A PBL-I Report on: Different Security Attacks in Healthcare-IoT and Blockchain-Based Mitigation

Submitted to Manipal University Jaipur Towards the partial fulfillment for the Award of the Degree of BACHELORS OF TECHNOLOGY In Computers Science and Engineering 2025-2026

By Name of the Candidate(s) (12 pt.) Registration Number(s) (12 pt.)

Under the guidance of Prof. / Dr. / Mr./ Ms. XXXX…..XXXX……..XXXX

Signature of Supervisor

Department of Computer Science and Engineering School of Computer Science and Engineering Manipal University Jaipur Jaipur, Rajasthan

---

Table of Contents

I. Introduction to Problem (What, Why, How)

The integration of the Internet of Things (IoT) into the medical domain, forming the **Healthcare Internet of Things (H-IoT)** or **Internet of Medical Things (IoMT)**, has ushered in a

transformative era for patient care [C3]. H-IoT encompasses a vast network of interconnected medical devices, sensors, and software that facilitate real-time patient monitoring, remote diagnostics, and intelligent decision-making [C1]. These systems, ranging from wearable health monitors and implantable devices like pacemakers to hospital-wide asset tracking systems, promise to improve patient outcomes, reduce healthcare costs, and enhance the efficiency of medical services [C5]. However, this rapid digital transformation introduces a corresponding increase in **cybersecurity vulnerabilities**, posing a direct threat to patient safety and the integrity of sensitive medical data.

1.1 What is Healthcare IoT (H-IoT)?

H-IoT is defined as the ecosystem of connected medical devices and software applications that communicate with healthcare IT systems over a network [C3]. The primary components of this ecosystem include:

1. **Wearable and Remote Monitoring Devices:** Devices that collect physiological data (e.g., heart rate, blood glucose, ECG) from patients outside of traditional clinical settings.
2. **Implantable Medical Devices (IMDs):** Devices such as insulin pumps and cardiac devices that are directly connected to the patient’ s body and often communicate wirelessly.
3. **Hospital Infrastructure:** Connected devices within a hospital, including smart beds, infusion pumps, and imaging machines, which are networked for centralized management and data sharing.

The data generated by H-IoT devices is highly sensitive, often classified as **Electronic Health Records (EHRs)**, and is subject to stringent regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) in the US and the General Data Protection Regulation (GDPR) in Europe [C2]. The sheer volume, velocity, and variety of this data necessitate robust, scalable, and secure infrastructure.

1.2 Why is H-IoT Security Critical?

The criticality of H-IoT security stems from the direct link between device compromise and potential **physical harm** to patients, alongside the severe consequences of data breaches. Unlike traditional IT systems where a breach primarily results in financial or reputational damage, a successful cyberattack on an H-IoT device can lead to life-threatening scenarios, such as altering drug dosages in an infusion pump or disabling a pacemaker [C4].

The primary security challenges in H-IoT are rooted in the inherent limitations of the devices and the centralized nature of traditional healthcare IT systems [C5]:

- **Resource Constraints:** Many H-IoT devices are small, battery-powered, and have limited computational capacity, making it difficult to implement complex, high-overhead

cryptographic algorithms or robust security patches.

- **Legacy Systems:** Hospitals often rely on older, proprietary medical devices that were not designed with modern cybersecurity standards, creating easily exploitable entry points into the network.
- **Centralized Data Storage:** Traditional EHR systems rely on centralized servers, creating a **single point of failure**. A breach of this central authority exposes the entire patient population's data to theft, manipulation, or ransomware attacks [C1].

These vulnerabilities are actively exploited by malicious actors through various attack vectors, including **Man-in-the-Middle (MITM) attacks**, **Distributed Denial-of-Service (DDoS) attacks**, **Data Breaches**, and **Replay Attacks** [C4]. The consequences are severe, including unauthorized access to sensitive patient records, operational disruption of life-saving services, and the potential for direct patient harm.

1.3 How does Blockchain Address these Challenges?

Blockchain technology, a decentralized and distributed ledger, offers a paradigm shift in securing H-IoT ecosystems by addressing the fundamental weakness of centralization [C2]. By distributing data records across a network of nodes, blockchain eliminates the single point of failure and establishes a **trustless environment** where data integrity is maintained through cryptographic hashing and consensus mechanisms [C6].

