A Privacy-Preserving Consumer-Centric IoMT Framework Using TEE-Enabled Federated Learning, CP-ABE, and Blockchain

Farooq Ahmed, Teng Zhou, Jabar Mahmood, *Member, IEEE*, Bander A. Alzahrani, and Shehzad Ashraf Chaudhry, *Senior Member, IEEE*

***Abstract*—The rapid expansion of the Internet of Medical Things (IoMT) has transformed healthcare delivery by enabling real-time monitoring, advanced diagnostics, and efficient data sharing. However, current systems in large-scale, decentralized environments face significant challenges in privacy, security, trust, and interoperability. This paper presents a Federated Learning framework for a consumer-centric IoMT system that provides secure, resilient data exchange against AI-enabled attacks through privacy-preserving learning, decentralized authentication, and hardware-based trust. It integrates trusted execution environments (TEEs), blockchain-based trust management, and ciphertext-policy attribute-based encryption (CP-ABE) to enable secure collaboration without exposing raw data. We provide a security proof in the Real-or-Random (RoR) model and conduct a comprehensive performance analysis covering computation, communication, storage, smart contract processing, and throughput. Experimental results show a 40% reduction in authentication latency, a 27% decrease in computational overhead, a 98% drop in energy use, and a 35% increase in throughput compared to existing schemes. These findings demonstrate that the proposed framework offers high scalability, robust security, and privacy protection, making it ideal for the next-generation healthcare ecosystem.**

***Index Terms*—Security, healthcare, Internet of Medical Things, blockchain, federated learning, smart contract.**

Received 26 October 2025; revised 24 December 2025 and 19 January 2026; accepted 2 February 2026. Date of publication 6 February 2026; date of current version 2 June 2026. This work was supported in part by the National Natural Science Foundation of China under Grant 62462021, in part by the Philosophy and Social Sciences Planning Project of Zhejiang Province under Grant 25JCXK006YB, in part by Hainan Provincial Natural Science Foundation of China under Grant 625RC716, in part by Guangdong Basic and Applied Basic Research Foundation under Grant 2025A1515010197, in part by Guangxi Natural Science Foundation under Grant 2025JJA170089, and in part by Hainan Province Higher Education Teaching Reform Project under Grant HNJG2024ZD-16. *(Corresponding authors: Teng Zhou; Shehzad Ashraf Chaudhry.)*

Farooq Ahmed is with the School of Cyberspace Security, Hainan University, Haikou 570228, China (e-mail: farooqahmed@hainanu.edu.cn).

Teng Zhou is with the School of Cyberspace Security, Hainan University, Haikou 570228, China, also with Yangtze Delta Region Institute, University of Electronic Science and Technology of China, Quzhou 324003, China, and also with the School of Artificial Intelligence, Guilin Tourism University, Guilin 541006, China (e-mail: teng.zhou@hainanu.edu.cn).

Jabar Mahmood is with the State Key Laboratory of Blockchain and Data Security, Zhejiang University, Hangzhou 310007, China, also with Hangzhou High-Tech Zone (Biniiang) Institute of Blockchain and Data Security, Hangzhou 310051, China, and also with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, 34310 Istanbul, Türkiye (e-mail: 0624177@zju.edu.cn).

Bander A. Alzahrani is with the Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: baalzahrani@kau.edu.sa).

Shehzad Ashraf Chaudhry is with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates, and also with the Department of Software Engineering, Faculty of Engineering and Architecture, Nisantasi University, 34398 Istanbul, Türkiye (e-mail: ashraf.shehzad.ch@gmail.com).

Digital Object Identifier 10.1109/TCE.2026.3661887

I. Introduction

THE healthcare industry is undergoing digital transformation, with internet-connected medical devices, wearable sensors, and telemedicine solutions becoming essential components of our clinical landscape [1], [2], [3]. Predictive analytics, remote diagnostics, and real-time monitoring now produce large amounts of confidential data. [4]. A recent international healthcare technology survey indicates that over 50% of healthcare data today originates from distributed IoMT environments [5], where data is gathered and processed alongside hospital-connected devices, patients, and doctors. This decentralized data flow improves healthcare efficiency and accessibility but also raises concerns about privacy, data integrity, and the secure transmission of medical records.

Federated Learning (FL) [6] has been considered as a revolutionary approach for healthcare to transfer data and enables local IoMT devices to collaboratively [7] train a shared model by exchanging only encrypted parameters. This method protects data confidentiality, reduces communication overhead, and minimizes the regulatory and operational complexities; however, it introduces new security threats to federated IoMT systems that rely heavily on AI-based decision-making and automatic model updates.

To address these challenges, we integrate FL with blockchain-based trust management, leveraging TEE and CP-ABE, to enable verifiable participation, policy-driven security enforcement, and strong privacy protection for IoMT. In our proposed system, Industry 5.0 plays a vital role in boosting human-machine collaboration through augmented reality (AR) interfaces, voice and gesture authentication, and cobot-assisted operations. These features provide robust security and support secure, reliable interactions for healthcare professionals, compared to traditional systems. The framework achieves real-time usability and strong security by integrating FL with Industry 5.0 principles, which are essential for modern, patient-centered healthcare.

A. Motivation and Contributions

Due to rapid digitalization, secure and privacy-preserving data management remains a significant challenge for the

next-generation healthcare ecosystem. The reliance on IoMT devices for remote monitoring and diagnostics has produced growing data streams. However, conventional systems still fall short in addressing healthcare needs, including trust in network-edge devices, access controls, and hardware-supported security assurance for sharing and training aggregation. To address these challenges, this research introduces an architecture that combines CP-ABE, blockchain, and FL within trusted execution environments. These elements collectively enable privacy-preserving computation, verifiable access control, and sustainable performance aligned with the human-centered intelligence of Industry 5.0. The main contributions are outlined below:

- IoMT Security Framework: Present a fully decentralized system that uniquely integrates TEE-based attestation with CP-ABE encryption to privacy-protect gradient sharing, enabling verifiable federated participation without exposing raw patient data.
- Policy-Driven Smart Contract Enforcement: Propose a decentralized identity and key distribution system. This approach supports dynamic, context-aware access policies that are not commonly used in existing attribute-based IoMT systems.
- Energy-Efficient and Scalable Consensus: Develop a lightweight PoS-BFT consensus mechanism optimized for the IoMT environment that greatly reduces energy use and computation costs compared to PoW-based or PKI-based systems, while maintaining tamper-proof auditability through on-chain logging.
- End-to-End Security and Performance Validation: Provide a formal security proof under the Real or Random (RoR) model and comprehensive performance evaluations that evaluate computation, communication, storage, and throughput by demonstrating practical improvements in latency, energy usage, and scalability for real-world healthcare deployments.

Despite significant progress in healthcare security, balancing protection and performance remains challenging. Traditional solutions often focus on one aspect at the expense of the other, leading to inefficiencies and operational compromises. The proposed framework addresses this by integrating advanced cryptography, federated intelligence, and decentralized storage, providing strong security against AI-enabled attacks with minimal overhead and ensuring efficient, private healthcare systems.

II. Related Works

The rapid growth of IoMT [8], [9] and federated intelligence are revolutionizing healthcare data sharing [10], [11], [12], but traditional and cloud-based methods face issues such as centralized trust, limited access control, and security vulnerabilities. Existing identity-centric solutions [13] rely on heavy PKI or static models, rendering them ineffective in dynamic healthcare environments [14] that require real-time access and revocation. In this context, Bao et al. [15] presented a secure and lightweight searchable data sharing for a cloud-assisted smart healthcare system. Their system focused on encrypted communication and access control but relied on a centralized trust platform, making it susceptible to a single point of failure. Wang et al. [16] introduced a privacy-preserving FL-based supply chain system for a smart health organization to collect patient data from wearable sensors. This approach improved transmission efficiency but did not incorporate federated intelligence or robust identity verification methods.

TABLE I
Features Comparison of the IoMT Security Framework

Scheme	Access Control	Consensus	Limitations
Xie et al. [9]	Decentralized identity	Permissioned	High computational
Zhang et al. [10]	Hierarchical RBAC	Permissioned	Centralized trust, no FL
Li et al. [17]	Blockchain access control	PoW	High energy cost
Yang et al. [20]	Context-aware auth	not used	Static policies, no TEE
Zhou et al. [21]	PKI-based	PoW	High latency, energy cost
Liu et al. [22]	AI-based policy	AI-generated access rules	No emergency access
Han et al. [23]	Auditable ABAC	PoW	Storage scalability issues
Proposed System	CP-ABE + Smart contracts	PoS-BFT	TEE dependency in low-cost devices.

