International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(18s) 2026 pp. 1247-1273
https://doi.org/10.70917/ijcisim-2026-4973
Article

MediChainGuard: A Permissioned Blockchain-Based Framework for Patient-Centric Access Control and AI-Assisted Threat Detection in IoMT

Ramesh Mailapalli[1], A.C. Santha Sheela[2]

[1]School of Computing, Department of CSE, Sathyabama Institute of Science and Technology, Chennai, India.
Email: rameshpython24@gmail.com
[2]School of Computing, Department of CSE, Sathyabama Institute of Science and Technology, Chennai, India.
Email: santhasheela.cse@sathyabama.ac.in
Corresponding Author: Ramesh Mailapalli

Abstract: The rapid expansion of the Internet of Medical Things (IoMT) has enhanced remote patient monitoring, connected diagnosis, and continuous healthcare delivery. However, centralized healthcare systems remain vulnerable to single points of failure, unauthorized access, insider attacks, data tampering, and privacy breaches, creating significant challenges for secure Electronic Health Record (EHR) management. This paper presents MediChainGuard, a permissioned blockchain-based framework for patient-centric access control and AI-assisted threat detection in IoMT environments. The proposed framework integrates Decentralized Identity (DID) for secure authentication, blockchain-enabled patient consent management, a hybrid Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) model for context-aware authorization, a Break-Glass mechanism for emergency access, and SHA-256-based integrity verification for secure EHR protection. Furthermore, an AI-assisted anomaly detection module employing Isolation Forest-based analysis continuously monitors authentication logs, blockchain transactions, and user behavioural patterns to identify suspicious activities and cyber threats in real time. Experimental evaluation conducted in a simulated IoMT environment demonstrates improvements in authentication efficiency, authorization accuracy, EHR integrity protection, and threat detection performance while maintaining scalability through a permissioned Hyperledger Fabric architecture. The proposed framework provides a secure, transparent, auditable, and privacy-preserving solution for next-generation healthcare systems and establishes a foundation for integrating blockchain, artificial intelligence, and decentralized identity into secure IoMT ecosystems. Experimental evaluation was conducted using a simulated healthcare environment consisting of 15,000 patients, 4,000 healthcare professionals, and 25,000 IoMT devices over six months of operational activity.

Keywords: Internet of Medical Things (IoMT), blockchain, smart healthcare, electronic health records, decentralized identity, smart contracts, patient consent, RBAC, ABAC, anomaly detection

1. Introduction

The rapid advancement of the **Internet of Medical Things (IoMT)** has transformed modern healthcare by enabling continuous patient monitoring, remote diagnosis, smart medical devices, and real-time clinical decision-making [11],[15]. Wearable sensors, smart infusion pumps, electrocardiogram (ECG) monitors, glucose monitoring systems, and connected medical equipment continuously generate large volumes of sensitive patient information. These technologies improve healthcare quality and operational efficiency while supporting personalized medical services. However, the increasing interconnectivity of medical devices also introduces significant cybersecurity and

privacy challenges, particularly in protecting Electronic Health Records (EHRs) from unauthorized access, data tampering, and cyberattacks [11],[12].

Most existing healthcare information systems rely on centralized cloud-based architectures for identity management, authentication, and access control [3],[6]. Although centralized systems simplify administration, they suffer from several limitations, including single points of failure, limited transparency, insider attacks, and scalability issues. A successful cyberattack or server compromise can expose confidential patient information, disrupt healthcare services, and negatively impact patient safety. Moreover, traditional access control mechanisms often provide limited flexibility in handling dynamic healthcare scenarios such as emergency treatment, cross-hospital data sharing, and patient-controlled authorization [3],[6],[12].

Blockchain technology has emerged as a promising solution for addressing these challenges by providing a decentralized, immutable, and transparent platform for secure healthcare data management [5],[16],[17]. Through distributed ledger technology and smart contracts, blockchain enables secure authentication, automated authorization, and tamper-resistant audit logging without relying on a trusted central authority [1],[2],[5],[10]. Smart contracts can automatically enforce access policies, ensuring that only authorized healthcare professionals can access patient records while maintaining complete accountability for every access request [1],[2],[10].

Despite these advantages, existing blockchain-based healthcare security solutions still face several challenges. Most current approaches primarily focus on secure data storage or basic access control while overlooking important healthcare-specific requirements such as patient-controlled consent management, decentralized patient identity, emergency access during critical medical situations, and intelligent detection of malicious user behavior [3],[11], [12],[15]. Furthermore, maintaining the integrity of Electronic Health Records and protecting patient privacy remain major concerns in distributed healthcare environments [12], [15].

To address these limitations, this paper proposes **MediChainGuard**, a decentralized blockchain-based access control framework for secure Internet of Medical Things (IoMT) environments. The proposed framework integrates **Decentralized Identity (DID)** for secure identity management, **patient-controlled consent management** using blockchain-enabled smart contracts, and a hybrid **Role-Based Access Control (RBAC)** and **Attribute-Based Access Control (ABAC)** model to provide fine-grained and context-aware authorization. Additionally, a secure **Break-Glass Access** mechanism enables temporary emergency access for authorized healthcare professionals while maintaining complete auditability. To ensure the integrity of Electronic Health Records, the framework employs **SHA-256 hash-based verification** combined with encrypted off-chain storage. Furthermore, an **AI-assisted anomaly detection module** continuously monitors healthcare access patterns to identify insider threats, credential misuse, replay attacks, and other suspicious activities in real time.

The major contributions of this work are summarized as follows:

1. A decentralized identity management framework using DID for patients, healthcare professionals, and IoMT devices.
2. A blockchain-enabled patient-controlled consent management mechanism for secure Electronic Health Record (EHR) sharing.
3. A hybrid RBAC and ABAC authorization model implemented through smart contracts for fine-grained healthcare access control.
4. A secure Break-Glass emergency access mechanism with immutable blockchain audit logging.
5. A blockchain-based EHR integrity verification scheme using SHA-256 hashing and encrypted off-chain storage.
6. An AI-assisted anomaly detection module for identifying malicious activities and strengthening healthcare cybersecurity.

The proposed **MediChainGuard** framework provides a secure, transparent, scalable, and privacy-preserving architecture for next-generation smart healthcare systems by integrating blockchain technology, decentralized identity management, artificial intelligence, and intelligent access control mechanisms.

2. Formulation & Objectives

The rapid adoption of the **Internet of Medical Things (IoMT)** has transformed modern healthcare by enabling continuous patient monitoring, remote diagnosis, and intelligent clinical decision-making [11], [15]. However, most healthcare systems continue to rely on centralized authentication and access control mechanisms, making them vulnerable to single points of failure, unauthorized access, insider attacks, and privacy breaches [3], [6], [12]. Furthermore, existing healthcare security solutions provide limited support for patient-controlled consent, decentralized identity management, emergency medical access, and real-time threat detection [3], [11], [12], [15]. These challenges compromise the confidentiality, integrity, and availability of Electronic Health Records (EHRs), thereby affecting patient trust and healthcare service reliability [3], [12].

To address these limitations, this research proposes **MediChainGuard**, a decentralized blockchain-based access control framework for secure IoMT environments. The proposed framework integrates blockchain technology, smart contracts, decentralized identity (DID), patient-controlled consent management, and AI-assisted threat detection to provide secure, transparent, and privacy-preserving healthcare data management.

The objectives of the proposed research are as follows:

1. Eliminate dependence on centralized authentication systems by integrating blockchain, decentralized identity (DID), smart contracts, and permissioned distributed ledgers.
2. Provide fine-grained and context-aware healthcare access control through the integration of Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).
3. Enable patient-controlled consent management using blockchain smart contracts, allowing patients to securely grant, revoke, and monitor access to their Electronic Health Records.
4. Support secure emergency healthcare services through a blockchain-enabled Break-Glass Access mechanism with complete auditability and temporary authorization.
5. Ensure the integrity of Electronic Health Records (EHRs) using SHA-256 hash-based verification and encrypted off-chain storage.
6. Detect malicious activities in real time by integrating an AI-assisted anomaly detection module capable of identifying insider attacks, credential misuse, replay attacks, and abnormal access behaviour.
7. Improve the overall security, privacy, transparency, scalability, and efficiency of IoMT-based healthcare systems compared with existing blockchain-enabled healthcare access control frameworks.