The core features of blockchain that are particularly relevant to H-IoT security include:

- **Decentralization:** Data is not stored in one location, making it resilient to single-point attacks like DDoS or data breaches targeting a central server.
- **Immutability:** Once a transaction (e.g., a patient's vital sign reading) is recorded on the blockchain, it cannot be altered or deleted without the consensus of the network, providing a tamper-proof audit trail [C1].
- **Transparency and Auditability:** All transactions are visible to network participants, ensuring accountability and making it easy to trace the origin and access history of any data record.
- **Smart Contracts:** These self-executing contracts can automate access control policies, ensuring that only authorized entities (e.g., a specific doctor or a research institute with patient consent) can access specific data, thereby enforcing fine-grained authorization [C2].

By leveraging these properties, blockchain can serve as a secure, transparent, and auditable layer for managing H-IoT data, mitigating the risks associated with the most prevalent cyberattacks.

II. Literature Survey

A thorough review of recent literature reveals a growing consensus on the necessity of integrating Distributed Ledger Technology (DLT), particularly blockchain, to overcome the inherent security limitations of H-IoT systems. The research is primarily focused on developing novel frameworks that combine the decentralized nature of blockchain with advanced cryptographic and machine learning techniques to ensure data integrity, confidentiality, and availability [C7].

2.1 Overview of H-IoT Security Challenges and Traditional Solutions

The current landscape of H-IoT security is characterized by a constant struggle to secure resource-constrained devices against sophisticated attacks. Traditional security measures, while necessary, have proven insufficient due to their reliance on centralized trust models and the difficulty of patching a vast, heterogeneous network of devices [C3].

Common H-IoT Attack Vectors:

Attack Type	Description in H-IoT Context	Traditional Mitigation & Limitation
Man-in-the-Middle (MITM)	Interception of communication between an H-IoT device (e.g., a continuous glucose monitor) and a server, allowing attackers to eavesdrop on or manipulate data in transit.	**Mitigation:** TLS/SSL encryption, mutual authentication. **Limitation:** Vulnerable to certificate spoofing and weak key management on resource-constrained devices [C4].
Distributed Denial-of-Service (DDoS)	Flooding hospital networks or cloud servers with traffic, rendering critical services (e.g., EHR access, remote monitoring) unavailable.	**Mitigation:** Firewalls, Intrusion Detection Systems (IDS), traffic filtering. **Limitation:** Centralized servers remain a single point of failure; difficult to distinguish malicious from legitimate traffic under high load [C8].
Data Breaches/Tampering	Unauthorized access to centralized EHR databases, leading to the theft, alteration, or deletion of sensitive patient records.	**Mitigation:** Access control lists (ACLs), database encryption. **Limitation:** Insider threats, compromised central authority, and lack of an immutable audit trail to detect subtle data manipulation [C1].
Replay Attacks	Intercepting a legitimate command or data packet (e.g., a command to an insulin pump) and re-transmitting it later to trigger an unauthorized action or falsify a reading.	**Mitigation:** Timestamping, nonces (random numbers used once). **Limitation:** Requires robust synchronization and secure storage of nonces, which is challenging for low-power devices [C4].

Traditional solutions, such as simple encryption and centralized access control, often fail to provide the necessary resilience and auditability required for life-critical H-IoT applications. This gap has spurred research into decentralized, blockchain-based frameworks.

2.2 Review of Blockchain-Based Access Control Models

Access control is paramount in healthcare, ensuring that only authorized personnel (doctors, nurses, researchers) can view or modify specific patient data. Blockchain-based access control models leverage smart contracts to automate and enforce these policies in a tamper-proof manner [C2].

