Zero-Trust Privacy Enforcement and Threat-Aware Monitoring in Consumer Healthcare Systems

Usama Arshad, Abdallah Tubaishat, Fawaz Alarfaj, Zahid Halim, Sajid Anwar, Hisham Alfuhaid, Muhammad Waqas

***Abstract*—Consumer healthcare applications increasingly rely on AI-driven monitoring, IoMT devices, and continuous data collection, creating critical challenges involving privacy, unauthorized access, excessive surveillance, and secure healthcare-data management. This paper proposes a zero-trust, threat-aware architecture that integrates context-aware computer vision, blockchain-based decentralized access control, and zero-knowledge proofs for privacy-preserving healthcare monitoring. The framework filters incoming streams to retain only healthcare-relevant events; encrypted records remain off-chain, whereas hashes, access decisions, consent states, and audit logs are recorded on a consortium blockchain. Zero-knowledge proofs support confidential authorization, whereas reputation-aware trust management and blockchain-enabled incentives promote reliable participation and discourage malicious behavior. Clinical events, including falls and abnormal postures, are detected through a CNN-LSTM model, while cybersecurity threats are identified through policy evaluation, transaction validation, and behavioral monitoring. Across 30 independent runs under varied workloads and attack conditions, the proposed architecture achieved a 54.5% reduction in data-access time, a 52.4% reduction in breach-response time, and a 78.1% reduction in privacy and integrity incidents compared with a conventional architecture. Simulated participation increased by 43.7% after incentive deployment across 12 monthly scenarios. These results indicate improved efficiency, privacy preservation, and threat responsiveness for AI-enabled consumer healthcare monitoring.**

***Index Terms*—Computer Vision, Zero-Trust Security, Blockchain, Zero-Knowledge Proofs, Healthcare Monitoring, Privacy Preservation**

I. Introduction

Artificial intelligence (AI), the Internet of Medical Things (IoMT), and computer vision are increasingly used in healthcare monitoring and assisted-living environments [1]. These technologies support continuous observation, emergency response, fall detection, and automated healthcare services [2]. However, large-scale sensing and persistent monitoring introduce concerns involving privacy leakage, unauthorized access, excessive surveillance, and secure healthcare-data management [3]. Smartphone and connected-device ecosystems may further increase privacy exposure and discontinuance risks [4]. Wearable healthcare devices also expand the attack surface of consumer monitoring systems [5]. Recent IoT security studies have explored physical unclonable functions for device authentication [6], RFID-enabled distributed services [7], cyber-physical coordination under dynamic operating conditions [8], human-centered reliability in IoT-enabled systems [9], encrypted protection for medical IoT data [10], and resilience against denial-of-service attacks [11]. Traditional healthcare architectures commonly rely on centralized storage and static role-based access control, creating risks of insider misuse, data tampering, and single points of failure [12]. Continuous vision-based monitoring may additionally capture identities, domestic activities, and behavioral patterns beyond the information required for healthcare intervention [13]. Existing approaches often address monitoring accuracy, device security, privacy protection, access control, or system reliability independently, with limited integration of contextual filtering, confidential authorization, decentralized auditing, and real-time threat monitoring [14].

Corresponding authors: Zahid Halim, Sajid Anwar

Usama Arshad is with FAST National University, Islamabad, Pakistan. (e-mail: usamajanjua9@gmail.com)

Abdallah Tubaishat is with the College of Technological Innovation, Zayed University, UAE. (e-mail: abdallah.tubaishat@zu.ac.ae)

Fawaz Alarfaj is with the MIS Department, Business School, King Faisal University, Hofuf, Saudi Arabia. (e-mail: falarfaj@kfu.edu.sa)

Zahid Halim is with the Machine Intelligence and Affective Systems Laboratory, National Yunlin University of Science and Technology, 123 University Road, Section 3, Douliu, Yunlin 64002, Taiwan. (e-mail: zahidh@yuntech.edu.tw)

Sajid Anwar is with the Institute of Management Sciences, Peshawar, Pakistan. (e-mail: sajid.anwar@imsciences.edu.pk)

Hisham Alfuhaid is with the Department of Computer Science, King Khalid University, Abha 62521, Saudi Arabia.

Muhammad Waqas is with the Centre for Sustainable Cyber Security, Faculty of Engineering and Science, University of Greenwich, SE10 9LS, London, UK. (e-mail: muhammad.waqas@gre.ac.uk)

A. Motivation

AI-enabled consumer healthcare systems require an architecture that minimizes unnecessary data collection while supporting secure authorization, confidential verification, and timely threat response. To address these requirements, this paper proposes a zero-trust, threat-aware framework integrating context-aware computer vision, consortium-blockchain access control, ZKP-based authorization, reputation-aware trust management, and incentive-driven participation. Encrypted healthcare records remain off-chain, whereas hashes, access decisions, consent states, and audit logs are recorded on-chain.