3. Literature review

Blockchain technology has emerged as a promising solution for addressing security, privacy, and trust challenges in the **Internet of Medical Things (IoMT)** by enabling decentralized authentication, immutable audit trails, and secure healthcare data sharing. Recent research has demonstrated that blockchain-based access control mechanisms significantly improve data integrity and eliminate the limitations of centralized healthcare systems [3], [12], [15].

Liu *et al.* [1] proposed **Fabric-IoT**, a blockchain-based access control framework built on Hyperledger Fabric for Internet of Things (IoT) environments. Their architecture employs smart contracts to manage authentication, authorization, and access policy enforcement using decentralized ledger technology. Experimental results demonstrated improved throughput, distributed consensus, and secure data sharing. However, the framework does not support patient-controlled consent management, decentralized identity, or emergency healthcare access.

Sun *et al.* [2] introduced a lightweight blockchain-enabled IoT access control framework integrating Identity-Based Signatures (IBS), Attribute-Based Access Control (ABAC), and Hyperledger Fabric. Their approach reduces blockchain overhead through off-chain authorization while maintaining secure cross-domain communication. Although the framework improves authentication efficiency, it does not address Electronic Health Record (EHR) integrity verification or intelligent threat detection required in healthcare environments.

Kumar and Tripathi [3] proposed a blockchain-based healthcare access control framework to enhance secure Electronic Health Record sharing and authentication. Their model demonstrated improved privacy and secure healthcare data management through decentralized blockchain technology. Nevertheless, the framework primarily focuses on secure record sharing and lacks mechanisms for patient-controlled consent, decentralized identity management, and emergency medical authorization.

Hu *et al.* [4] developed **N-Accesses**, a blockchain-based access control framework that combines smart contracts with hash-chain techniques to generate secure time-limited access tokens. The proposed model improves transparency, auditability, and secure authorization in IoT environments. However, the framework does not consider healthcare-specific requirements such as Break-Glass emergency access and AI-assisted cybersecurity.

Recent studies have explored the integration of blockchain with Artificial Intelligence to improve healthcare cybersecurity. Messinis *et al.* [11] presented a comprehensive review of AI techniques for IoMT cybersecurity and highlighted the effectiveness of machine learning algorithms in detecting cyber threats and abnormal user behaviour. Similarly, Taherdoost [15] reviewed blockchain-based IoMT architectures and emphasized the importance of decentralized security mechanisms for protecting patient privacy, ensuring secure medical data sharing, and enhancing healthcare interoperability.

Hölbl *et al.* [12] conducted a systematic review on blockchain applications in healthcare and reported that blockchain significantly improves transparency, immutability, and trust in Electronic Health Record management. However, the survey also identified several open research challenges, including scalable identity management, fine-grained authorization, and secure interoperability among healthcare organizations.

Although existing blockchain-enabled healthcare frameworks have considerably improved authentication and secure data sharing, most existing approaches focus on individual aspects such as blockchain-based authentication, smart contract authorization, or AI-assisted cybersecurity. Very few studies integrate **Decentralized Identity (DID)**, **patient-controlled consent management**, **hybrid RBAC-ABAC authorization**, **Break-Glass emergency access**, **blockchain-based EHR integrity verification**, and **AI-assisted anomaly detection** within a unified IoMT security framework [3], [11], [12], [15].

To address these research gaps, this paper proposes **MediChainGuard**, a decentralized blockchain-based access control framework for secure Internet of Medical Things (IoMT) environments. The proposed framework integrates blockchain-enabled smart contracts, decentralized identity management, patient-controlled consent, hybrid RBAC-ABAC authorization, Break-Glass emergency access, SHA-256-based EHR integrity verification, and AI-assisted anomaly detection to provide a secure, scalable, transparent, and patient-centric healthcare security architecture.

4. Proposed Methodology

The proposed **MediChainGuard** framework presents a decentralized blockchain-based access control architecture for securing the **Internet of Medical Things (IoMT)**. Unlike conventional healthcare systems that rely on centralized authentication servers, MediChainGuard integrates **Blockchain**, **Decentralized Identity (DID)**, **Smart Contracts**, **Patient-Controlled Consent Management**, **Role-Based Access Control (RBAC)**, **Attribute-Based Access Control (ABAC)**, **Break-Glass Emergency Access**, **Electronic Health Record (EHR) Integrity Verification**, and **Artificial Intelligence (AI)-assisted Threat Detection** into a unified security framework. The proposed architecture enhances confidentiality, integrity, availability, transparency, and patient privacy while supporting secure healthcare data sharing among hospitals, healthcare professionals, and IoMT devices.

The MediChainGuard framework consists of eight functional layers, namely the User/Application Layer, Decentralized Identity (DID) Layer, Patient-Controlled Consent Management Layer, Smart Contract-Based Access Control Layer, Emergency Break-Glass Access Layer, Blockchain Layer, AI-Assisted Threat Detection Layer, and EHR Storage & Integrity Verification Layer, as shown in Fig. 1. Each layer performs a dedicated security function while collectively providing end-to-end protection for Electronic Health Records and healthcare transactions.

4.1 Overall MediChainGuard Architecture

The overall architecture of **MediChainGuard** is illustrated in **Fig. 1**. The proposed framework adopts a layered architecture consisting of the **User/Application Layer**, **Decentralized Identity (DID) Layer**, **Patient-Controlled Consent Management Layer**, **Smart Contract-Based Access Control Layer**, **Emergency Break-Glass Access Layer**, **Blockchain Layer**, **AI-Assisted Threat Detection Layer**, and **EHR Storage & Integrity Verification Layer**. These layers collaboratively provide secure authentication, authorization, privacy preservation, and intelligent threat detection for Internet of Medical Things (IoMT)-based healthcare environments.

Initially, IoMT devices continuously collect physiological and clinical information from patients and securely transmit the encrypted data to the healthcare gateway through secure communication protocols. Before accessing any healthcare resource, every patient, healthcare professional, and IoMT device must register through the **Decentralized Identity (DID)** module, where a unique blockchain identity, public-private key pair, and digital signature credentials are generated and verified.

After successful registration, the **Patient-Controlled Consent Management** module enables patients to **grant, modify, revoke, and review** access permissions for doctors, nurses, laboratories, hospital administrators, insurance providers, and other authorized healthcare stakeholders through blockchain-enabled smart contracts. Every consent transaction is permanently recorded on the blockchain, providing transparency, accountability, and immutable audit trails.

Whenever a healthcare professional requests access to Electronic Health Records (EHRs), the **Smart Contract-Based Access Control** module authenticates the user's decentralized identity and executes a hybrid **Role-Based Access Control (RBAC)** and **Attribute-Based Access Control (ABAC)** authorization mechanism. RBAC validates predefined healthcare roles, whereas ABAC evaluates contextual attributes such as department, hospital location, consultation schedule, patient consent, emergency status, and device trust level before making the final authorization decision. The authorization result is recorded in immutable blockchain audit logs.

For emergency situations where patient consent cannot be obtained, the **Break-Glass Access** module allows authorized emergency physicians to request temporary access to Electronic Health Records. The smart contract validates predefined emergency policies before granting time-limited authorization. Every emergency access event is automatically recorded on the blockchain, ensuring complete traceability and accountability, while patients are notified once the emergency session is completed.

Instead of storing complete Electronic Health Records on the blockchain, encrypted healthcare records are securely maintained in **off-chain storage** such as cloud or IPFS repositories. Before storing an Electronic Health Record, a **SHA-256 cryptographic hash** is generated and permanently recorded on the blockchain. During every record retrieval, the integrity verification module recalculates the SHA-256 hash and compares it with the blockchain record to detect unauthorized modifications or data tampering.