Framework 1: Attribute-Based Access Control (ABAC) on Blockchain [C9]

- **Concept:** Policies are defined based on the attributes of the user (e.g., "Doctor," "Cardiology Department") and the data (e.g., "ECG Data," "Patient X"). The smart contract checks these attributes against the policy before granting access.
- **Blockchain Role:** The blockchain stores the access policies and the encrypted data index. The smart contract executes the authorization logic.
- **Pros:** Highly flexible and fine-grained control; easily adaptable to complex healthcare hierarchies.
- **Cons:** High computational overhead for attribute matching and policy evaluation, which can impact the latency of real-time data access.

Framework 2: Role-Based Access Control (RBAC) with PoA Consensus [C1]

- **Concept:** A more structured approach where access is granted based on the user's defined role (e.g., "Primary Care Physician," "Nurse"). This is often implemented on a permissioned blockchain.
- **Blockchain Role:** Uses a **Proof of Authority (PoA)** consensus mechanism, where a limited number of pre-approved nodes (e.g., trusted hospitals or regulatory bodies) validate transactions. This ensures high throughput and low latency, making it suitable for real-time IoMT data.
- **Pros:** High performance and scalability due to PoA; strong accountability; simpler policy management than ABAC.
- **Cons:** Less granular control than ABAC; relies on the trust of the "authority" nodes.

Framework 3: Decentralized Storage with IPFS and Blockchain [C10]

- **Concept:** To address the storage limitations of blockchain, this model stores the actual large EHR files on a decentralized file system like the InterPlanetary File System (IPFS).
- **Blockchain Role:** The blockchain only stores the immutable hash (fingerprint) and the access control pointer to the data stored on IPFS. Smart contracts manage the decryption keys and access permissions.
- **Pros:** Solves the scalability and storage overhead issues of storing large medical files directly on the blockchain; ensures data integrity through hash verification.
- **Cons:** Introduces a dependency on a second system (IPFS); data retrieval latency can be a concern.

2.3 Review of Blockchain-Based Intrusion and Attack Detection Systems

Beyond access control, blockchain is being integrated with Artificial Intelligence (AI) and Machine Learning (ML) to create intelligent Intrusion Detection Systems (IDS) that can proactively identify and mitigate cyberattacks [C11].

Framework 4: Hybrid AI- and Blockchain-Powered Secure IoMT [C12]

- **Concept:** This framework uses a deep learning model (e.g., CNN-LSTM) to analyze network traffic and device behavior for anomalies indicative of an attack (e.g., DDoS, MITM).
- **Blockchain Role:** The ML model’ s training data, detection rules, and final attack reports are stored on the blockchain. This ensures that the IDS itself is tamper-proof and that the security logs are immutable and auditable.
- **Pros:** High accuracy in detecting zero-day and known attacks; the blockchain provides a trusted record of security events.
- **Cons:** High computational cost for the AI component; latency in recording real-time security events to the blockchain.

Framework 5: Dual-Channel Blockchain for Secure EHR Management [C13]

- **Concept:** Utilizes two separate blockchain channels: one for storing sensitive patient data (private/permissioned) and another for managing access control and device registration (public/permissionless or a second private chain).
- **Blockchain Role:** The dual-channel approach separates high-volume, sensitive data transactions from lower-volume, high-security access control transactions, optimizing performance and privacy.
- **Pros:** Enhanced privacy through data separation; improved scalability and throughput.
- **Cons:** Increased complexity in design and maintenance; requires secure cross-chain communication protocols.

Framework 6: Lightweight Trusted Framework for Secure Data Exchange [C14]

- **Concept:** Focuses on creating a framework suitable for resource-constrained H-IoT devices by employing lightweight cryptographic primitives and a streamlined consensus mechanism.
- **Blockchain Role:** Often uses a lightweight DLT like IOTA or a specialized private blockchain with a low-overhead consensus (e.g., PoA or Delegated Proof of Stake).

- **Pros:** Low computational and communication overhead, making it practical for IMDs and wearables; fast data exchange.
- **Cons:** May compromise on decentralization or security strength compared to full-scale public blockchains.

III. Comparative Study

The following tables provide a comparative analysis of the security attacks targeting H-IoT and the proposed blockchain-based mitigation frameworks, highlighting the necessity and effectiveness of the decentralized approach.

3.1 Comparative Analysis of H-IoT Security Attacks

This table compares the four major attack types identified in the H-IoT context, focusing on their target, impact, and the inherent limitations of traditional security measures.