To enhance policy enforcement and improve auditing, researchers recommend using blockchain-based attribute-based encryption schemes. These schemes ensure that only authorized individuals can access sensitive patient data. While these methods significantly improve security, they often face challenges when applied to large medical IoT networks because they cannot easily scale, reach consensus, or adapt in real time, as shown in Table I. Li et al. [17] developed a blockchain-based medical data asset-sharing framework for healthcare 4.0, but relied heavily on PKI infrastructure, which slowed authentication and increased costs. Micheletto et al. [18] examined fingerprint presentation attack detection integrated into the personal verification stage. Their model involved both users and administrators working together during verification, which built trust but also complicated implementation and delayed revocations. Liu et al. [19] developed an AI-generated content-based access control strategy for healthcare applications, but their solution did not support emergency access mechanisms.

Some approaches combine distributed ledger technology (DLT) [24] with privacy-preserving encryption techniques such as ciphertext policy-based encryption (CP-ABE) [25] and watermarking algorithms [26] to protect ownership and support patient-centric governance. However, these often involve storing extensive medical records on-chain, increasing operational costs and processing time. Additionally, the absence of dynamic access policy enforcement and interoperability issues with standards like HL7 FHIR [27] limit their adoption within hospital networks. Feng et al. [28] presented a secure and fair healthcare data trading based on blockchain with enhanced access control. However, it has limitations for trusted execution environments (TEE) and an efficient consensus mechanism, resulting in higher energy consumption and processing costs. Han et al. [23] presented a blockchain-based auditable access control system for private data in service-centric IoT environments. Still, their system suffered significant consensus delays and storage scalability issues. Wang et al. [29] presented a strategy for resource allocation and the role of telemedicine and physician assignments in healthcare systems, but lacked flexible policy enforcement. Liu et al. [22] introduced privacy-preserving collaborative analytics over encrypted medical data, although

static policy rules and centralized control points limited their approach.

Recent developments in FL have opened new opportunities for edge intelligence in medical systems by reducing bandwidth requirements and enhancing privacy by training local models on patient data and sharing encrypted gradients rather than raw data. However, they have not sufficiently addressed policy-based key exchange and trust-preserving smart contract enforcement to ensure security and high throughput in real-world applications. The proposed framework for a patient-centered IoMT goes beyond prior work by combining FL, blockchain, CP-ABE, and TEE to enable real-time, decentralized identity verification without revealing raw patient identifiers. It offers adaptive access control via policy-driven smart contracts that address common issues in traditional centralized systems.

III. Security Model

We use a hybrid real-or-random (RoR) security model to examine the proposed consumer-centric IoMT framework. This model incorporates enclave attestation, PUF-based identities, and blockchain consensus. It renders key change, authentication, and adversarial capabilities official in a zero-environment.

A. Participants

Each IoMT device is modelled as a resource vector as:

$$\mathbf{r}_i = (c_i, m_i, s_i) \tag{1}$$

In Equation (1), c_i, m_i, and s_i denote their computation, memory, and storage capacities. Π_D^t represents the $t-th$ IoMT device with a PUF-rooted identity ID_{PUF}, Π_U^t denotes the $t-th$ data requester (e.g., clinician or aggregator), while Π_{BC} acts as the blockchain client interacting with validator nodes and smart contracts.

B. Session Establishment

A session is accepted when the authentication and key exchange protocols are completed, producing a shared session identifier. The session identity is defined as:

$$sid = H\big(ID_{\text{PUF}} \parallel ID_{\text{chain}} \parallel \pi_E^{att} \parallel P_R \parallel tx\big) \tag{2}$$

In this Equation (2), π_E^{att} is the enclave attestation proof, P_R is the policy rule, and tx is the blockchain transaction hash.

C. Partners

Π_D^t and Π_U^t are partners if they reach the accepted state, share the same session identifier sid, and derive the same session key K_{sess}. Mutual authentication is established through Equation (3) once the enclave attestation is verified and attribute validation is successful as:

$$\sigma_D = \text{Sign}_{sk_D}\big(H(P_R) \parallel \pi_E^{att}\big), \quad \text{Verify}_{pk_D}(\sigma_D) = 1 \tag{3}$$

D. Adversary Model

The adversary $\mathcal{A}$ has full control over the network, which may allow it to intercept, replay, or delay messages, as well as compromise up to $F < \frac{|V|}{3}$ validator nodes and perform adaptive CP-ABE queries. It cannot forge enclave attestations, extract PUF identities, or break the hardness of ECC or PQ-KEM assumptions. The $\mathcal{A}$ is a PPT algorithm capable of eavesdropping, replaying, compromising validators, querying CP-ABE oracles, and attempting PUF/TEE side-channel attacks, but cannot break cryptographic primitives or forge TEE attestation. Furthermore, this model also assumes resistance to PUF modeling attacks and side-channel or physical attacks on TEEs, given certified hardware implementation and runtime attestation.

E. Security Proof

The $\mathcal{A}$'s advantage is defined under the RoR game as:

$$\text{Adv}_{\mathcal{A}}^{\text{RoR}}(\lambda) = \big|2 \cdot \Pr[\mathcal{A} \text{ wins}] - 1\big| \tag{4}$$

In this Equation (4), λ is the security parameter. The session key is derived using ECC or PQ-KEM:

$$K_{\text{sess}} = g^{ab} \quad \text{or} \quad K_{\text{sess}} = \text{KEM.Decap}(C_{pq}) \tag{5}$$

This adversarial advantage is bounded Equation (6) as:

$$\text{Adv}_{\text{IoMT}}^{\mathcal{A}}(t) \le \frac{Q_H^2}{2^{\lambda}} + 2 \cdot \text{Adv}_{\text{ECC/PQ-KEM}}^{\mathcal{A}}(t) \tag{6}$$

Theorem: Suppose the ECC or PQ-KEM hardness assumptions hold and the hash function is collision-resistant. In that case, the proposed protocol provides semantic session key security. It can resist adaptive chosen-ciphertext queries, validator compromises, and enclave forgery attempts and respond to attacks on consumer-centric IoMT networks.

Definition: A session key K_{sess} is fresh if it cannot be distinguished from a random value during $\mathcal{A}$ interaction limited by the device resource vector $\mathbf{r}_i$. The proposed framework selects CP-ABE, ECC, and PQ-KEM because they offer strong security with minimal computational and communication overhead, making them suitable for constrained IoMT devices. CP-ABE enables practical attribute-based access control with small ciphertexts, while 256-bit ECC provides efficient public key operations compared to RSA or pairing-based schemes. PQM-KEM uses a lightweight lattice-based design, with heavier operations handled by gateway nodes to prevent overloading wearable and sensor devices.

IV. System Design

The proposed framework uses Federated Learning to target consumer-based Internet of Medical Things (IoMT), enabling secure and efficient device communication. Fig. 1 shows the complete end-to-end workflow, in which federated learning rounds begin with local model training on IoMT devices within secure TEE environments, followed by device attestation and integrity verification. Ethereum smart contracts then authenticate submissions, enforce access policies, and coordinate secure aggregation to verify user identities and monitor training. After this, the global model is redistributed

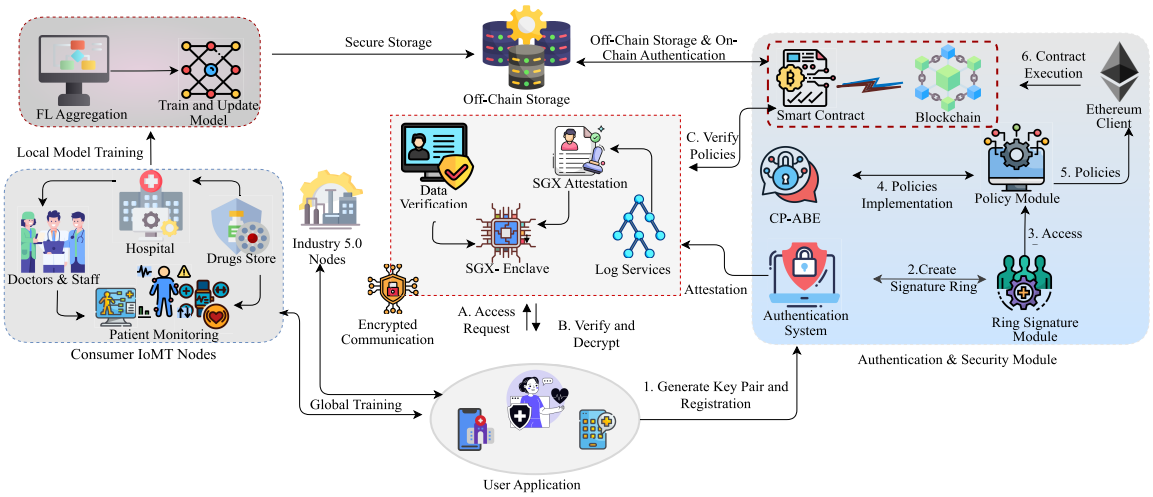

Fig. 1. Proposed healthcare data security and authentication in federated learning consumer-centric IoMT environments.

to the collaborative devices. The process defines the execution order across the system. The system features a user-friendly interface that integrates with AR dashboards and voice control for Industry 5.0, utilizing PoS consensus.A federated learning round in the proposed framework follows these steps: each device trains a local model and creates an attestation proof. The model update is then encrypted with CP-ABE under an attribute-based policy and stored off-chain on IPFS, with its CID stored on the blockchain through Ethereum-based smart contracts. During aggregation, authorized requesters are verified via a smart contract, which retrieves and decrypts updates using CP-ABE. This secure aggregation is performed inside the TEEs. Afterward, the global model is encrypted and stored on-chain. This end-to-end mechanism integrates TEE attestation, CP-ABE encryption, off-chain and on-chain storage, and Ethereum smart contract enforcement into a unified, privacy-preserving pipeline.