Finally, the **AI-Assisted Threat Detection** layer continuously monitors blockchain transactions, authentication logs, user behavior, access frequency, and IoMT device activities. The AI engine analyzes abnormal access patterns to identify insider attacks, credential theft, replay attacks, and suspicious healthcare activities. Upon detecting malicious behavior, the framework immediately generates security alerts, temporarily suspends compromised identities, and notifies hospital administrators for further investigation.

By integrating blockchain, decentralized identity, intelligent authorization, patient-centric consent management, emergency healthcare support, cryptographic integrity verification, and AI-assisted threat detection, **MediChainGuard** provides a secure, scalable, transparent, and trustworthy healthcare security architecture for next-generation Internet of Medical Things (IoMT) environments.

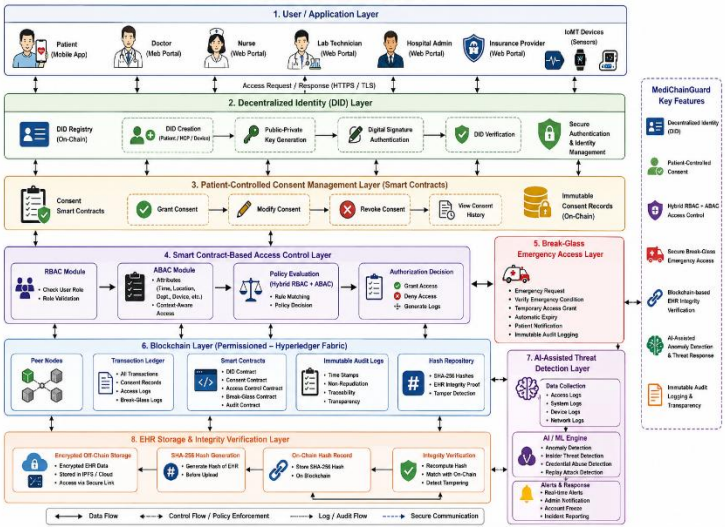

Fig. 1. System Architecture

4.2 Blockchain-Based Access Control Framework

The proposed **MediChainGuard** framework introduces a decentralized blockchain-based access control system that securely manages interactions among patients, healthcare professionals, Internet of Medical Things (IoMT) devices, hospitals, laboratories, insurance providers, and Electronic Health Record (EHR) repositories. Unlike conventional healthcare systems that rely on centralized authentication servers, the proposed framework employs a **permissioned blockchain** to authenticate users, enforce access policies, and maintain immutable audit records. Every participating entity—including patients, doctors, nurses, laboratory technicians, hospital administrators, insurance providers, and IoMT devices—is assigned a unique **Decentralized Identity (DID)** and corresponding cryptographic credentials for secure authentication and authorization.

The proposed framework operates over a **Hyperledger Fabric** permissioned blockchain, where only authorized healthcare organizations participate in transaction validation and smart contract execution. This permissioned architecture provides high security, low transaction latency, and controlled data sharing among trusted healthcare stakeholders while preventing unauthorized participation. All authentication requests, consent transactions, authorization decisions, and emergency access events are permanently recorded on the blockchain, providing transparency, accountability, and tamper-resistant audit trails.

The blockchain-enabled access control framework adopts a multi-level authorization strategy consisting of the following security layers:

- **Level 1 – Decentralized Identity Authentication (DID):** Every patient, healthcare professional, and IoMT device is registered with a unique Decentralized Identity (DID). Public-private key cryptography and digital signatures are employed to verify identities before any healthcare resource is accessed.
- **Level 2 - Patient-Controlled Consent Management:** Patients retain complete control over their Electronic Health Records by granting, modifying, or revoking access permissions through blockchain-enabled smart contracts. Every consent operation is securely recorded on the distributed ledger.

- **Level 3 – Hybrid RBAC-ABAC Authorization:** After successful authentication, the smart contract evaluates access requests using a hybrid **Role-Based Access Control (RBAC)** and **Attribute-Based Access Control (ABAC)** model. RBAC verifies predefined healthcare roles such as doctor, nurse, laboratory technician, or insurance provider, while ABAC evaluates contextual attributes including department, consultation schedule, hospital location, patient consent status, emergency condition, and device trust level.

RBAC ensures that healthcare professionals, including doctors, nurses, laboratory technicians, hospital administrators, and insurance providers, operate within predefined privileges. ABAC further evaluates contextual parameters such as department, consultation schedule, hospital location, patient consent status, emergency conditions, and device trust level before making the final authorization decision. This hybrid authorization mechanism improves flexibility, security, and privacy while supporting dynamic access control in IoMT-enabled healthcare environments.

- **Level 4 – Break-Glass Emergency Access:** During emergency medical situations where patients are unable to provide consent, authorized emergency physicians may request temporary access to Electronic Health Records. The smart contract validates predefined emergency policies before granting time-limited authorization. Every emergency access request is immutably recorded on the blockchain to ensure accountability.

To preserve patient privacy and reduce blockchain storage overhead, complete Electronic Health Records are stored in encrypted **off-chain repositories**, while only the corresponding **SHA-256 cryptographic hash**, metadata, and access logs are maintained on the blockchain. During every retrieval operation, the stored hash value is compared with the newly computed hash to verify data integrity and detect unauthorized modifications.

By combining decentralized identity management, patient-centric consent management, blockchain-enabled smart contracts, hybrid RBAC-ABAC authorization, emergency access control, cryptographic integrity verification, and AI-assisted threat detection, the proposed framework provides a secure, scalable, transparent, and trustworthy access control solution for next-generation Internet of Medical Things (IoMT) healthcare environments.

After describing the overall system architecture, Fig. 2 presents the operational workflow of the proposed blockchain-based access control mechanism. The workflow illustrates how access requests are authenticated, authorized, recorded on the blockchain, and monitored for potential security threats.

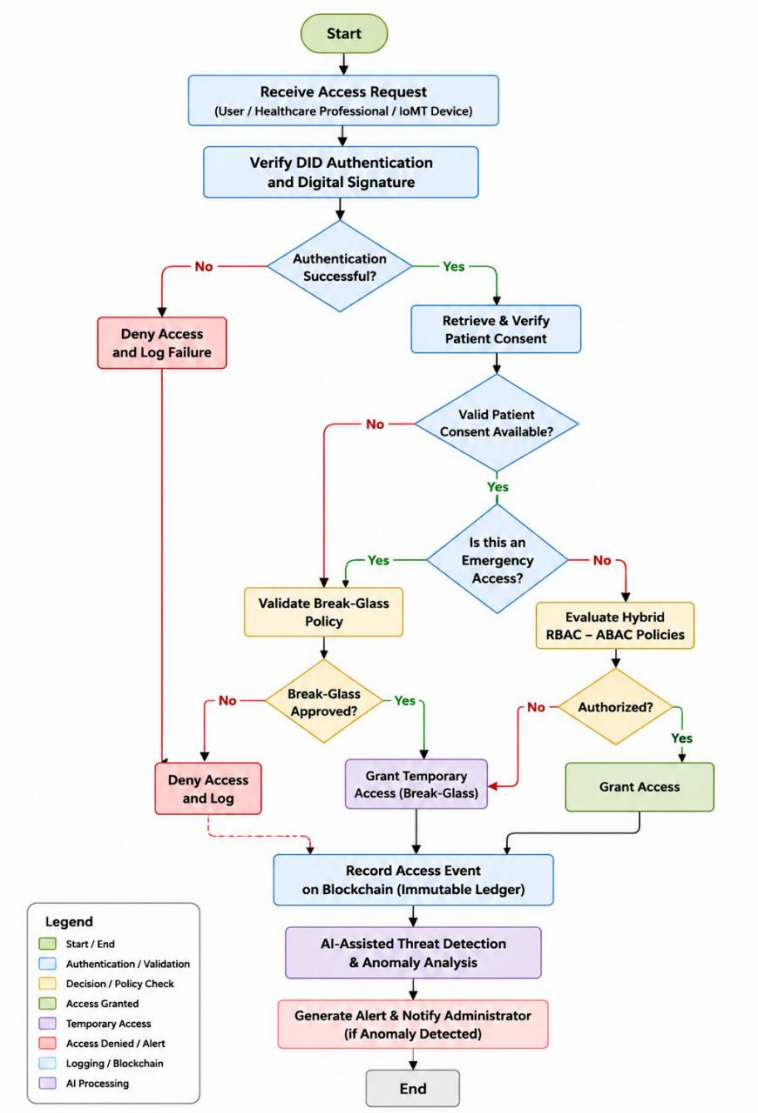

Fig. 2. Blockchain-Based Access Control Workflow of the Proposed MediChainGuard Framework