Attack Type	Primary Target	Impact on Patient Care	Traditional Mitigation	Limitation of Traditional Mitigation
Man-in-the-Middle (MITM)	Data in Transit (Device-Server Communication)	Data manipulation (e.g., false readings), privacy breach, unauthorized command injection.	TLS/SSL, Mutual Authentication, VPNs.	Vulnerable to key compromise; high overhead for low-power devices; reliance on centralized Certificate Authorities.
Distributed Denial-of-Service (DDoS)	Network Availability (Hospital Servers, Cloud Infrastructure)	Service disruption, inability to access EHRs, delayed diagnosis, failure of remote monitoring.	Firewalls, Rate Limiting, IDS, Load Balancers.	Centralized architecture remains a single point of failure; difficulty in filtering sophisticated, distributed attacks.
Data Breaches/Tampering	Centralized EHR Databases	Identity theft, insurance fraud, compromised medical history, loss of patient trust.	Database Encryption, Access Control Lists (ACLs), Audit Logs.	Insider threats; lack of immutable, cryptographically verifiable audit trail; compromised central authority exposes all data.
Replay Attacks	Device Commands/Data Packets	Unauthorized medical intervention (e.g., incorrect insulin dose), falsification of current medical data.	Timestamping, Nonces, Session Keys.	Challenging to implement robust synchronization and secure nonce storage on resource-constrained devices; lack of a global, trusted time source.

3.2 Comparative Analysis of Blockchain Mitigation Frameworks

This table compares the key features and trade-offs of the blockchain-based frameworks reviewed in the literature, demonstrating how they collectively address the limitations of

traditional security.

Framework	Primary Focus	Blockchain Type	Consensus Mechanism	Key Security Feature	Trade-offs/Challenges
RBAC with PoA [C1]	Access Control, Data Integrity	Permissioned (Private)	Proof of Authority (PoA)	Fine-grained access control via Smart Contracts; High throughput.	Relies on trusted authorities; less decentralized than public chains.
ABAC on Blockchain [C9]	Fine-grained Access Control	Permissioned/Public	PoS/PoW (Variable)	Highly flexible policy definition based on user/data attributes.	High computational overhead for policy evaluation; latency issues.
IPFS & Blockchain [C10]	Data Storage Scalability	Permissioned/Public	PoS/PoW (Variable)	Stores large EHRs off-chain; integrity verified by on-chain hash.	Dependency on IPFS; potential data retrieval latency.
Hybrid AI- & BC-Powered IDS [C12]	Intrusion Detection	Permissioned (Private)	PoA/DPoS	Tamper-proof security logs; high accuracy in attack detection via ML.	High computational cost for the AI component; potential latency in log recording.
Dual-Channel BC [C13]	Privacy and Scalability	Dual (Private/Public)	PoA/PoS	Separation of sensitive data and access control transactions.	Increased system complexity; requires secure cross-chain communication.
Lightweight Trusted Framework [C14]	Resource-Constrained Devices	Permissioned (Private)	PoA/DPoS/IOTA Tangle	Low computational overhead; suitable for IMDs and wearables.	May compromise on decentralization or security strength.

IV. Problem Statement

The core problem addressed by this research is the **critical vulnerability of centralized Healthcare IoT (H-IoT) systems to sophisticated cyberattacks**, including Man-in-the-Middle (MITM), Distributed Denial-of-Service (DDoS), Data Breaches, and Replay Attacks, which not only compromise the confidentiality and integrity of sensitive Electronic Health Records (EHRs) but also pose a direct and life-threatening risk to patient safety due to the potential for unauthorized manipulation of medical devices. This vulnerability is exacerbated by the resource constraints of H-IoT devices and the single point of failure inherent in traditional centralized security architectures, necessitating the design and evaluation of a **decentralized, robust, and intelligent security framework** utilizing blockchain technology.