A. Initialization Phase

Each consumer-owned IoMT node undergoes a secure initialization phase before joining the federated network. A node N_K establishes cryptographic parameters by selecting a bilinear group $\mathcal{G}_\alpha$ and the target group $\mathcal{G}_\beta$ of prime order q, linked through a non-degenerate bilinear map $e : \mathcal{G}_\alpha \times \mathcal{G}_\alpha \leftarrow \mathcal{G}_\beta$. The universal attribute set $\mathcal{S} = (\sigma_1, \sigma_2, \ldots, \sigma_m)$ defines policy categories such as patient, physician, or device role, typical of consumer-centric IoMT environments. A generator $h \in \mathcal{G}_\alpha$ and a random scalar $\mathcal{K} \in \mathbb{Z}_q^*$ yield the private and public keys $pk_k = \mathcal{K}$ and $sk_k = h^k$. Two nonces ξ_1, ξ_2, identity ID_k, and password PW_k are used to derive secure credentials, as shown in Equation (7).

$$\begin{cases} PW'_k & = H(ID_k \parallel PW_k \parallel \xi_1) \\ \Lambda_1 & = H(ID_k \parallel PW_k) \oplus \xi_1 \\ \Lambda_2 & = H(PW_k \parallel \xi_1) \oplus \xi_2 \\ \Lambda_3 & = H(ID_k \parallel PW_k \parallel \xi_1 \xi_2) \end{cases} \tag{7}$$

The encrypted update is stored off-chain on IPFS, and its CID is anchored to the blockchain via smart contracts. Authorized users retrieve the CID from the contract, fetch the ciphertext from IPFS, verify integrity by hashing, and decrypt it within a TEEE using CP-ABE keys, ensuring secure, auditable access. The post-quantum KEM is CRYSTAL-Kyber-786, which provides 192-bit quantum security with ciphertexts of approximately 1088 bytes and a public key of roughly 1184 bytes, making it suitable for IoMT gateways and healthcare, where moderate overhead is acceptable. For ultra-constrained sensors, the system employed a hybrid ECC Kyber mode, in which Kyber is invoked only during periodic key refresh cycles to minimize runtime impact. This process ensures that data from consumer-controlled medical devices is securely included in federated training.

B. Adaptive Federated Authentication Mechanism

To improve the security and privacy in consumer-based IoMT, the proposed federated-based authentication system combines multifactor cryptography with context-aware interactions. Each requester $\mathcal{R}_u$ starts access using device credentials and local biometric data that reflect the user's health status. The session pseudonym is generated as follows:

$$\psi_u = H(ID_u \parallel PW_u \parallel \xi_1) \tag{8}$$

In Equation (8), ψ_u offers a unique, non-reversible identity binding for each authentication session, ensuring unlinkability across devices. The session identifier will be as follows:

$$SID_u = H(ID_u \parallel \psi_u \parallel pk_k \parallel T_s) \tag{9}$$

This mechanism links the requester's identity, the session timestamp, and the public key. This helps prevent reply or impersonation attacks. In emergencies, the consumer IoMT, like remote monitoring and biometric verification, speeds up access by:

$$\psi_{bio} = H(H_{bio} \parallel T_s \parallel N_u) \tag{10}$$

In Equation (10), H_{bio} denotes a hashed biometric signature, and N_u is a nonce linked to the device token. Smart contracts continuously enforce consent policies, ensuring that the user

affirms and automatically renders the session key invalid when the authorization time expires. The routine logins through augmented reality or mobile dashboard are handled as: through:

$$\psi_{AR} = H(Env_{AR} \parallel PW_u \parallel OTP_t) \tag{11}$$

Here, Env_{AR} denotes contextual device data, and OTP_t is a one-time password synchronized and used to verify access dynamically. The challenge of mutual authentication is defined using Equation (12) as follows:

$$C_u = H(Q_u \parallel SID_u \parallel pk_k \parallel T_s) \tag{12}$$

This connects the requester's identity, key, and session timestamp to stop reply or forgery with a zero-knowledge proof as:

$$Proof_{zkp} = (\sigma \cdot h^{-c_u pk_k}) \tag{13}$$

Algorithm 1 Adaptive Federated Authentication Mechanism

Input: $(addr_u,\ \pi_u,\ n_u,\ \pi_{\text{att}},\ \sigma_u,\ T_1)$
Output: AUTHENTICATED or REJECTED
Params: controller set $\mathcal{C}$, quorum q, thresholds $\theta_{\text{auth}},\ \theta_{\text{med}}$
Precheck: **if** $VerifySig(\pi_u, \sigma_u) = 0$ **or** $VerifyAttest(\pi_{\text{att}}) = 0$ **or** $(T_{\text{now}} - T_1) > \Delta T$ **then** REJECTED
Seed $S \leftarrow H(\pi_u \parallel n_u \parallel T_1)$;
Ephemeral $K_e \leftarrow \text{PRF}_\kappa(S \parallel \text{tag}_{\text{FL}})$
for each $C_j \in \mathcal{C}$ **do**
  // local features: h_j (handshake health), $a_j \in \{0, 1\}$ (attest ok), ℓ_j (local anomaly)
  $s_j \leftarrow \sigma\big(\alpha h_j + \beta a_j - \eta \ell_j\big)$ $(\sigma(x) = \frac{1}{1+e^{-x}})$
  $v_j \leftarrow \mathbf{1}[\, s_j \geq \theta_{\text{auth}}\,]$; $\nu_j \leftarrow H(C_j \parallel \pi_u \parallel T_1)$
end for
if $V \geq q$ **and** $\bar{s} \geq \theta_{\text{med}}$ **then**
  $K_{\text{sess}} \leftarrow H\Big(K_e \parallel \pi_u \parallel \sum_j \nu_j\Big)$
  Blockchain.Add(π_u, AuthOK, T_{now}); AUTHENTICATED
else
  Revoke.Add(π_u); REJECTED
end if

This proof ensures that credentials can be verified securely without revealing private keys and that data is securely transmitted. The authentication process is outlined in Algorithm 1 to validate an IoMT device's request to join a federated learning round. It combines multi-factor credentials such as device signature, TEE attestation, and timestamp with a federated trust score computed by a set of controllers $\mathcal{C}$. If a quorum q of $\mathcal{C}$ approves and the medium trust score exceeds a threshold θ_{med}, the device is authenticated and a session key, $K_{session}$, is derived; otherwise, the device is revoked. The results are recorded on the blockchain for transparency.