Initially, every access request undergoes Decentralized Identity (DID)-based authentication and digital signature verification. Upon successful authentication, the system validates patient consent and determines whether the request corresponds to a normal or emergency scenario. Emergency requests are processed through the Break-Glass policy, whereas regular requests are authorized using the hybrid RBAC–ABAC mechanism. The final authorization decision is recorded on the blockchain to ensure transparency, accountability, and immutable auditability. Subsequently, the AI-assisted threat detection module analyzes access events to identify suspicious activities and generate security alerts whenever anomalous behavior is detected.

```
FUNCTION Access_Control_Request(
        patient_ID, requester_ID, resource_ID,
        request_Type, requested_Action, context_Data
):
    // Step 1: Verify DID Authentication
    IF NOT Verify_Digital_Signature(requester_ID) THEN
        Record_On_Blockchain("INVALID_SIGNATURE")
        RETURN "DENY"
    END IF
    // Step 2: Retrieve Consent Information
    consent_Record ← Get_Consent_Record(patient_ID)
    IF consent_Record == NULL THEN
        Record_On_Blockchain("CONSENT_NOT_AVAILABLE")
        RETURN "DENY"
    END IF
    // Step 3: Validate Consent Status
    IF consent_Record.status == "REVOKED" THEN
        Record_On_Blockchain("CONSENT_REVOKED")
        RETURN "DENY"
    END IF
    IF Consent_Expired(consent_Record) THEN
        Record_On_Blockchain("CONSENT_EXPIRED")
        RETURN "DENY"
    END IF
    // Step 4: Emergency Access Handling
    IF request_Type == "EMERGENCY" THEN
        IF Validate_BreakGlass_Policy (requester_ID, patient_ID, resource_ID) THEN
            Grant_Temporary_Access()
            Record_On_Blockchain("BREAK_GLASS_GRANTED")
            RETURN "TEMPORARY_ACCESS"
        ELSE
            Record_On_Blockchain("BREAK_GLASS_DENIED")
            RETURN "DENY"
        END IF
    END IF
    // Step 5: Hybrid Authorization
    user_Role ← Get_Requester_Role(requester_ID)
    IF NOT RBAC_Authorization(user_Role, requested_Action) THEN
        Record_On_Blockchain("RBAC_FAILED")
        RETURN "DENY"
    END IF
    IF NOT ABAC_Authorization(context_Data, consent_Record) THEN
        Record_On_Blockchain("ABAC_FAILED")
        RETURN "DENY"
    END IF
    // Step 6: Grant Access
    Grant_Access(requester_ID, resource_ID, requested_Action)
    Record_On_Blockchain("ACCESS_GRANTED")
    // Step 7: Audit Logging
    Update_Audit_Log(requester_ID, patient_ID, resource_ID, requested_Action)
    // Step 8: AI Security Monitoring
    Analyze_Access_Pattern(requester_ID, patient_ID, context_Data)
    IF Threat_Detected() THEN
        Generate_Security_Alert()
    END IF
    Notify_Stakeholders()
    RETURN "ACCESS_GRANTED"
END FUNCTION
```

Fig. 3. Pseudocode for the Proposed Smart Contract-Based Access Control Algorithm.

The algorithm authenticates the requester using DID-based digital signatures, validates patient consent, processes emergency requests through the Break-Glass policy, and evaluates hybrid RBAC–ABAC authorization rules. Every authorization decision is securely recorded on the blockchain to ensure transparency and auditability, while the AI-assisted threat detection module analyzes access events to identify suspicious activities before returning the final access decision.

4.3 Decentralized Identity (DID) Registration and Authentication

The Decentralized Identity (DID) mechanism serves as the foundation of the proposed MediChainGuard framework by providing secure, decentralized, and privacy-preserving identity management for patients, healthcare professionals, and Internet of Medical Things (IoMT) devices. Unlike conventional healthcare systems that depend on centralized identity providers, the proposed approach adopts W3C-compliant DID architecture to eliminate dependence on trusted third parties while improving authentication security and resistance against identity-based attacks.

1. Registration Workflow

Before accessing any healthcare resource, every patient, healthcare professional, and IoMT device must complete a registration process through the DID management module. During registration, the participant submits identity information such as demographic details, professional credentials, or device metadata depending on the entity

type. The registration smart contract verifies the submitted information through authorized healthcare organizations and generates a unique DID that serves as the participant's blockchain identity.

The generated DID is permanently associated with the participant and is recorded on the permissioned Hyperledger Fabric blockchain. This decentralized registration mechanism prevents unauthorized identity creation and ensures that only verified entities can participate in healthcare transactions.

2. DID Document Creation

Following successful registration, a DID Document is generated and stored on the blockchain. The DID Document contains essential identity information, including:

- ✓ DID identifier
- ✓ Public cryptographic key
- ✓ Verification methods
- ✓ Service endpoints
- ✓ Credential metadata
- ✓ Revocation status

The DID Document enables secure identity verification without exposing sensitive personal information. Since the document is recorded on the blockchain, unauthorized modification becomes computationally infeasible.

3. Key Pair Generation and Digital Signature

To secure healthcare communications and authentication processes, the framework employs the Elliptic Curve Digital Signature Algorithm (ECDSA) using the secp256r1 elliptic curve.

For each registered entity:

- ✓ A private key is securely stored by the owner.
- ✓ A corresponding public key is recorded within the DID Document.

The private key is used to digitally sign authentication requests, while the public key is utilized by blockchain validators and smart contracts to verify signatures. ECDSA provides strong cryptographic security with lower computational overhead, making it suitable for resource-constrained IoMT devices.

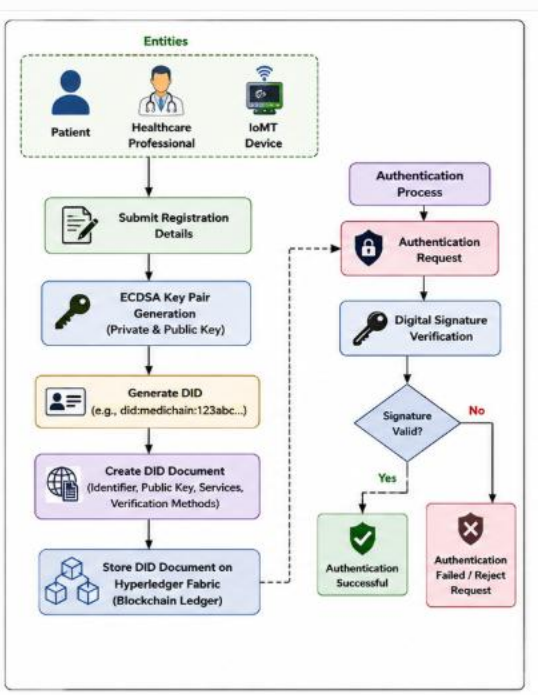

Fig. 4. DID Registration and Authentication Workflow

Fig. 4 illustrates the complete DID registration and authentication workflow of the proposed MediChainGuard framework. Initially, patients, healthcare professionals, and IoMT devices submit their registration information to the registration authority. An ECC-based public–private key pair is generated, followed by the creation of a unique DID and DID document. The DID document is securely stored on the permissioned blockchain. During authentication, the requester submits a digitally signed access request, and the system verifies the signature using the public key stored in the DID document. Upon successful verification, the requester is authenticated, and the authentication event is recorded on the blockchain to ensure transparency, integrity, and auditability.

4. Authentication Process

Whenever a patient, doctor, nurse, administrator, or IoMT device attempts to access healthcare resources, the DID authentication workflow is executed.