V. Objective

The primary objectives of this project are:

1. **Threat Classification and Analysis:** To systematically study and categorize the major security threats in Healthcare IoT systems, analyzing the attack vectors, vulnerabilities, and potential impact on patient safety, with a specific focus on MITM, DDoS, Data Breaches, and Replay Attacks.
2. **Design of a Blockchain-Based Security Framework:** To design a comprehensive, multi-layered security architecture that integrates H-IoT medical devices with a blockchain infrastructure, specifically utilizing a **Proof of Authority (PoA)** consensus mechanism for high performance and accountability.
3. **Integration of Advanced Security Components:** To incorporate advanced security techniques, including **XChaCha20-Encryption** for data confidentiality, a **Role-Based Access Control (RBAC)** mechanism enforced by smart contracts, and a **blockchain-integrated Machine Learning (ML) model** for real-time cyberattack detection.
4. **Evaluation of Mitigation Effectiveness:** To quantitatively assess the proposed framework’ s effectiveness in mitigating the identified security risks, particularly in terms of data integrity, access control, and the accuracy of attack detection, demonstrating superior performance over existing state-of-the-art approaches.

VI. Planning of Work/ Proposed Solution: Methodology

The proposed solution is a novel, highly secure, and intelligent healthcare ecosystem based on a **Blockchain-Based Security Framework** [C1]. This framework is designed to address the security and privacy challenges of IoMT data by combining the decentralization and immutability of blockchain with advanced cryptographic and machine learning techniques. The methodology outlines the architecture, key components, and the plan for implementation and evaluation.

6.1 Proposed Framework Architecture

The framework is structured into four main layers, ensuring end-to-end security from the H-IoT device to the data consumer:

1. **IoT Data Collection Layer:** Consists of all H-IoT devices (wearables, IMDs, sensors) that collect patient data. This layer is responsible for initial data acquisition and transmission to the next layer.
2. **Encryption Layer:** Data received from the IoT devices is immediately encrypted using a lightweight, high-performance cipher. The framework proposes using **XChaCha20-Encryption** due to its speed and strong security properties, making it suitable for resource-constrained devices [C1].
3. **Blockchain Layer:** This is the core of the framework, built on a **Permissioned Blockchain** utilizing the **Proof of Authority (PoA)** consensus mechanism.
    - **PoA Selection:** PoA is chosen for its high transaction throughput and low latency, which are critical for real-time H-IoT applications. It also provides strong accountability by relying on a set of pre-approved, trusted nodes (e.g., hospitals, regulatory bodies) to validate transactions.
    - **Smart Contracts:** Smart contracts are deployed to enforce the **Role-Based Access Control (RBAC)** policies, manage device registration, and record all data access attempts.
4. **Application and ML Layer:** This layer includes the user applications (e.g., doctor’s dashboard) and the **Blockchain-Integrated ML Model**.
    - **ML Model:** A machine learning model (e.g., Random Forest or a deep learning classifier) is trained on H-IoT network traffic data (e.g., the WUSTL-EHMS-2020 dataset) to detect cyberattacks in real-time.
    - **Blockchain Integration:** The ML model’s detection results and security logs are recorded on the blockchain, ensuring an immutable record of all security events and attack attempts.

6.2 Key Technological Components

XChaCha20-Encryption

The XChaCha20 stream cipher is selected for its **superior performance and security** compared to older ciphers like AES in resource-constrained environments [C1]. Its key advantages include:

- **Speed:** It is highly optimized for modern processors, offering faster encryption and decryption times (e.g., 0.61 and 0.71 seconds, respectively, in a similar study [C1]).
- **Security:** It uses a large 256-bit key and a 192-bit nonce, providing a high level of security against brute-force and collision attacks.
- **Lightweight:** Its simple design makes it ideal for implementation on low-power H-IoT devices without significant battery drain.

Role-Based Access Control (RBAC) via Smart Contracts

The RBAC model is implemented entirely through smart contracts on the blockchain. This approach ensures that access policies are transparent, immutable, and automatically enforced [C2].

- **Mechanism:** Each user is assigned a specific role (e.g., "Patient," "Nurse," "Specialist Doctor"). The smart contract checks the user's role and the requested data type against the predefined policy before releasing the decryption key or granting access.
- **Benefit:** This decentralized enforcement eliminates the risk of a central administrator being compromised, which is a major vulnerability in traditional RBAC systems.