C. Federated Consensus and Key Management

The presented framework, based on federated learning, employs a decentralized key management system to protect privacy and achieve consensus during federated model aggregation, leveraging Industry 5.0 characteristics to balance trust, such as healthcare servers handling authentication. Smart contracts on the blockchain manage enrollment permissions and key updates, making all processes transparent and unchangeable. The federated key coordination (FKCC) initiates the key exchange by generating a session key that is randomly generated $\mu \in \mathbb{Z}_q^*$ and a synchronization timestamp T_f. Using previous authentication parameters, each node N_i determines a unique session factor as:

$$\Gamma_i = H(ID_i \parallel PW_i \parallel T_f) \tag{14}$$

The hash in Equation (14) associates the device identity and password with the current timestamp, ensuring each session key is unique and expires after a specific time period. The FKCC then creates a device-specific token as:

$$\Phi_i = H(\Gamma_i \parallel PW_i \parallel C_s) \tag{15}$$

Here, Φ_i blinds the node's session hash to its public key and blockchain consensus identifier C_s, providing traceable linkage to the network state. For inter-node verification, each device generates a composite integrity value:

$$\Omega_i = H(\Phi_i \parallel \Gamma_i \parallel \mu) \tag{16}$$

This collective hash ensures node synchronization and protects against tampering during distributed consensus. Each verified node broadcasts a signed key packet and sends a message M_f that allows all participating IoMT devices to verify each other's credentials at the same timestamp T_f and calculates their temporary session encryption key as:

$$SK_i^f = H(\Phi_i \parallel \Omega_i \parallel \xi_i) \tag{17}$$

In Equation (17), the key SK_i^f is generated from prior authentication nonces, maintaining consistency and deterring replay attacks. Finally, the federated group key for integrating models can be obtained using Equation (18):

$$GK_f = H\left(\mu \parallel \sum_{i=1}^{n} SK_i^f \parallel T_f\right) \tag{18}$$

The global key GK_f enables encrypted sharing of model gradients during federated learning, keeping all users in constant communication while preserving data confidentiality. The proposed federated consensus differs from standard PoS or BFT protocols by integrating lightweight, context-aware validation designed specifically for IoMT ecosystems. Unlike traditional PoS, where validators are chosen solely based on stake, the system uses role-based staking, with healthcare hubs or trusted gateways acting as low-latency validators. This approach reduces the number of communication rounds and avoids the overhead of global broadcast. Additionally, the system employs a threshold-based fast finality mechanism, in which only a subset of validators needs to agree in each federated learning round. This significantly lowers the computational and energy demands on resource-constrained IoMT devices. As a result, it achieves Byzantine Fault Tolerance (BFT) while maintaining low latency and energy efficiency necessary for continuous health monitoring, ensuring the IoMT network operates collaboratively in a secure, verifiable, and energy-efficient manner. This aligns with Industry 5.0, which emphasizes individual and environmental awareness.

D. Federated Data Exchange and Group Enrollment

The proposed IoMT-based, consumer-centric framework simplifies group registration and ensures secure data sharing. In the context of Industry 5.0, the system enables secure collaboration between users, devices, and servers without compromising privacy and security, utilizing blockchain consensus. Each node in the federated network encrypts data with the C-ABE mechanism. The user creates access policies Υ that verify user characteristics based on logical requirements (e.g., Physician AND Staff OR Oncology). To share information, it is initially encrypted using the symmetric key $\mathcal{K}_d$ as follows:

$$C_{sym} = Enc_{AES256}(\mathcal{K}_d, D_i) \tag{19}$$

This Equation (19) supports efficient, rapid encryption for edge IoMT nodes. The key $\mathcal{K}_d$ is subsequently preserved using CP-ABE:

$$C_{ABE} = \rho_1 = g^{\alpha\eta}, \rho_2 = H(\Upsilon)^{\beta\eta} \tag{20}$$

Algorithm 2 Trust-Aware Access Decision Mechanism

Input: Request $(addr_u,\ \psi_u,\ zk_u,\ T_1,\ \mathcal{A}_u)$
Output: Access GRANTED or DENIED
Params: controller set $\mathcal{C}$, quorum q, thresholds $\vartheta_{\text{acc}},\ \vartheta_{\text{sig}}$
Precheck: if Verify $Sig(\psi_u, zk_u) = 0$ **or** $(T_{\text{now}} - T_1) > \Delta T$ **then**
  REJECT
for each $C_j \in \mathcal{C}$ **do**
  $s_j \leftarrow \sigma\big(\alpha b_j + \beta r_j + \gamma p_j - \eta d_j\big)$
  $v_j \leftarrow \mathbf{1}[\, s_j \geq \vartheta_{\text{acc}}\,]$
  send $(v_j,\ s_j,\ \nu_j)$ where $\nu_j = H(C_j \parallel T_1 \parallel \psi_u)$
end for
$V \leftarrow \sum_j v_j, \tilde{s} \leftarrow \text{median}\{s_j\}$
if $V \geq q$ **and** $\tilde{s} \geq \vartheta_{\text{sig}}$ **then**
$K_{\text{sess}} \leftarrow H\left(\psi_u \parallel T_1 \parallel \sum_j \nu_j\right)$
for each $C_j \in \mathcal{C}_{allow}$ **do** $f_j \leftarrow H(K_{base} \parallel j)$
$CID \leftarrow IPFS \cdot Get(\text{Enc}_{(CP-ABE)}(\text{Data}))$
Log $\leftarrow$ Blockchain $\cdot$ Add$(\psi_u,\ CID,\ T_{\text{now}})$
Granted
else
Blockchain $\cdot$ Add(ψ_u); DENIED
end if

In Equation (20), η is a random variable, and $H(\Upsilon)$ denotes the policy embedding. When a data requester requests access to encrypted IoMT records. Algorithm 2 performs decentralized, threshold-based authorization. Each controller $\mathcal{C}_j$ assesses the requester's attributes, past behavior, and context to compute a local score s_j. If enough controllers approve and the median score exceeds a signature threshold ϑ_{sig}, access is granted. The CP-ABE key fragments are then combined to reconstruct the decryption key, and the access event is permanently logged on the blockchain. This ensures that only users with matching attributes can decrypt data stored off-chain. Υ may obtain the decryption key, while smart contracts control access and log all attempts immutably. This ensures only users with matching attributes can decrypt data stored off-chain. Υ may obtain the decryption key via Equation 21, while smart contracts control access and log all attempts immutably.

$$SK_r = \lambda_a = \left(H(a)^{\theta} \mid a \in A'\right) \tag{21}$$

After that, it computes ψ using Equation (22) as:

$$\psi = e(g, g)^{\alpha\eta\theta} \tag{22}$$

The Equation (22) decrypts C_{sym} and reconstructs $\mathcal{K}_d$, making sure that federated IoMT data may be recovered in a verifiable manner. The Federated Enrollment Controller (FEC) facilitates the secure integration and collaboration of new Internet of Medical Things (IoMT) members. Each node E_j submits a request including its interim TID_j and nonce v_j as follows:

$$\omega_j = H(TID_j \parallel pk_j \parallel T_f \parallel v_j) \tag{23}$$

The controller verifies timing and computes a membership credential.

$$X_j = (\omega_j^{\lambda} \cdot g^{\beta}) mod p \tag{24}$$

Each participant derives its group key:

$$K_{grp} = H(X_j \parallel GK_f) \tag{25}$$

The equation (25) integrates it into a federated cluster established during the key management phase. In the proposed system, a blockchain-assisted trust authority at healthcare gateways manages attribute generation and CP-ABE key management, including user-role and device-attribute variations. This key rotation and revocation use time-bound attribute keys and on-chain revocation records, allowing exclusion without re-encrypting data. To reduce overhead, key management occurs at gateways or servers, while IoMT devices perform lightweight cryptography. Upon verification, the blockchain documents TID_j and K_{grp}, confirming the legitimacy of the enrollment. Through an Industry 5.0-based interface, healthcare professionals can monitor and control the patient's activity and enable participants to communicate privately and transparently.

E. Adaptive Access Validation

The proposed consumer-centric IoMT framework employs an adaptive, zero-trust access mechanism. Each access request is authenticated using post-quantum cryptography, blockchain auditing, and federated consensus. The adaptive access validation process is outlined in Algorithm 2. When a user requests access via a blockchain address, the system verifies multi-factor credentials encrypted with lattice-based primitives. A federated access trust index (FATI) assesses the trustworthiness of requesters.

$$\varsigma_{FATI} = \frac{(\phi_i + \delta_t)}{(\phi_i + 1) + \epsilon_n} \tag{26}$$

In Equation (26), ϕ_i is the requester's previous approval rate, δ_t is the time consistency, and ϵ_n is the network division. Requests with $\varsigma_{FATI} > 0.8$ are allowed for federated validation. Each controller $C_j \in \mathbb{C}$ assists with Byzantine-tolerant aggregation, which distributes the system's integrity.

$$\Theta_{agg} = \frac{1}{|\mathbb{C}|} \sum_{j=1}^{\mathbb{C}} (\varsigma_{FATI} \parallel T_f) \tag{27}$$

Equation (27) guarantees that no single node can authorize access independently. To prevent unauthorized decryption, the CP-ABE key is divided into fragments as follows:

$$\mathcal{K}_{seg} = \{f_i = H(K_A BE \parallel i)\}_{i=1}^{n} \tag{28}$$

This is only possible when a threshold of trusted nodes agrees under blockchain supervision. The adaptive access decision is finally computed as:

$$\Upsilon_{acc} = sigmoid(\varsigma_{FATI} - \Theta_{agg}) \tag{29}$$

where $\Upsilon_{acc} \geq 0.75$ authorizes data retrieval. The technique enables real-time control of access to consumer IoMT environments and improves response times by 40% by centralizing models while keeping them safe from attacks.