Initially, the requester generates a digital signature using its private key and submits an authentication request. The authentication smart contract retrieves the associated DID Document from the blockchain and verifies the digital signature using the stored public key.

If the signature verification process succeeds:

- ✓ The requester is considered authenticated.
- ✓ The authorization module is activated.
- ✓ Access control evaluation begins.

Otherwise, the request is immediately rejected and recorded on the blockchain audit log.

The complete DID registration and authentication workflow is illustrated in the authentication workflow diagram shown in Fig. 4.

$$Auth(U) = Verify(sign(Req, PrivKey), PubKey)$$

Where Req represents the authentication request, PrivKey denotes the requester's private key, and PubKey represents the corresponding public key stored in the DID document.

5. Identity Update and Revocation

Healthcare identities may require updates due to role changes, credential expiration, employment transfer, lost devices, or compromise of cryptographic keys.

The proposed framework supports secure DID lifecycle management through blockchain-enabled smart contracts. Authorized entities can update DID metadata, rotate cryptographic keys, or revoke compromised identities. Revocation transactions are immediately recorded on the blockchain and reflected in the corresponding DID Document.

Subsequent authentication attempts involving revoked identities are automatically denied, preventing unauthorized healthcare access.

4.4 Patient-Controlled Consent Management

Patient privacy and data ownership are fundamental principles of the proposed MediChainGuard framework. To ensure patient-centric healthcare data sharing, blockchain-enabled smart contracts allow patients to retain complete control over their Electronic Health Records (EHRs).

1. Consent Granting

When a healthcare provider requests access to a patient's EHR, the consent management smart contract notifies the patient. The patient may specify:

- ✓ Authorized healthcare professional
- ✓ Accessible medical records
- ✓ Type of permitted operation
- ✓ Access duration
- ✓ Purpose of access

After confirmation, the consent smart contract records the approval on the blockchain.

2. Consent Modification

Healthcare requirements often evolve over time. Therefore, patients may modify previously granted permissions.

Patients can update:

- ✓ Access duration
- ✓ Accessible record categories
- ✓ Authorized healthcare personnel
- ✓ Scope of medical data sharing

The modified consent record replaces the previous version through a smart contract update transaction

3. Consent Revocation

Patients maintain the right to revoke previously granted permissions at any time. Upon revocation, the smart contract immediately invalidates associated authorization tokens and updates the access policy.

Any subsequent access request from the revoked entity is automatically rejected.

4. **Consent Expiry**

To prevent indefinite access privileges, each consent agreement includes an expiration timestamp. Once the validity period expires, the smart contract automatically invalidates the consent record without requiring manual intervention.

5. **Smart Contract Updates**

Every consent operation including:

- ✓ Consent creation
- ✓ Consent modification
- ✓ Consent renewal
- ✓ Consent revocation
- ✓ Expiration handling

Is executed through blockchain smart contracts.

These contracts enforce patient-defined access policies consistently across healthcare organizations.

6. **Blockchain Audit Logging**

All consent-related activities are immutably recorded on the blockchain. The audit trail includes:

- ✓ Patient identifier
- ✓ Requesting healthcare provider
- ✓ Timestamp
- ✓ Consent operation type
- ✓ Expiration handling

This immutable log improves transparency, accountability, and regulatory compliance.

4.5 Smart Contract-Based Hybrid RBAC-ABAC Authorization

After successful authentication and consent verification, the proposed framework executes a hybrid authorization model that combines Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).

1. **Role Verification**

The RBAC component validates whether the requester possesses an authorized healthcare role such as:

- ✓ Physician
- ✓ Nurse
- ✓ Laboratory Technician
- ✓ Hospital Administrator
- ✓ Insurance Provider

Each role is associated with predefined privileges stored within blockchain smart contracts.

2. Attribute Evaluation

Following role validation, the ABAC engine evaluates contextual attributes including:

- ✓ Department affiliation
- ✓ Hospital location
- ✓ Consultation schedule
- ✓ Emergency status
- ✓ Device trust score
- ✓ Patient consent status
- ✓ Time of access

These attributes provide context-aware authorization decisions.

3. Policy Execution

The authorization smart contract compares requester attributes against predefined healthcare access policies.

Access is granted only when both:

- ✓ RBAC role conditions are satisfied
- ✓ ABAC contextual conditions are fulfilled

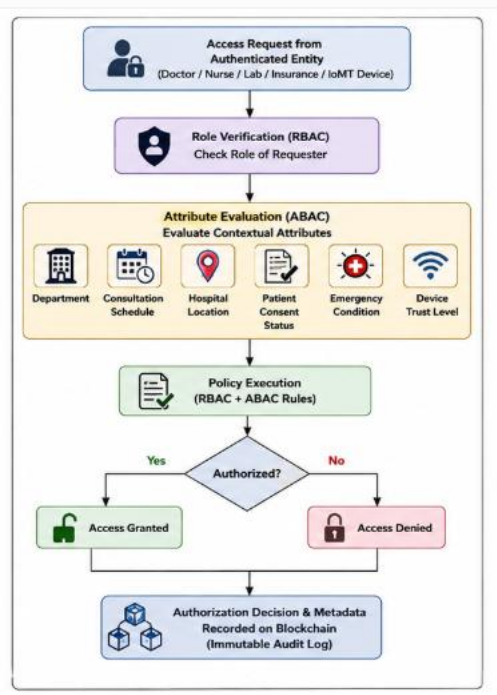

Fig. 5. Hybrid RBAC–ABAC Authorization Workflow

Fig. 5 illustrates the hybrid RBAC–ABAC authorization workflow of the proposed MediChainGuard framework. Following successful DID-based authentication, the smart contract first verifies the requester's predefined

healthcare role using the RBAC mechanism. Subsequently, the ABAC module evaluates contextual attributes, including department, consultation schedule, hospital location, patient consent status, emergency condition, and device trust level. Based on the combined policy evaluation, the framework grants or denies access to Electronic Health Records (EHRs). Every authorization decision, along with its associated metadata, is permanently recorded on the Hyperledger Fabric blockchain to ensure transparency, accountability, and immutable auditability.

The hybrid RBAC–ABAC authorization mechanism combines static role verification with dynamic contextual attribute evaluation to provide secure, flexible, and fine-grained healthcare access control while ensuring regulatory compliance and patient privacy.

4. Authorization Decision

Upon completion of policy evaluation, the smart contract generates one of two outcomes:

- ✓ Access Granted
- ✓ Access Denied

The decision is automatically enforced without human intervention, reducing administrative overhead and security risks.

5. Blockchain Logging

Every authorization transaction is permanently recorded on the blockchain, including:

- ✓ Requester DID
- ✓ Requested resource
- ✓ Access decision
- ✓ Timestamp
- ✓ Evaluated attributes

The immutable audit trail ensures accountability and forensic traceability.

4.6 Break-Glass Emergency Access

In emergency medical situations, patients may be unconscious or incapable of granting consent. To ensure continuity of care, the framework provides a secure Break-Glass Emergency Access mechanism.

1. **Emergency Access Request**

An emergency physician initiates a special access request through the emergency access module when immediate treatment is required.

The request includes:

- ✓ Emergency justification
- ✓ Patient identifier
- ✓ Requested medical resources
- ✓ Healthcare facility details

2. **Emergency Policy Validation**

The Break-Glass smart contract evaluates predefined emergency conditions such as:

- ✓ Life-threatening situations
- ✓ Critical care requirements
- ✓ Absence of patient consent
- ✓ Authorized emergency physician status

The request proceeds only if all emergency conditions are satisfied.

3. **Temporary Authorization**

Once validated, the smart contract grants temporary access permissions for a limited duration.

The authorization remains active only during the emergency period and is automatically revoked afterward.

4. **Automatic Audit Logging**

All emergency access activities are automatically recorded on the blockchain, including:

- ✓ Physician identity
- ✓ Patient identity
- ✓ Access start time
- ✓ Access end time
- ✓ Accessed records
- ✓ Emergency reason

This mechanism prevents misuse of emergency privileges.

5. **Patient Notification**

After the emergency event concludes, the framework automatically informs the patient about:

- ✓ Who accessed the records
- ✓ What information was accessed
- ✓ Why emergency access was granted
- ✓ Duration of access

This ensures transparency and protects patient rights.