Blockchain-Integrated ML Model for Attack Detection

The integration of an ML model (e.g., Random Forest or a specialized deep learning model) is crucial for providing an **intelligent defense layer** against evolving cyber threats [C12].

- **Function:** The ML model continuously analyzes network traffic and device behavior patterns. When an anomaly is detected, it is classified as a specific cyberattack (e.g., DDoS, MITM).
- **Blockchain Role:** The model's high-confidence detection results are immediately recorded as a transaction on the blockchain. This creates an immutable, cryptographically verifiable log of the attack, which can be used for immediate network response and post-incident auditing. This integration achieved a high accuracy of **99.43%** in detecting cyberattacks in a similar study [C1].

6.3 Detailed Mitigation Strategy for Specific Attacks

The proposed framework specifically counters the four identified attacks through its layered, decentralized design:

1. **Mitigation of Man-in-the-Middle (MITM) Attacks:**
    - **XChaCha20-Encryption:** Ensures that even if communication is intercepted, the data remains unintelligible to the attacker.
    - **Blockchain Authentication:** All devices and users must be registered and authenticated on the blockchain. The decentralized nature of the ledger prevents a single point of failure for certificate issuance or key management, making spoofing significantly harder.
2. **Mitigation of Distributed Denial-of-Service (DDoS) Attacks:**
    - **Decentralization:** The use of a distributed ledger eliminates the single, centralized server target. An attacker would need to overwhelm the entire network of PoA validator nodes, which is computationally infeasible.
    - **PoA Consensus:** The PoA mechanism ensures that only authorized, trusted nodes can participate in validation, effectively filtering out malicious traffic originating from botnets.
3. **Mitigation of Data Breaches/Tampering:**
    - **Immutability:** The core blockchain property ensures that once data is recorded, any attempt to tamper with it is immediately detectable by all other nodes, as the cryptographic hash of the block would change.
    - **RBAC Smart Contracts:** Unauthorized access is prevented by the smart contract, which acts as an unchangeable gatekeeper to the data. Any successful access is logged on the blockchain, providing a transparent and auditable record.
4. **Mitigation of Replay Attacks:**
    - **Timestamping and Sequence Numbers:** Every transaction (data reading or command) is automatically timestamped and assigned a unique sequence number by the smart contract before being recorded on the blockchain.
    - **Immutability Check:** The blockchain acts as a global, trusted sequence ledger. If an attacker attempts to replay an old command, the smart contract or the ML model will detect the duplicate sequence number or the invalid timestamp relative to the current block, and the transaction will be rejected [C4].

6.4 Implementation and Evaluation Plan

The implementation will follow a phased approach, focusing on proof-of-concept development and rigorous performance evaluation.

Phase 1: Proof-of-Concept Development

- **Blockchain Setup:** Deploy a private/permissioned blockchain network (e.g., using Hyperledger Fabric or Ethereum with PoA) and configure the validator nodes.
- **Smart Contract Deployment:** Develop and deploy the RBAC smart contracts to manage user roles and access policies.
- **Encryption Integration:** Implement the XChaCha20 encryption module on a simulated H-IoT device and integrate it with the blockchain transaction submission process.

Phase 2: ML Model Training and Integration

- **Dataset Acquisition:** Utilize a publicly available H-IoT security dataset, such as the **WUSTL-EHMS-2020 dataset** [C1], which contains labeled network traffic data for various cyberattacks.
- **Model Training:** Train the chosen ML model (e.g., Random Forest) to achieve high accuracy in classifying attack types.
- **Integration:** Integrate the trained ML model with the blockchain to record security events and trigger automated responses via smart contracts.

Phase 3: Performance Evaluation and Validation

The framework’ s performance will be evaluated against the following key metrics:

Metric	Description	Target Value (Based on Literature)
Attack Detection Accuracy	The ML model’ s accuracy in correctly identifying cyberattacks.	> 99.0% [C1]
Encryption/Decryption Latency	Time taken for the XChaCha20 cipher to process data on a simulated H-IoT device.	< 1.0 second [C1]
Transaction Throughput	Number of transactions (data records) the PoA blockchain can process per second.	High (Suitable for real-time H-IoT data volume)
Access Control Latency	Time taken for the smart contract to verify a user’ s access request.	Low (Minimal delay for medical personnel)

The final validation will involve simulating the four key attacks (MITM, DDoS, Data Breaches, Replay Attacks) against the framework and demonstrating the effectiveness of the blockchain-based mitigation strategies.