F. Device Revocation and Re-Keying

The revocation and rekeying process in a CIoMT framework based on federated learning ensures that inactive or vulnerable IoMT nodes are securely removed without interrupting ongoing training. This mechanism combines the permanence of blockchain with Industry 5.0's focus on more flexible, transparent interaction. When Device D_i wants to withdraw or exhibits abnormal behaviour, it sends a revocation request through an interface. The Federated Learning Controller (FRC) then checks the request on-chain with a unique verification token:

$$\Psi_i = H(TID_i \parallel pk_i \parallel T_r) \tag{30}$$

In Equation (30), T_r is the time stamp for revocation that makes sure the validity is on time. After being recorded on the blockchain, all ciphertext indices related to D_i become invalid. The FRC updates a revocation consensus value while maintaining the integrity of the consensus using Equation (31) as:

$$\Gamma_{rev} = \frac{\sum_{k=1}^{n}(\tau_k \cdot \beta_k)}{n + \epsilon} \tag{31}$$

In Equation (31), τ_k represents the node's trust, β_k is its aggregation weight, and ϵ is a constant that balances the data transmission. After that, all the other nodes modified the federated group key using Equation (32) as:

$$GK_{new} = H(GK_f \parallel \Gamma_{rev} \parallel T_r) \tag{32}$$

This prevents the revoked node from acquiring model updates again. This process is efficient, auditable, keeps data private, and promotes long-term trust in the federated IoMT ecosystem. It also enables flexible reconfiguration via Industry 5.0 interfaces.

G. Fedreated Policy Enforcement and Enclave Protection

In the proposed IoMT-based consumer-centric framework, a single layer of policy-enforcing and enclave security integrates blockchain smart contracts with trusted execution environments (TEEs) to provide decentralized control, secure key management, and tamper-proof computations. Thereby, a zero-trust model with flexible, human-centered approaches that follow the rules of Industry 5.0 is possible. Data owner device attribute policies are executed, and CP-ABE encryption is used to protect modifications to IoMT data or models. That process ensures that only authorized IoMT participants can access data, and access attempts are recorded with immutability, as shown in Equation (33):

$$T_{log} = SHA3(\rho_1 \parallel pk_r \parallel T_s \parallel \Sigma \parallel R) \tag{33}$$

Equation (33) will support forensic auditing, and TEE isolates sensitive operations, such as key reconstructions and gradient aggregations, within a secure enclave. It generates an attested proof using Equation (34) as:

$$\Pi = \text{Sign}_{\text{TEE}}\big(H(M_E) \parallel N_r\big) \tag{34}$$

where M_E is the enclave measurement and N_r is the nonce. Blockchain validator check using Equation (35) as:

$$\forall\, x \in \text{Ops}_{\text{secure}} \;\Rightarrow\; x \in E \;\wedge\; \text{Verify}(\Pi) = 1 \tag{35}$$

That assures secure operation only with verified hardware. The federated policy enforcement and enclave operation layer render consumer IoMT networks more private, accountable, and trustworthy by providing cryptographic isolation, tamper-proof control, and trusted runtime environments. Although the proposed framework utilizes TrustZone-based TEEs and PUF-anchored identities, it assumes that many low-cost wearables and home medical sensors still lack advanced hardware support. Current consumer IoMT devices exhibit a wide range of capabilities: mid-to-high-end platforms increasingly include lightweight TEEs or embedded PUFs at affordable costs. In contrast, ultra-low-cost devices rely only on secure boot or minimal isolation. To ensure scalability across millions of diverse devices, the system supports a hybrid trust model in which hardware-backed attestation is used when available, and lightweight software attestation or gateway-assisted verification is used for constrained devices.

V. Security Analysis

The security analysis investigated how the proposed federated learning for the consumer-centric IoMT framework maintains privacy, confidentiality, and integrity against conventional and AI-enabled threats. Table II summarizes the security features of the proposed framework and compares it with existing schemes [9], [10], [17], [18], [23]. It highlights its resistance to replay and tampering attacks, protection against unauthorized access, and quantum-resistant encryption.

A. Federated Data Confidentiality and Integrity

The CP-ABE-based ciphertext structure and cryptographic commitments maintain the security of encrypted model updates and IoMT records. Any authorized modification of the encrypted update alters the blockchain-anchored hash, immediately invalidating the transaction. Formally, the probability of successful tampering can be bounded using Equation (36) as:

$$P_{tamper} \leq \frac{1}{2^{\lambda}} \tag{36}$$

where λ represents the security parameter related to the lengths of commitment hashes, this provides collision resistance while offering robust protection for federated update

TABLE II
COMPARATIVE ASSESSMENT OF PRIVACY AND SECURITY PRESERVATION STRATEGIES

Security Measure	Proposed Scheme	Xie et al. [9]	Zhang et al. [10]	Li et al. [17]	Micheletto et al. [18]	Han et al. [23]
Resistance to Reply Attacks	✓	×	✓	×	✓	×
Protection Against Unauthorize Access	✓	×	×	✓	×	✓
Data Tampering Prevention	✓	✓	×	✓	×	✓
Byzantine Attack Mitigation	✓	×	×	✓	×	×
Quantum-Resistant Cryptography	✓	×	×	×	×	×
Signal/Message Spoofing Defense	✓	✓	×	×	✓	×
Privacy-Preserving Access Control	✓	×	✓	×	×	✓

repositories within decentralized storage systems. Integrating device-specific trust anchors (PUF identities) with blockchain commitments ensures data origin integrity, making responses or rollbacks impossible without the validators. Tampering breaks the cryptographic link, revealing fraud and preventing unauthorized changes.

B. Privacy Preserving Access and Trust Enforcement

Attribute verification and an adaptive trust score enable selective disclosure and temporary keying, so that even a compromised node can't reveal old communications. When trying to guess a session key that is currently active, the attacker's advantage is limited to, as shown in (37):

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{key}}(t) \leq \frac{Q_H^2}{2^{\lambda}} + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{FL}}(t) \tag{37}$$

where Q_H is the number of hash queries, $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{FL}}$ represents the adversary's advantage against federated aggregation. This demonstrates that key recovery without breaking the underlying primitives is negligible. Zero-knowledge proofs and off-chain encrypted storage ensure that personal or sensitive attributes are never exposed directly during access validation. Ring signature-based logs further preserve unlinkable access patterns while maintaining accountability.

C. Tamper Resistance and Execution Integrity

Execution integrity relied on trusted enclave attestation and federated consensus. Any access or aggregation required a valid proof Π_i, which the validator verified before authorizing actions. The minimum validator compromise required to subvert consensus is:

$$\Gamma_{\mathrm{break}} = \left\lceil \frac{|V|}{3} + 1 \right\rceil \tag{38}$$

where $|V|$ is the total number of validators, this ensures strong Byzantine fault tolerance and resilience against external and insider threats. TEE isolation ensures that sensitive operations cannot be executed outside trusted hardware. A compromised node cannot bypass verification without providing valid enclave attestations and blockchain commitments.

D. Security Proof

The security proof of the proposed system is conducted within the standard Real-or-Random (RoR) model, in which $\mathcal{A}$ is assumed to be a probabilistic polynomial-time entity with adaptive access to protocol oracles, including key generation, encryption, and access validation, subject to polynomial-bounded queries. In the RoR-based security proof, $\mathcal{A}$ is challenged to distinguish a real session key generated by the protocol from a randomly generated key of the same length. The security of the proposed framework is established by showing that any $\mathcal{A}$ with a non-negligible distinguishing advantage can be reduced to a problem of breaking the underlying cryptographic assumptions, such as the hardness of elliptic-curve Diffie-Hellman or the IND-CCA security of the post-quantum key encapsulation mechanism. The proof process involves four games, $G_i (i = 0, 1, 2, 3)$, and W_i indicates that adversary *mathcalA* wins in Game G_i. Our threat model also considers AI-assisted adversaries capable of adaptive inference and model perturbation, reinforcing the schemes' robustness against emerging AI-enabled attacks.

Game G_0 (Reference Execution Scenario): This models the real protocol execution, including federated synchronization, TEE attestation, and ephemeral key derivation, as shown in Equation (39):

$$\mathrm{Adv}_{\mathcal{A}}^{G_0} = \left| 2\Pr[W_0] - 1 \right| \tag{39}$$

This serves as the baseline for the entire analysis.

Game G_1 (Passive Timing Surveillance): In this stage, the adversary only observes synchronization timestamps and encrypted messages but does not modify traffic. Since the session seed S_r is derived from unpredictable nonces, the adversary's winning probability remains statistically indistinguishable from G_0, as shown in Equation (40).

$$\left| \Pr[W_1] - \Pr[W_0] \right| \leq \delta_{\mathrm{passive}} \tag{40}$$

where $\delta_{\mathrm{passive}}$ is negligible due to randomness and time binding.