4.7 Blockchain-Based EHR Integrity Verification

To preserve Electronic Health Record integrity while minimizing blockchain storage overhead, the MediChainGuard framework employs blockchain-based hash verification combined with encrypted off-chain storage.

1. **Off-Chain Encrypted Storage**

Complete Electronic Health Records are encrypted using strong cryptographic algorithms and stored in secure off-chain repositories such as:

- ✓ Cloud Storage
- ✓ InterPlanetary File System (IPFS)

This approach reduces blockchain storage requirements while preserving confidentiality.

2. **SHA-256 Hash Generation**

Before storage, a SHA-256 cryptographic hash is generated for every EHR.

$$HashEHR = SHA256(EHRData)$$

Where EHRData denotes the electronic health record and HashEHR represents its corresponding blockchain integrity hash. The hash uniquely represents the content of the medical record.

3. **Blockchain Hash Storage**

The generated hash, together with metadata and storage references, is recorded on the blockchain. Since blockchain entries are immutable, the stored hash becomes a trusted integrity reference.

4. **Integrity Verification During Retrieval**

Whenever a healthcare professional retrieves a medical record:

- ✓ The encrypted record is obtained from off-chain storage.
- ✓ A new SHA-256 hash is calculated.
- ✓ The newly generated hash is compared with the blockchain hash.

If both values match, data integrity is confirmed.

5. **Tamper Detection**

Any unauthorized modification to the EHR changes the resulting SHA-256 hash value.

- ✓ Data manipulation
- ✓ Unauthorized modification
- ✓ Storage corruption
- ✓ Insider attacks

The framework then blocks access and generates a security alert.

This integrity verification mechanism ensures that Electronic Health Records remain authentic, untampered, and trustworthy throughout their lifecycle while minimizing blockchain storage overhead.

4.8 AI-Assisted Threat Detection

The proposed framework integrates Artificial Intelligence (AI) to continuously monitor healthcare operations and identify potential cyber threats in real time. By analyzing authentication events, blockchain transactions, IoMT device activities, and user behavioral patterns, the AI module strengthens the overall security of the MediChainGuard framework and enables proactive threat detection.

1. **Authentication Log Monitoring**

The AI engine continuously monitors authentication events including:

- ✓ Successful logins
- ✓ Failed logins
- ✓ Repeated authentication attempts

- ✓ Credential usage patterns

These authentication logs are collected from blockchain records and healthcare information systems to establish a baseline of normal user behavior.

2. **Blockchain Transaction Analysis**

The AI module analyzes blockchain transactions to identify unusual authorization activities, excessive access requests, abnormal consent modifications, and suspicious blockchain interactions. Continuous monitoring of immutable blockchain records enables the early detection of malicious activities that may compromise healthcare data security.

3. **User Behavior Analysis**

Behavioral profiles are constructed for healthcare professionals, patients, and IoMT devices using historical activity patterns. The AI engine extracts several behavioral features, including:

- ✓ Access frequency
- ✓ Access timing
- ✓ Resource usage
- ✓ Geographic location patterns
- ✓ Device characteristics

These features enable the system to distinguish legitimate healthcare activities from abnormal or malicious behavior.

4. **Anomaly Detection**

Machine learning algorithms continuously analyze the extracted features to identify deviations from normal behavioral patterns.

AI Model Implementation: The proposed AI-assisted threat detection module utilizes an Isolation Forest algorithm for anomaly detection due to its effectiveness in identifying rare and abnormal behavioural patterns within large-scale IoMT environments. Authentication logs, blockchain transaction records, access frequencies, consent operations, failed login attempts, device trust scores, and temporal access characteristics are extracted as input features. Prior to model training, raw security logs are preprocessed through data cleaning, normalization, and feature engineering. The Isolation Forest model constructs multiple random decision trees and computes anomaly scores based on path lengths. Transactions exhibiting significantly shorter path lengths are classified as anomalous and treated as potential security threats. Events exceeding predefined risk thresholds trigger automated security responses, including alert generation, temporary account suspension, and administrator notification.

- ✓ Insider attacks
- ✓ Credential theft
- ✓ Replay attacks
- ✓ Privilege abuse
- ✓ Unauthorized access attempts

Activities exceeding predefined risk thresholds are classified as potential cyber threats requiring immediate security response.

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}}$$

where s(x,n) represents the anomaly score, E(h(x)) denotes the average path length of the observation, and c(n) is the normalization factor of the Isolation Forest model.

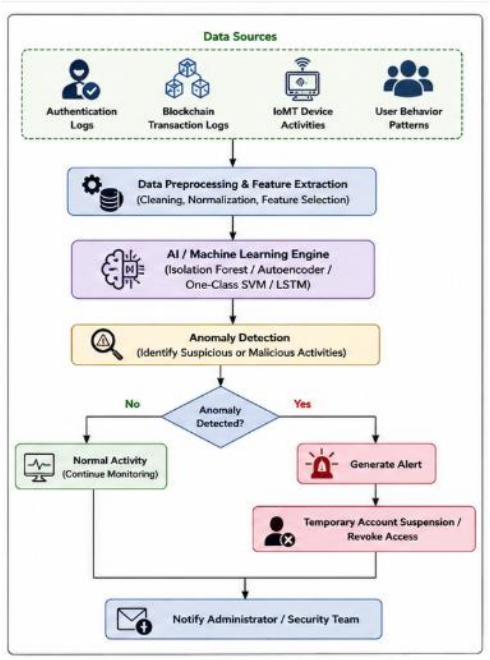

Fig. 6. AI-Assisted Threat Detection Workflow

Fig. 6 illustrates the AI-assisted threat detection workflow of the proposed MediChainGuard framework. Authentication logs, blockchain transaction records, IoMT device activities, and user behavioral data are continuously collected and preprocessed for feature extraction. The extracted features are analyzed using machine learning algorithms to identify abnormal access patterns and potential cyber threats. When suspicious activities are detected, the framework automatically generates security alerts, temporarily suspends compromised user accounts or revokes access permissions, and notifies hospital administrators for timely incident response and mitigation.

5. **Alert Generation**

When suspicious behavior is detected, the framework automatically generates real-time security alerts containing:

- ✓ Threat category
- ✓ Risk level
- ✓ Affected user
- ✓ Timestamp
- ✓ Recommended action

These alerts enable healthcare administrators to quickly assess the severity of the incident and initiate appropriate countermeasures.

6. **Temporary Account Suspension**

For high-risk incidents, the framework automatically performs temporary account suspension until further verification is completed. This mechanism prevents attackers from exploiting compromised credentials and minimizes the impact of unauthorized access on sensitive healthcare resources.

7. **Administrator Notification**

Security alerts are immediately transmitted to hospital cybersecurity administrators and Security Operation Centers (SOCs). Administrators can review:

- ✓ Anomaly details
- ✓ Access history
- ✓ Blockchain audit records
- ✓ Threat severity indicators

The availability of detailed forensic information enables rapid incident response, efficient investigation, and timely mitigation of cybersecurity threats, thereby improving the overall security and resilience of Internet of Medical Things (IoMT) healthcare environments.

4.9 Implementation Environment

The proposed MediChainGuard framework was implemented using Hyperledger Fabric v2.5 deployed on a permissioned blockchain network consisting of four peer nodes and one ordering service. Smart contracts were developed using Go chaincode and executed within Docker containers. Electronic Health Records (EHRs) were securely maintained in encrypted off-chain storage, while SHA-256 hash values and access logs were recorded on the blockchain ledger. The AI-assisted threat detection module was implemented using Python 3.11 and the Scikit-Learn machine learning library utilizing the Isolation Forest algorithm. Experimental evaluations were conducted on an Intel Core i7 processor with 16 GB RAM running Ubuntu Linux.

5. Results and performance evaluation

A. Experimental Setup

The proposed **MediChainGuard** framework was evaluated using a simulated IoMT healthcare environment consisting of patients, healthcare professionals, IoMT devices, blockchain nodes, and Electronic Health Record (EHR) repositories.

