorithm has been stable even amidst the changing light absorption levels. The very fact that the MAX30102 is able to provide accurate pulse detection at various strengths of contact and signal intensities is confirmed.

Fig 5.2: Health Dashboard Output once forming a local host to display the data

The system's real-time health monitoring dashboard is presented in Figure 5.2, which shows uninterrupted physiological data streamed from IoMT sensors. The upper left section depicts the temperature trend (°C), where step-wise alterations are reflective of gradual changes in the environment or the body surface that are being monitored by the DHT22 sensor. The upper right part shows the humidity (%) trend, which has been verified by room moisture conditions, indicating a smooth ramp-up. Heart rate (BPM) from the MAX30102 sensor is represented in the lower left section, where stable readings with negligible physiological changes are observed. The ECG waveform of the AD8232 module is shown in the lower right, the periodic R-peaks and normal cardiac electrical activity are easily visible. A "Latest 10 Readings" table below the charts provides synchronized timestamps and sensor values for quick reference. This figure is a testament to the system that it has been able to acquire, process, and display the real-time physiological signals loud and clear enough to continuously monitor health.

References

1. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678–708, 2015

2. D. A. A. Raj, K. V. Rukmani, S. Subiksha, P. Vimal, and K. Deepak, "A Survey on Transforming Healthcare with IoMT : The Power of Connected Medical Devices," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 2, pp. 267–277, 2024

3. M. Aledhari, R. Razzak, B. Qolomany, A. Al-Fuqaha, and F. Saeed, "Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions," IEEE Access, vol. 10, pp. 31306–31339, 2022

4. Abdulmalek, S.; Nasir, A.; Jabbar, W.A.; Almuhaya, M.A.M.; Bairagi, A.K.; Khan, M.A.-M.; Kee, S.-H. IoT-Based Healthcare- Monitoring System towards Improving Quality of Life: A Review. Healthcare 2022, 10, 1993.

5. D. Mohanapriya, S. Suresh Kumar, P. J. Vivin Shanker, M. Mukesh, and M. Sathish, "Med-Block: Secure Health Record Management System Using Blockchain with IPFS," Dept. of Computer Science and Engineering, Nandha College of Technology, Erode, Tamil Nadu, India.

6. R. Haque, H. Muhammad, and A.-S. K. Pathan, "Security and Privacy Management in Internet of Medical," J. Cybersecur. Priv., vol. 2, 2022

7. K. K. Kakumani, M. Tasnim, S. Parida, F. Omura, and S. Thapa, "Smart Contracts, Blockchain and Health Policies Past, Present and Future [v1]," Preprints.org, 2025

8. S. Svandova and Z. Smutny, "Internet of Medical Things Security Frameworks," Journal of Multidisciplinary Healthcare, vol. 17, pp. 2281–2301, 2024

9. R. Patel, "Internet of Things (IoT): Cybersecurity Risks in Healthcare," Undergraduate Research Project, Old Dominion University, 2020

10. A. Shahzad, W. Chen, Y. Zhang, and R. Kumar, "Zero-Trust Medical Image Sharing: A Secure and Decentralized Approach Using Blockchain and the IPFS," Symmetry, vol. 17, no. 4, p. 551, 2025

11. S. Thapa, A. Bello, A. Maurushat, and F. Farid, "Security Risks and User Perception towards Adopting Wearable Internet of Medical Things," Int. J. Environ. Res. Public Health, vol. 20, no. 8, p. 5519, 2023

12. J. Wu, Z. Bian, H. Gao, and Y. Wang, "A Blockchain-Based Secure Data Transaction and Privacy Preservation Scheme in IoT System," Sensors, vol. 25, no. 15, p. 4854, 2025

13. A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, and M. Iranmanesh, "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," Internet of Things, vol. 22, p. 100721, 2023

14. Y.-W. Hwang and I.-Y. Lee, "A Study on CP-ABE-Based Medical Data Sharing," Sensors, vol. 20, no. 17, p. 4934, 2020.

15. A. Corte-Real, T. Nunes, and P. R. da Cunha, "Reflections about Blockchain in Health Data Sharing: Navigating a Disruptive Technology," Int. J. Environ. Res. Public Health, vol. 21, p. 230, 2024

16. P. Bai, S. Kumar, K. Kumar, O. Kaiwartya, M. Mahmud, and J. Lloret, "GDPR Compliant Data Storage and Sharing in Smart Healthcare System: A Blockchain-Based Solution," Electronics, vol. 11, no. 20, p. 3311, 2022

17. M. Aledhari, R. Razzak, B. Qolomany, A. Al-Fuqaha, and F. Saeed, "Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions," IEEE Access, vol. 10, pp. 31306–31339, 2022

18. Y. Hu, H. Qiao, J. Ren, Z. Wang, J. Li, and P. Han, "Compulsory Black-Box Traceable CP-ABE with Outsourcing of Computation," Symmetry, vol. 17, no. 9, p. 1539, 2025

19. ARMIS - Medical and IoT Device Security for Healthcare

20. O. Simonoski and D. C. Bogatinoska, "BLOCK MEDCARE: Advancing healthcare through blockchain integration," International Journal on Cybernetics & Informatics (IJCI), vol. 13, no. 5, pp. 63–84, 2024

21. V. Salunkhe, C. Mokkapati, and A. Aggarwal, "Advanced Encryption Techniques in Healthcare IoT: Securing Patient Data in Connected Medical Devices," Modern Dynamics: Mathematical Progressions, vol. 1, no. 2, pp. 224-246, 2024

22. O. Sabri, B. Al-Shargabi, A. AbuArqoub, and T. Al-Hakami, "A Lightweight Encryption Method for IoT-Based Healthcare Applications A Review and Future Prospects," IoT, vol. 6, p. 23, 2025

23. A.-E. Jabri, C. Drocourt, M. Azizi, and G. Utard, "Leveraging Blockchain and Proxy Re-Encryption to Secure Medical IoT Records,"International Journal on Cybernetics & Informatics (IJCI), vol. 13, no. 4 pp, 2021.

24. E. O. Okpu and O. E. Taylor, "Analysing the Integration of AES-256 Encryption and HMAC Hashing in IoT Smart Healthcare Systems," Ci-STEM Journal of Digital Technologies and Expert Systems, vol. 2, no. 1, pp. 18–24, 2025