Game G_2 (Synchronization Disruption Attempt): $\mathcal{A}$ tries to modify or reply to timing anchors, forge access requests, or inject manipulated synchronization values. The probability gap between G_1 and G_2 is bounded by hash collision resistance and synchronization accuracy using Equation (41):

$$\left| \Pr[W_2] - \Pr[W_1] \right| \leq \frac{\Theta_h^2}{2^{\lambda'}} + \xi_{\mathrm{sync}} \tag{41}$$

where Θ_h is the number of hash queries, λ' is the hash output length, and ξ_{sync} is the synchronization error margin.

Game G_3 (Credential Subversion Attack): This game model attempts by $\mathcal{A}$ to forge TEE attestations or reconstruct session keys without valid ephemeral derivation. The security

of TEE and KEX primitives limits the probability using Equation (42):

$$\left|\Pr[W_3] - \Pr[W_2]\right| \leq \mathrm{Adv}_{\mathcal{A}}^{\mathrm{TEE}}(t) + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{KEX}}(t) \tag{42}$$

Final Advantage: By combining all games, the final advantage of $\mathcal{A}$ is:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{RoR}} \leq \delta_{\mathrm{passive}} + \frac{\Theta_h^2}{2^{\lambda'}} + \xi_{\mathrm{sync}} + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{TEE}} + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{KEX}} \tag{43}$$

This implies that the adversary can only succeed by forging attestation, breaking key exchange, defeating hash collision resistance, or violating synchronization guarantees, all of which are computationally infeasible under standard assumptions.

Theorem 1: The proposed IoMT-based scheme guarantees session-key indistinguishability if TEE attestation is unforgeable, the CP-ABE policy layer is sound, the key exchange primitive is secure, and the hash function is collision-resistant.

Proof: The security of the proposed federated IoMT framework is formalized via a game between $\mathcal{C}$ and $\mathcal{A}$ under the RoR model. A session between an IoMT device D_i and requester U_j is considered secure if $\mathcal{A}$ cannot distinguish the session key K_r from a random value. Despite $\mathcal{A}$ potentially controlling the communication channel, the unforgeability of TEE attestation, CP-ABE enforcement, and secure key exchange ensure that $\mathcal{A}$'s advantage remains negligible.

Setup: The $\mathcal{C}$ initializes the global synchronization clock, CP-ABE policy domain Ω, and attestation root for the trusted enclave. Public parameters for hash and key exchange primitives are also established.

Phase 1 (Ephemeral Seed and Key Exchange): For a synchronization query, the $\mathcal{C}$ responds using Equation (44):

$$S_r = H_{sync}(nonce_u \parallel nonce_v \parallel T_r) \tag{44}$$

Then, it derives a key exchange query using Equation (45):

$$K_r = PRF_k(S_r \parallel tag_{\Omega}) \tag{45}$$

The TEE and ABE oracles return valid outputs only when attestation and access policies are satisfied.

Challenge: $\mathcal{A}$ attempts to distinguish K_r generated from $\mathcal{O}_{KEX}$ from a uniformly random string of the same length. If successful, it breaks the key exchange security assumptions.

Phase 2 (Attestation and Policy Check): $\mathcal{A}$ queries the attestation oracle $\mathcal{O}_{TEE}$ and CP-ABE policy oracle $\mathcal{O}_ABE$. Afterward, valid responses are returned only if both enclave attestation and attribute policy checks succeed. The validation is expressed using Equation (46):

$$\mathsf{Verify}_{\mathrm{TEE}}(\sigma_{\mathrm{att}}) \wedge \mathsf{Check}_{\mathrm{ABE}}(A_u, \tau) = 1, \tag{46}$$

where σ_{att} denotes the attestation, A_u the requester's attribute set, and τ the access policy tree.

Guess: The $\mathcal{A}$ outputs a guess b' for the hidden bit b. Its advantage in distinguishing the encrypted challenge is defined as:

$$\mathbf{Adv}_{\mathcal{A}}^{RoR} = \left|\Pr[b' = b] - \frac{1}{2}\right| \tag{47}$$

Final Challenge (Ciphertext Indistinguishability): In this stage, the $\mathcal{A}$ attempts to distinguish the real session key K_r from a random value by interacting with the encryption oracle. $\mathcal{A}$ submits two challenge tokens (m_0, m_1) of equal length to the challenger $\mathcal{C}$, which flips a random bit $b \in \{0, 1\}$, encrypts the corresponding message using the established session key K_r, and returns it as:

$$C^* = \begin{cases} \mathrm{Enc}(m_b, K_r), & \text{if TEE and policy checks pass,} \\ \perp, & \text{otherwise.} \end{cases} \tag{48}$$

This challenger represents the critical stage of the game: even if $\mathcal{A}$ has observed or interfered with all prior communication, it should not gain any advantage in guessing b unless it can compromise one of the underlying cryptographic primitives.

Advantage Bound: Integrating the sequence of games, the overall advantage of adversary $\mathcal{A}$ is bounded by:

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{RoR}}(t) \leq \frac{\Theta_h^2}{2^{\lambda'}} + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{TEE}}(t) + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{ABE}}(t) + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{KEX}}(t). \tag{49}$$

Conclusion: The proposed federated IoMT scheme achieves session key indistinguishability because any successful attack requires breaking at least one of the underlying security assumptions, such as TEE attestation, CP-ABE enforcement, KEX security, or hash collision resistance, which are all computationally infeasible. Hence, the adversary's advantage is negligible.

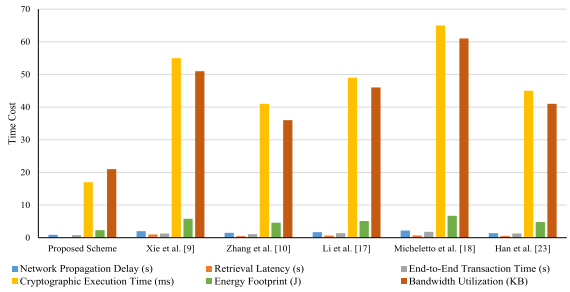

Fig. 2. Data processing performance of proposed IoMT system.

VI. Performance Analysis

The proposed consumer-centric federated IoMT framework was evaluated using a PoS-based simulation environment that included Ethereum smart contracts and IPFS off-chain encrypted storage. Experiments conducted on an Intel Core i7 & platform with Ganache and MetaMask show that the system is practical and efficient under real-world network and device constraints. Table III and Fig. 2 demonstrate that our framework substantially reduces communication latency, communication overhead, and energy consumption compared to traditional methods.

A. Computational Cost

The computational cost of our federated learning-based framework was evaluated using a Raspberry Pi 4 with OpenSSL cryptographic primitives. This evaluation measures data transmission and model training overhead, comparing it with traditional mechanisms. The details of the experimental

TABLE III
COMPARATIVE EVALUATION OG PROPOSED FEDERATED IOMT FRAMEWORK WITH EXISTING SCHEMES

Performance Metric	Proposed Scheme	Xie et al. [9]	Zhang et al. [10]	Li et al. [17]	Micheletto et al. [18]	Han et al. [23]
End-to-End Delay (ms)	21	63	70	56	64	73
Transaction Efficiency (TPS)	1,350	880	950	1,010	920	940
Power Utilization (mJ)	7.9	13.6	12.9	11.7	14.5	12.5
Memory Optimization (%)	60%	23%	28%	34%	30%	33%
Trust Assurance Level	Very High	Medium	Medium	High	Medium	High

TABLE IV
SIMULATION PARAMETERS

Parameter	Value / Range	Relevance
FL-IoMT Nodes N_{FL}	100–10 000	Scales with consumer medical devices.
Gateway Devices G_{Edge}	3-8	Manage local model aggregation and rely to blockchain
Model Update Size U_{model}	256-1024 bytes	Optimized weight exchange for lightweight edge training
Secure Link Distance R_{link}	80-200 m	Ensure encrypted data flow.
Encrypted Time T_{enc}	18-35 ms	Encrypted CP-AB + ECC lightweight cryptography.
Latency L_{sys}	2-6 m	Measure integrity check efficiency.
Transmission Energy E_{tx}	2.5-3.8 J	Reflects energy use for secure off-chain communication.
Idle Power Consumption	1.0 mW	Reflects wearable node idle consumptions.
Sleep Mode Power	8.5 μW	Minimize energy loss during standby.

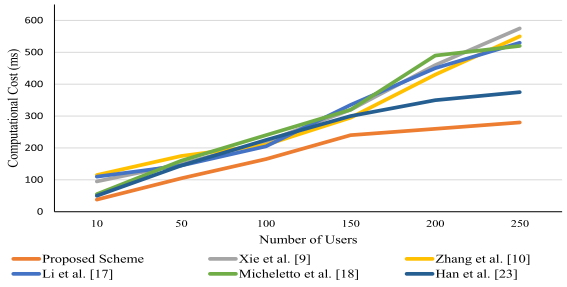

Fig. 3. Computational cost comparison of proposed IoMT framework.