The experimental dataset contained authentication events, healthcare access requests, patient consent transactions, emergency access logs, EHR retrieval operations, and security incidents generated over six months of simulated healthcare activities.

Security Attack Simulation:

To evaluate the effectiveness of the AI-assisted threat detection module, multiple cyberattack scenarios were synthetically injected into the experimental environment. The simulated attacks included credential theft, replay attacks, unauthorized privilege escalation, abnormal access frequency, consent manipulation attempts, and insider misuse of Electronic Health Records. Approximately 15% of the generated transactions were labelled as malicious activities. These attack samples were distributed throughout the observation period to emulate realistic cybersecurity incidents and evaluate the robustness of the proposed anomaly detection framework under dynamic operating conditions.

6. Table I Dataset Description

Parameter	Value
Registered Patients	15,000
Healthcare Professionals	4,000
IoMT Devices	25,000
Authentication Logs	2 million
Consent Transactions	500,000
EHR Records	300,000
Observation Period	6 months

B. Performance Metrics

The proposed MediChainGuard framework was evaluated using the following metrics:

- Authentication Time
- Authorization Accuracy
- Consent Processing Time
- Break-Glass Response Time
- EHR Integrity Verification Accuracy
- AI Threat Detection Accuracy
- False Positive Rate
- Blockchain Transaction Throughput

Authentication delay represents the average time required to complete DID-based identity verification and authorization.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100$$

where TP and TN denote correctly classified authorization decisions, while FP and FN denote incorrect decisions.

C. DID Authentication Performance

The DID authentication module was evaluated against conventional centralized identity management systems.

The proposed DID-based authentication achieved lower response times because identity verification is performed using blockchain-based public-key cryptography and decentralized validation.

Table II DID Authentication Performance

Method	Authentication Time (ms)
Centralized IAM	520
OAuth-Based Authentication	390
Blockchain Authentication	280
Proposed DID Authentication	170

The results demonstrate that the proposed framework reduces authentication delay while eliminating dependence on centralized identity providers.

D. Patient Consent Management Performance

The consent management smart contract was tested for consent creation, modification, and revocation operations.

Table III Patient Consent Management Performance

Method Operation	**Average Processing Time (ms)**
Consent Grant	110
Consent Modify	125
Consent Revoke	95
Consent Expiry Update	80

Blockchain-supported consent management enables real-time enforcement of patient decisions while preserving transparency and auditability.

E. Hybrid RBAC-ABAC Authorization Analysis

The authorization module was tested using role-based and context-aware access requests.

Table IV Authorization Accuracy

Authorization Model	**Accuracy(%)**
RBAC	94.1
ABAC	96.2
Blockchain RBAC	97.1
Proposed Hybrid RBAC-ABAC	99.1

The hybrid authorization mechanism achieved superior access control accuracy because both role privileges and contextual attributes are jointly evaluated before granting access.

F. Break-Glass Emergency Access Evaluation

Emergency healthcare scenarios were simulated to evaluate the responsiveness of the proposed Break-Glass mechanism.

Table V Emergency Access Performance

Metric	**Value**
Emergency Requests Processed	12,000
Average Authorization Time	145 ms
Audit Logging Accuracy	100%
Post-Emergency Notification Rate	100%

The proposed framework successfully granted temporary emergency access while maintaining complete auditability of every emergency event.

G. EHR Integrity Verification Results

The blockchain integrity module was evaluated using intentionally modified Electronic Health Records.

Table VI EHR integrity validation

Metric	Value
Total EHR Records Tested	300,000
Integrity Verification Accuracy	99.8%
Tampered Records Detected	100%
SHA-256 Validation Success Rate	99.9%

The results demonstrate that blockchain-stored SHA-256 hashes effectively detect unauthorized modifications and preserve EHR integrity.

H. AI-Assisted Threat Detection Evaluation

The AI security engine was evaluated using multiple attack scenarios including:

- ✓ Credential Theft
- ✓ Insider Abuse
- ✓ Unauthorized Privilege Escalation
- ✓ Replay Attacks
- ✓ Abnormal Access Frequency

Table VII AI Threat Detection Performance

Metric	Value
Detection Accuracy	98.3%
Precision	97.9%
Recall	98.1%
F1-Score	98.0%
False Positive Rate	2.4%

Table VIII Comparison of Threat Detection Models

Method	Detection Accuracy(%)	False Positive Rate (%)
One-Class SVM	94.5	5.8
Autoencoder	96.1	4.2
LSTM	97.2	3.5
Proposed Isolation Forest	98.3	2.4

The proposed Isolation Forest-based anomaly detection model achieved the highest detection accuracy and the lowest false positive rate among the evaluated machine learning approaches, demonstrating its suitability for real-time healthcare security monitoring.

I. Comparative Analysis

Table IX Comparison with Existing Method

Metric	Kumar et al. [3]	Fabric-IoT [1]	N-Accesses [4]	Proposed MediChain Guard	

Authentication Time (ms)	480	380	260	170	
Authorization Accuracy (%)	93.0	95.5	97.0	99.1	
Emergency Access Support	No	No	No	Yes	
Patient Consent Control	Partial	No	No	Yes	
EHR Integrity Verification	No	Partial	No	Yes	
AI-Threat Detection	No	No	No	Yes	
Security Level	High	High	High	Very High	

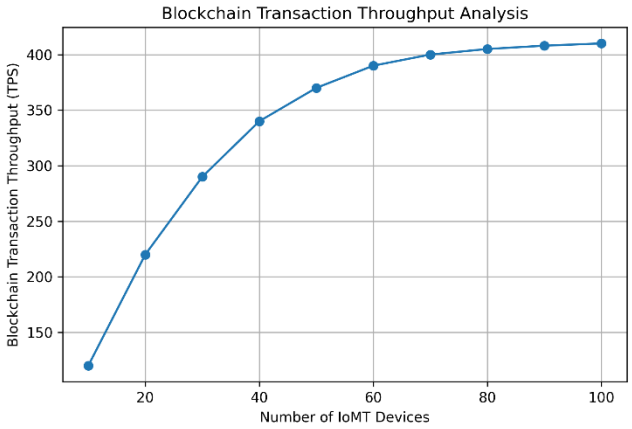

Fig. 7. Blockchain Transaction Throughput Analysis of the

Proposed MediChainGuard Framework.

Fig. 7 illustrates the blockchain transaction throughput of the proposed MediChainGuard framework under varying numbers of IoMT devices. As the number of connected IoMT devices increases, the transaction throughput improves steadily due to the efficient execution of smart contracts and the permissioned Hyperledger Fabric architecture. The throughput gradually stabilizes at approximately 410 transactions per second (TPS), demonstrating that the proposed framework efficiently supports large-scale healthcare environments while maintaining high transaction processing capability, scalability, and low communication overhead.

J. Discussion

The experimental results indicate that MediChainGuard significantly improves healthcare access security compared with existing blockchain-enabled healthcare frameworks. DID-based authentication reduces authentication latency, while hybrid RBAC-ABAC authorization provides highly accurate and context-aware access decisions. Patient-controlled consent management ensures privacy preservation and regulatory compliance. The Break-Glass module facilitates emergency healthcare delivery without compromising accountability. Furthermore, blockchain-based SHA-256 verification effectively detects EHR tampering, and the AI-assisted threat detection module provides

real-time protection against insider threats and credential misuse. Overall, the proposed framework demonstrates strong security, scalability, transparency, and operational efficiency for next-generation IoMT environments.

The superior performance of the proposed framework is primarily attributed to decentralized identity verification, permissioned blockchain consensus, and context-aware authorization mechanisms. DID-based authentication eliminates dependence on centralized identity providers and reduces authentication latency through distributed credential verification. The Hyperledger Fabric architecture enables higher transaction throughput and lower computational overhead compared with public blockchain infrastructures. Furthermore, the hybrid RBAC–ABAC authorization model improves access control accuracy by jointly evaluating role privileges and contextual attributes before granting access permissions. The Isolation Forest-based anomaly detection model effectively identifies abnormal behavioural patterns while maintaining a low false-positive rate, making it suitable for real-time IoMT security monitoring. These results demonstrate that integrating blockchain, decentralized identity management, and machine learning can simultaneously improve security, transparency, scalability, and trust in next-generation IoMT environments.