VIII. Bibliography/References

The following sources were consulted and referenced in the preparation of this report.

[C1] Verma, P., Bharot, N., Jhaveri, R. H., & Breslin, J. G. (2025). **A Blockchain-Based Security Framework for a Highly Secure and Intelligent Healthcare Ecosystem**. *Procedia Computer Science*, 270, 3668-3677. https://www.sciencedirect.com/science/article/pii/S1877050925031655

[C2] Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025). **Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey**. *Cluster Computing*. https://link.springer.com/article/10.1007/s10586-025-05308-x

[C3] Othman, S. B., et al. (2025). **Leveraging blockchain and IoMT for secure and scalable healthcare data management**. *Nature Scientific Reports*. https://www.nature.com/articles/s41598-025-95531-8

[C4] Fereidouni, H. (2025). **IoT and Man‐in‐the‐Middle Attacks**. *Security and Privacy*. https://onlinelibrary.wiley.com/doi/10.1002/spy2.70016

[C5] Khan, A. A., et al. (2025). **Blockchain-enabled secure Internet of Medical Things (IoMT) architecture for precision cancer data management**. *Journal of Cloud Computing*. https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-025-00775-4

[C6] Almarri, S., et al. (2024). **Blockchain Technology for IoT Security and Trust**. *Sustainability*, 16(23), 10177. https://www.mdpi.com/2071-1050/16/23/10177

[C7] Patruni, M. R., et al. (2026). **Intelligent IoT-Blockchain Ecosystem: A security perspective**. *Future Generation Computer Systems*. https://www.sciencedirect.com/science/article/abs/pii/S1574013725001194

[C8] Akkal, M., et al. (2024). **An Intrusion Detection System For Detecting DDoS Attacks In Blockchain-Enabled IoMT Networks**. *IEEE*. https://ieeexplore.ieee.org/document/10812635/

[C9] Namane, S., & Ben Dhaou, I. (2022). **Blockchain-Based Access Control Techniques for IoT Applications**. *Electronics*, 11(14), 2225. https://www.mdpi.com/2079-9292/11/14/2225

[C10] Patel, R., & Gupta, S. (2023). **Enhancing data integrity with IPFS and Polygon blockchain**. *IEEE Conference on Blockchain Applications*. https://ieeexplore.ieee.org/document/10288446/

[C11] Alsolai, H., et al. (2025). **A hybrid blockchain and AI-based approach for attack detection in IoMT**. *Ain Shams Engineering Journal*. https://www.sciencedirect.com/science/article/pii/S111001682500674X

[C12] Wang, X., et al. (2025). **Hybrid AI- and Blockchain-Powered Secure Internet of Medical Things Framework**. *Applied Sciences*, 13(5), 1466. https://www.mdpi.com/2227-9717/13/5/1466

[C13] Sahoo, A., Chatterjee, S., & Sobhanayak, S. (2025). **Secure Electronic Health Records Distribution in a Blockchain Enabled H-IoT System**. *SN Computer Science*. https://link.springer.com/article/10.1007/s42979-025-03918-1

[C14] Samant, P. K., et al. (2025). **A lightweight trusted framework for secure data exchange and medical diagnosis in IoMT**. *BMC Medical Informatics and Decision Making*. https://pmc.ncbi.nlm.nih.gov/articles/PMC12603095/

[C15] Shukla, H. (2025). **Different Security Attacks in Healthcare IoT and Blockchain-Based Mitigation**. *PBL-I Presentation Slides*. (User Provided)

[C16] Anonymous. (2025). **PathFinder Project Report Final**. *PBL-I Report Sample*. (User Provided)

[C17] Anonymous. (2025). **PBL-I Synopsis Format**. *PBL-I Format Document*. (User Provided)