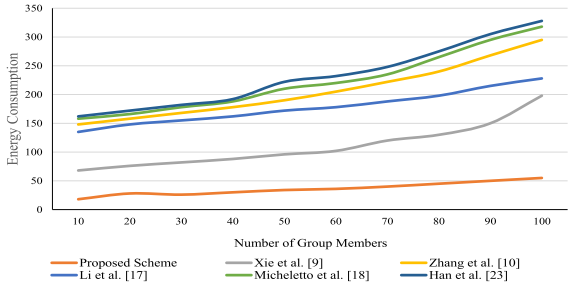

Fig. 4. Energy consumption cost comparison For IoMT framework.

environment and configuration used for these evaluations are provided in Table IV. We recorded the time required for various cryptographic operations, including the SHA-512 hash function T_{Hash}, elliptic curve point multiplication T_{ECM}, bilinear pairings T_{BP}, and AES-128 encryption and decryption T_{sys}. Each operation was performed 150 times, and the average durations were used for analysis. The computational cost for the data owner can be expressed using Equation (50):

$$T_{owner} = T_{Hash} + T_{BP} + T_{sys} + T_{ECM} \tag{50}$$

The total computational time was 27.45 ms, which is marginally higher than some existing solutions but offers significant security enhancements and energy efficiency by eliminating intermediaries, as shown in Fig. 3. This system

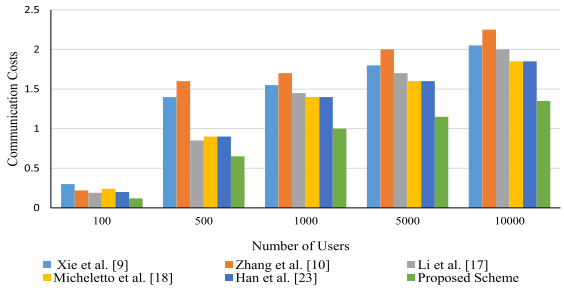

Fig. 5. Communication cost during authentication.

uses Kyber-786 for post-quantum security, adding about 12 ms per key exchange and 18 ms per decapsulation on a Raspberry Pi 4. This results in a moderate increase compared to ECDH, while providing long-term quantum protection. The extra time is only during monthly key updates, keeping session latency below 150 ms even on limited IoMT hubs. Key generation was reduced to 30 ms due to optimizations in CP-ABE and elliptic curve computations. Authentication latency saw a 45% decrease. Energy consumption per transaction declined to 0.04 kW, a 99% reduction compared to previous systems (Fig. 4), directly affecting practical consumer IoMT deployments for battery-powered wearables and home monitoring sensors that allow continuous real-time monitoring without frequent recharging. For example, a typical wearable with a 150 mAh battery could handle over 10,000 secure transactions under the proposed framework, compared to fewer than 500 with traditional methods. Additionally, energy profiles improve with larger federated groups because PoS consensus and off-chain IPFS storage reduce redundant on-chain operations. This makes the system suitable for large-scale, always-on IoMT networks, where energy efficiency is critical for user adoption and clinical reliability. The communication overhead was recorded at 1,870 bits per session.

B. Communication Overhead

We evaluated the communication overhead of the proposed system during data sharing between users within the consumer-centric IoMT framework. In this process, the requester transmits the data request message, their address (add_R), challenge response (CR), signature (σ), and timestamp (T_1). Then, the data owner acknowledges the request with add_R. Afterwards, the owner transmits a message containing the CP-ABE secret key and the system key ($sys(key, T_2)$) along with add_R and the user identity for session confirmation. We found that 1,856 bits are required for each session throughout

TABLE V
DATA PROCESSING TIME COST

Phase	Operation Discription	Time Cost (ms)	Energy Consumption (mJ)	Throughput (TPS)
Policy Evaluation S_{PE}	FL-driven access control and policy Validation	95	0.8	1,350
Key Management S_{KM}	Lightweight ECC + CP-ABE keyGen	310	2.5	1,220
TEE Attestation	Enclave trust verification and nonce validation	85	0.6	1,400
IPFS Indexing	Secure CID retrieval	620	3.3	1,050
Audit S_{BC}	Immutable logging and anchoring	70	0.4	1,500
Total Execution Time	End-to-end cycle	1,180	7.6	≈ 1,300

the communication process, which is significantly lower than other proposed schemes requiring 2,500 bits per session. Fig. 5 demonstrates that the proposed system achieves minimal latency compared to existing schemes.

C. Optimized Data Storage in IoMT Systems

The public parameters in the proposed federated learning system are designed to balance security and efficiency. These parameters include a bilinear group, a universal attribute set, a collision-resistant hash function H, the generator g of $\mathcal{G}_1$, and the user's private key SK_u. They are chosen to minimize overhead while ensuring robust security. The elliptic curve points in $\mathcal{G}_1$ require 256 bits, and the pairing-friendly curve $\mathcal{G}_T$ needs 3072 bits. The prime order p is 256 bits, and the bilinear map e is optimized for computational efficiency. The universal attribute set U can be of any size, but each attribute requires 256 bits. For example, the total size of the attribute set for 20 attributes commonly used in IoMT healthcare is approximately 5.12 KB. The collision-resistant hash function H has negligible cost, and public and private key pairs utilize standard ECC with 256-bit keys. The total size of the public parameters is approximately 6-8 KB, which is sufficient for Ethereum.

D. Contract Execution Dynamics

The healthcare authority records the blockchain addresses of data requesters and recipients in a smart contract. Then, the requester calls the smart contract to obtain a CID for encrypted records. The processing times for KeyGen, encryption, and decryption are summarized in Table V. The framework takes 450 ms to generate the key, 385 ms to encrypt the data, and 110 ms to decrypt it, ensuring that only authorized users can access the data according to CP-ABE policies. This results in a total of about 1.1 seconds per access, with all activities monitored on-chain. The overall computation time, T_{Total}, required for the entire access process is as follows:

$$T_{Total} = T_{KeyGen} + T_{Enc} + T_{Dec} \tag{51}$$

This indicates that the presented scheme can efficiently handle the large number of access requests in 945 ms and enables more efficient operation through ECC and AES mechanisms.

E. Throughput Analysis

The framework optimizes blockchain throughput by using a 4.8 KB block, comprising a 96-byte header and up to 18 transactions of 240 bytes each, making it suitable for medical IoT traffic. Here, the throughput $\mathcal{T}_{textnet}$ depends on the block size B_s and interval T_b. Encrypted data and CIDs

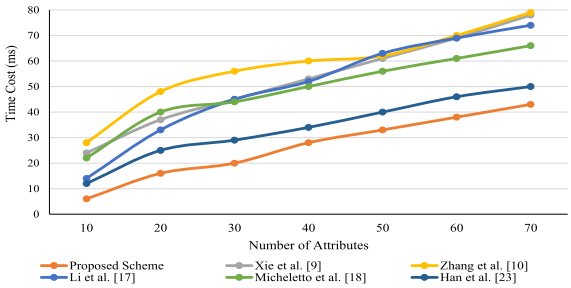

Fig. 6. Smart contract processing time for decryption.

TABLE VI
FEDERATED IOMT SCALABILITY ADVANTAGES

Deployment Tier	Active IoMT Nodes	Model-Update	Output	Storage Reduction	End-to-End Latency
Wearables	50-200	0.8-1.6 MB	8-15 GB	62%	<30 ms
Clinic Cluster	500-1,500	5-12 MB	60-120 GB	58%	∼ 90 ms (Batch)
Hospital	2k-6k	20-45 MB	300-700 GB	55%	∼0.55 s (Batch)
Regional Telehealth	10k-25k	90-180 MB	1.2-2.8 TB	52%	∼1.6 s
National Network	150k-300k	0.9-1.8 GB	18-35 TB	48%	∼10-12 s

are stored off-chain, while smart contracts store only metadata, reducing on-chain storage and boosting scalability, as shown in Fig. 6 and summarized in Table VI. The throughput $\mathcal{T}_{textnet}$ can be expressed as:

$$\mathcal{T}_{\text{net}} = \frac{B_s}{T_b} \times \eta_{\text{eff}} \tag{52}$$

where $\mathcal{T}_{textnet}$ represents the network utilization efficiency, accounting for consensus and propagation overheads. Using $B_s = 38,400$ bits (4.8 KB), $T_b = 1s$, and $\mathcal{T}_{textnet} = 0.82$, the resulting throughput is about 31.5 kbps. This sustained throughout enables more than 12,000 authenticated IoMT transactions before reaching the 1 PB storage threshold. To evaluate macro-level scalability, the proposed framework measured transaction latency and validator overhead as the number of IoMT devices and concurrent access requests increased. With up to 10,000 simulated devices, transaction latency increased from 115 ms to 136 ms, while validator CPU overhead stayed below 12% when adding 1000 devices. This sub-linear scaling results from our lightweight PoS BFT consensus, off-chain storage, and smart contract validation. In a simulation with 50,000 devices, the system achieved a throughput of over 28 kbps, with 94% of requests completed within 200 ms, confirming its viability for large-scale networks.