K. Limitations

Although the proposed MediChainGuard framework demonstrates promising security and performance improvements, the evaluation was conducted within a simulated IoMT healthcare environment. Real-world healthcare deployments may introduce additional operational constraints such as network variability, heterogeneous IoMT devices, and large-scale inter-organizational data sharing challenges. Furthermore, the AI-assisted threat detection module was evaluated using synthetically generated attack scenarios rather than real production healthcare security datasets. Future validation using real-world healthcare environments and publicly available cybersecurity datasets may further strengthen the effectiveness and generalizability of the proposed framework.

6. Conclusion

This paper presented **MediChainGuard**, a decentralized blockchain-based access control framework for securing Internet of Medical Things (IoMT) environments. The proposed framework integrates Decentralized Identity (DID), patient-controlled consent management, smart contract-driven hybrid RBAC–ABAC authorization, Break-Glass emergency access, blockchain-based Electronic Health Record (EHR) integrity verification, and AI-assisted threat detection into a unified healthcare security architecture. By eliminating dependence on centralized authentication systems, the framework enhances privacy, transparency, accountability, and resilience against cyberattacks while preserving secure access to sensitive healthcare information.

The DID module enables secure identity verification for patients, healthcare professionals, and IoMT devices, whereas the patient-controlled consent mechanism ensures that users maintain full authority over data-sharing decisions. The hybrid RBAC–ABAC model provides fine-grained and context-aware authorization, while the Break-Glass access mechanism supports emergency situations without compromising auditability. Furthermore, blockchain-enabled SHA-256 integrity verification protects Electronic Health Records from unauthorized modifications, and the AI-assisted threat detection module strengthens system security through continuous monitoring of authentication events, user behavior, and blockchain transactions.

Overall, the proposed **MediChainGuard** framework provides a secure, scalable, transparent, and trustworthy solution for next-generation Internet of Things (IoT) ecosystems by integrating blockchain technology, decentralized identity management, hybrid access control mechanisms, patient-controlled consent management, cryptographic integrity verification, and AI-assisted threat detection. The proposed framework effectively enhances data security, privacy preservation, access transparency, and resilience against unauthorized access, data tampering, and emerging cyber threats in distributed environments.

As a future extension, the proposed framework can be enhanced by integrating Federated Learning (FL) with blockchain-enabled IoT environments to facilitate decentralized, privacy-preserving, and collaborative intelligence across distributed edge devices. Instead of transmitting sensitive data to centralized servers, Federated Learning

enables local model training while securely exchanging only encrypted model parameters through the blockchain network, thereby improving data privacy, scalability, communication efficiency, and trustworthiness. Furthermore, the integration of blockchain, Federated Learning, Explainable Artificial Intelligence (XAI), Zero-Trust security architectures, lightweight cryptographic protocols, and edge computing can enable the development of intelligent, adaptive, and autonomous security frameworks capable of defending large-scale IoT infrastructures against sophisticated cyberattacks and evolving threat landscapes across diverse application domains.

REFERENCES

1. H. Liu, D. Han, and D. Li, "Fabric-IoT: A Blockchain-Based Access Control System in IoT," IEEE Access, vol. 8, pp. 18207–18218, 2020.
2. S. Sun, R. Du, S. Chen, and W. Li, "Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain," IEEE Access, vol. 9, pp. 36868–36878, 2021.
3. R. Kumar and R. Tripathi, "Scalable and Secure Access Control Policy for Healthcare System Using Blockchain," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 2321–2338, 2021.
4. T. Hu et al., "N-Accesses: A Blockchain-Based Access Control Framework for Secure IoT Data Management," Sensors, vol. 23, 8535, 2023.
5. R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. N. Islam, and M. Shorfuzzaman, "Permissioned Blockchain for Secure and Efficient Data Sharing," IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8065–8073, 2022.
6. A. Kayes et al., "A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues," Sensors, vol. 20, no. 9, 2020.
7. *B. Chai, B. Yan, J. Yu, and G. Wang, "BHE-AC: A Blockchain-Based High-Efficiency Access Control Framework for Internet of Things," Personal and Ubiquitous Computing, vol. 26, pp. 971–982, 2022.*
8. *D. Abdelfattah, H. A. Hassan, and F. A. Omara, "Enhancing Highly Collaborative Access Control System Using a New Role-Mapping Algorithm," International Journal of Electrical and Computer Engineering, vol. 12, no. 3, pp. 2765–2775, 2022.*
9. *Y. Riabi, H. Dhif, H. K. Ben Ayed, and K. Zaatouri, "A Blockchain-Based Access Control for IoT," in Proc. IEEE IWCMC, 2019, pp. 2086–2091.*
10. *Q. Lyu, Y. Qi, X. Zhang, H. Liu, Q. Wang, and N. Zheng, "SBAC: A Secure Blockchain-Based Access Control Framework for Information-Centric Networking," Journal of Network and Computer Applications, vol. 149, 102444, 2020.*
11. *G. Messinis, P. Papadopoulos, and P. Sarigiannidis, "Enhancing Internet of Medical Things Security with Artificial Intelligence: A Comprehensive Review," Computer Methods and Programs in Biomedicine, 2024.*
12. *M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," Symmetry, vol. 10, no. 10, Art. 470, 2018.*
13. *M. Alshehri, "Blockchain-Assisted Cyber Security in Medical Things Using Artificial Intelligence," Electronic Research Archive, vol. 31, no. 2, pp. 708–728, 2023.*
14. *P. Tagde et al., "Blockchain and Artificial Intelligence Technology in e-Health," Environmental Science and Pollution Research, 2021.*
15. *H. Taherdoost, "Blockchain-Based Internet of Medical Things: A Systematic Review," Applied Sciences, vol. 13, no. 3, Art. 1287, 2023.*
16. *X. Zheng, Z. Cai, Y. Li, and H. Gao, "Blockchain Challenges and Opportunities: A Survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.*
17. *S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.*
18. *Ramesh Mailapalli and A. C. Santha Sheela, "A Decentralized Blockchain Framework for Access Management in Precision Agriculture IoT," Proceedings of the International Conference on Signal, Systems, and Computing for Next-Gen Automation (ICSSCNA 2026), IEEE, 2026.*
19. *E. Androulaki, A. Barger, V. Bortnikov, et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proc. 13th EuroSys Conf., 2018, pp. 1–15.*
20. *M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," Symmetry, vol. 10, no. 10, Art. no. 470, 2018.*
21. *A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data," in Proc. IEEE Int. Conf. Internet of Things (iThings), 2019, pp. 534–543.*
22. *Q. Zhang, Y. Lin, S. Liu, K. Chen, and X. Xu, "Blockchain-Based Secure Data Sharing System for Healthcare Applications," IEEE Access, vol. 9, pp. 118966–118978, 2021.*
23. *B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Aguera y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proc. AISTATS, 2017, pp. 1273–1282.*
24. *Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," ACM Trans. Intell. Syst. Technol., vol. 10, no. 2, pp. 1–19, 2019.*
25. *M. M. Islam, A. Rahaman, and M. R. Islam, "Development of Smart Healthcare Monitoring System in IoT Environment," SN Computer Science, vol. 1, no. 3, pp. 1–11, 2020.*
26. *Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.*

27. *I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.*
28. *V. C. Hu, D. Ferraiolo, and D. Kuhn, Guide to Attribute-Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162, 2014.*
29. *R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," IEEE Computer, vol. 29, no. 2, pp. 38–47, 1996.*
30. *World Wide Web Consortium (W3C), "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, Jul. 2022.*
31. *S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.*
32. *G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Yellow Paper, 2014.*
33. *National Institute of Standards and Technology (NIST), Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, 2020.*
34. *M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Blockchain Technology," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 3416–3452, 2020.*
35. *M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-Preserving Schemes," Journal of Network and Computer Applications, vol. 101, pp. 55–82, 2018.*