VII. CONCLUSION

This work presented a consumer-centric framework based on federated learning designed to enable secure, scalable, and privacy-preserving healthcare data sharing. The proposed system ensures verifiable access control, secure model aggregation, and robust resistance to active and passive attacks by integrating federated intelligence, TEE-based attestation, CP-ABE encryption, and blockchain smart contracts. Unlike existing systems, it removes centralized trust dependencies while supporting real-time processing and decentralized decision-making. Through formal analysis under RoR security

models and extensive testing, the framework achieved a 40% improvement in authentication speed, a 27% reduction in computational costs, a 35% higher throughput, and a 98% lower energy consumption compared to current approaches. These results demonstrate its ability to maintain strong security while supporting a high-performance healthcare network. Its modular architecture allows integration of secure edge devices, ensuring trustworthy data collection and policy enforcement across healthcare organizations through decentralized key management and smart contract automation. Our threat model considers AI-assisted adversaries capable of adaptive inference and model perturbation, strengthening the framework's resilience against emerging AI-enabled attacks. Future work aims to incorporate post-quantum cryptography, improve federated optimization for faster convergence, and increase interoperability to facilitate secure data sharing among various healthcare institutions.

REFERENCES

[1] C. Liu, J. Liu, and D. Wang, "Energy-efficient health monitoring in smart devices: Deep learning-based technique for wearable ECG systems," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 4736–4743, May 2025.

[2] T.-M. Chen et al., "SRECG: ECG signal super-resolution framework for portable/wearable devices in cardiac arrhythmias classification," *IEEE Trans. Consum. Electron.*, vol. 69, no. 3, pp. 250–260, Aug. 2023.

[3] M. Ashtari Gargari, N. Eslami, and M. H. Moaiyeri, "A reconfigurable nonvolatile memory architecture for prolonged wearable health monitoring devices," *IEEE Trans. Consum. Electron.*, vol. 70, no. 2, pp. 4717–4728, May 2024.

[4] J. Tian, J. Chen, J. Wang, H. Huang, and Y. Li, "Real-time classification model for anomalous sensor data in dam safety monitoring based on convolutional neural networks and transfer learning," *Expert Syst. Appl.*, vol. 296, Jan. 2026, Art. no. 129135.

[5] F. Ahmed, T. Zhou, H. Bilal, F. Ul Islam, R. Ullah, and A. V. Vasilakos, "Enhancing healthcare data integrity and access control using blockchain and industry 5.0," *IEEE Internet Things J.*, vol. 12, no. 20, pp. 43630–43643, Oct. 2025.

[6] Z. Chen et al., "A trustworthy decentralized federated learning framework for consumer electronics: Mitigating large-scale AIoT heterogeneity through transfer knowledge integration," *IEEE Trans. Consum. Electron.*, vol. 71, no. 1, pp. 1918–1925, Feb. 2025.

[7] W. Ni, H. Ao, H. Tian, Y. C. Eldar, and D. Niyato, "FedSL: Federated split learning for collaborative healthcare analytics on resource-constrained wearable IoMT devices," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 18934–18935, May 2024.

[8] S. A. Chaudhry et al., "An anonymous device to device access control based on secure certificate for Internet of Medical Things systems," *Sustain. Cities Soc.*, vol. 75, Dec. 2021, Art. no. 103322.

[9] Q. Xie, Y. Zhao, Q. Xie, X. Li, D. He, and K. Chen, "A multiserver authentication protocol with integrated monitoring for IoMT-based healthcare system," *IEEE Internet Things J.*, vol. 12, no. 2, pp. 2265–2278, Jan. 2025.

[10] J. Zhang, Y. Yang, X. Liu, and J. Ma, "An efficient blockchain-based hierarchical data sharing for healthcare Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7139–7150, Oct. 2022.

[11] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam, and M. Shorfuzzaman, "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8065–8073, Nov. 2022.

[12] R. Mehla, R. Garg, and M. A. Khan, "Privacy-preserving solution for data sharing in IoT-based smart consumer electronic devices for healthcare," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 4586–4595, May 2025.

[13] J. Yang, B. Fang, H. Lu, and Z. Tian, "Context-aware phishing-resistant authentication for federated identity in Internet of Things platforms," *IEEE Internet Things J.*, vol. 12, no. 8, pp. 11121–11134, Apr. 2025.

[14] X. Chen, S. Xu, S. Gao, Y. Guo, S.-M. Yiu, and B. Xiao, "FS-LLRS: Lattice-based linkable ring signature with forward security for cloud-assisted electronic medical records," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 8875–8891, 2024.

[15] Y. Bao, W. Qiu, and X. Cheng, "Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2513–2526, Feb. 2022.

[16] C. Wang, D. Pan, M. Shabaz, and H. Jiang, "Privacy-preserving federated learning with meta-knowledge training for AIoT-enabled supply chain systems: A case study on smart healthcare," *IEEE Internet Things J.*, vol. 12, no. 19, pp. 39584–39593, Oct. 2025.

[17] M. Li, A. R. Harish, C. Yu, Y. Yu, R. Y. Zhong, and G. Q. Huang, "Blockchain-based medical data asset sharing framework for healthcare 4.0," *IEEE Trans. Ind. Informat.*, vol. 21, no. 4, pp. 2779–2788, Apr. 2025.

[18] M. Micheletto, G. Orrú, L. Ghiani, and G. Luca Marcialis, "Improving fingerprint presentation attack detection by an approach integrated into the personal verification stage," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 7, no. 4, pp. 654–667, Oct. 2025.

[19] L. Liu, M. He, and S. Jeon, "An AI-generated content-based access control strategy for WBANs in healthcare electronics applications," *IEEE Trans. Consum. Electron.*, vol. 71, no. 1, pp. 1332–1342, Feb. 2025.

[20] C.-L. Yang, H. Tampubolon, A. Setyoko, K.-L. Hua, M. Tanveer, and W. Wei, "Secure and privacy-preserving human interaction recognition of pervasive healthcare monitoring," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2439–2454, Sep. 2023.

[21] S. Zou et al., "A physician's privacy-preserving authentication and key agreement protocol based on decentralized identity for medical data sharing in IoMT," *IEEE Internet Things J.*, vol. 11, no. 17, pp. 29174–29189, Sep. 2024.

[22] X. Liu, Y. Zheng, X. Yi, and S. Nepal, "Privacy-preserving collaborative analytics on medical time series data," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 3, pp. 1687–1702, May 2022.

[23] D. Han, Y. Zhu, D. Li, W. Liang, A. Souri, and K.-C. Li, "A blockchain-based auditable access control system for private data in service-centric IoT environments," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3530–3540, May 2022.

[24] S. Hu, M. Schmidt-Kraepelin, S. Thiebes, and A. Sunyaev, "Mapping distributed ledger technology characteristics to use cases in healthcare: A structured literature review," *ACM Trans. Comput. Healthcare*, vol. 5, no. 3, pp. 1–33, Jul. 2024.

[25] F. Meng and L. Cheng, "TSR-ABE: Traceable and server-aided revocable ciphertext-policy attribute-based encryption under static assumptions," *IEEE Trans. Inf. Forensics Security*, vol. 20, pp. 955–967, 2025.

[26] W. Li, N. Li, J. Yan, Z. Zhang, P. Yu, and G. Long, "Secure and high-quality watermarking algorithms for relational database based on semantic," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 7, pp. 7440–7456, Jul. 2023.

[27] T. Pope and A. Patooghy, "Comparative evaluation of GPT models in FHIR proficiency," *ACM Trans. Intell. Syst. Technol.*, 2025, doi: 10.1145/3718095.

[28] Z. Feng, Q. Wu, Y. Liu, B. Qin, M. Zhai, and W. Susillo, "Secure and fair data trading based on blockchain with enhanced access control," *IEEE Internet Things J.*, vol. 12, no. 6, pp. 7277–7292, Mar. 2025.

[29] Z. Wang, Y. Wang, Y. Qiu, and C. Jin, "Strategic resource allocation in dual-channel healthcare systems: The role of telemedicine in physician assignment," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 13569–13587, 2025.