B. Research Contributions

The major contributions of this work are summarized as follows:

- A zero-trust healthcare architecture integrating contextual computer vision, blockchain-based authorization, and threat-aware monitoring is proposed to minimize unnecessary data exposure.

TABLE I
RECENT RELEVANT STUDIES AND THEIR KEY LIMITATIONS

Ref.	Model/Study	Tools/Techniques	Experiment	Contribution	Limitation
[12]	Privacy-Preserving AI in Healthcare	Federated learning, differential privacy, SMPC, homomorphic encryption	Review of privacy-preserving AI methods for healthcare applications	Presents major techniques for secure distributed healthcare analytics	Review-based work with limited real-time and deployment-level evaluation
[15]	Personal Health-Data Sharing Factors	Privacy calculus, planned behavior theory, SEM	Cross-sectional survey of 2,060 patients in China	Identifies privacy, trust, and behavioral factors affecting data-sharing willingness	Based on self-reported responses and a region-specific participant group
[16]	Information-Security Culture and Unauthorized Access	Survey, PLS-SEM	Survey of 527 nursing employees in Slovenia	Examines how organizational security culture influences unauthorized healthcare-data access	Limited generalizability due to profession-specific and country-specific sampling
[17]	ZeroMedChain	Blockchain, ZKP, proof of work, Layer 2	Simulation-based comparison with conventional blockchain approaches	Supports decentralized identity management and privacy-preserving healthcare authorization	Lacks real-world deployment and comprehensive evaluation under diverse attacks
[14]	Machine Learning for IoT-Based Medical Data Processing	Machine learning, deep learning, IoT, distributed computing	Review of IoT-enabled healthcare-data processing studies	Summarizes machine-learning methods for monitoring, diagnosis, and medical-data analysis	Provides no original experimentation or integrated privacy and threat evaluation
[18]	Blockchain and Reputation-Based Healthcare Incentives	PBFT, blockchain, reputation assessment, incentives	Simulation of a blockchain-enabled healthcare-service environment	Encourages trustworthy participation through reputation and incentive mechanisms	Validation is mainly simulation-based and excludes heterogeneous real-world conditions
[19]	Privacy-Preserving Medical-Image Exchange	Hyperchaotic neural networks, DNA encoding, image encryption	Experimental evaluation of encrypted online medical-image exchange	Protects medical images against unauthorized disclosure during transmission	Focuses on image protection rather than access control, auditing, or threat-aware monitoring

- A ZKP-based mechanism verifies healthcare-record integrity and requester authorization without disclosing confidential credentials or healthcare attributes.
- A reputation and incentive mechanism promotes policy-compliant participation while penalizing invalid, anomalous, or malicious contributions.
- Across 30 independently seeded runs, the framework reduced data-access time by 54.5%, breach-response time by 52.4%, and privacy and integrity incidents by 78.1%, while simulated participation increased by 43.7%.

C. Organization of the Paper

Section II reviews related healthcare-monitoring and privacy-preserving approaches. Section III presents the proposed architecture, while Section IV describes its implementation and algorithms. Section V reports the experimental evaluation and comparative results. Finally, Section VI concludes the paper and outlines future research directions.

II. RELATED WORK

Privacy-preserving artificial intelligence is increasingly important in healthcare because monitoring and learning systems process sensitive clinical and behavioral data. Khalid et al. reviewed federated learning, differential privacy, secure multiparty computation, and homomorphic encryption for protecting healthcare analytics [12]. Shi et al. showed that privacy, trust, and perceived benefits affect patients' willingness to share health data [15], while Mikuletič et al. linked organizational security culture with unauthorized healthcare-data access [16]. Blockchain and zero-knowledge proofs have also been explored for decentralized healthcare authorization. ZeroMedChain combines Layer-2 blockchain processing with ZKP-based identity and access management [17], although its evaluation remains simulation-based. Aminizadeh et al. reviewed machine-learning and deep-learning methods for medical-data processing in distributed IoT environments [14], but did not provide an integrated privacy-enforcement and threat-response framework. Reputation and incentive mechanisms can strengthen trust in decentralized healthcare services. Liu et al. proposed a blockchain-based reputation and incentive model for reliable participation [18]. Deng et al. developed a privacy-preserving medical-image exchange scheme using hyperchaotic neural networks and DNA encoding [19]; however, it focuses on image protection rather than access control, contextual filtering, or continuous threat monitoring. IoT-based monitoring supports remote observation and continuous healthcare-data collection [20]. Related human-centered systems show that physiological information can support safety-critical decision-making [13], while risk-aware planning demonstrates adaptive responses under changing conditions [21]. Privacy self-management and notice-and-choice mechanisms have also been examined for limiting surveillance risks, although their effectiveness depends on meaningful user control and enforceable protections [22]. Surveillance practices and privacy risks may also evolve together, reducing the effectiveness of static privacy mechanisms [23]. Edge–cloud AI and digital-twin architectures demonstrate distributed sensing and computation across heterogeneous resources [24], but do not inherently provide healthcare-specific privacy enforcement. Overall, existing studies address privacy-preserving

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2026.3723896

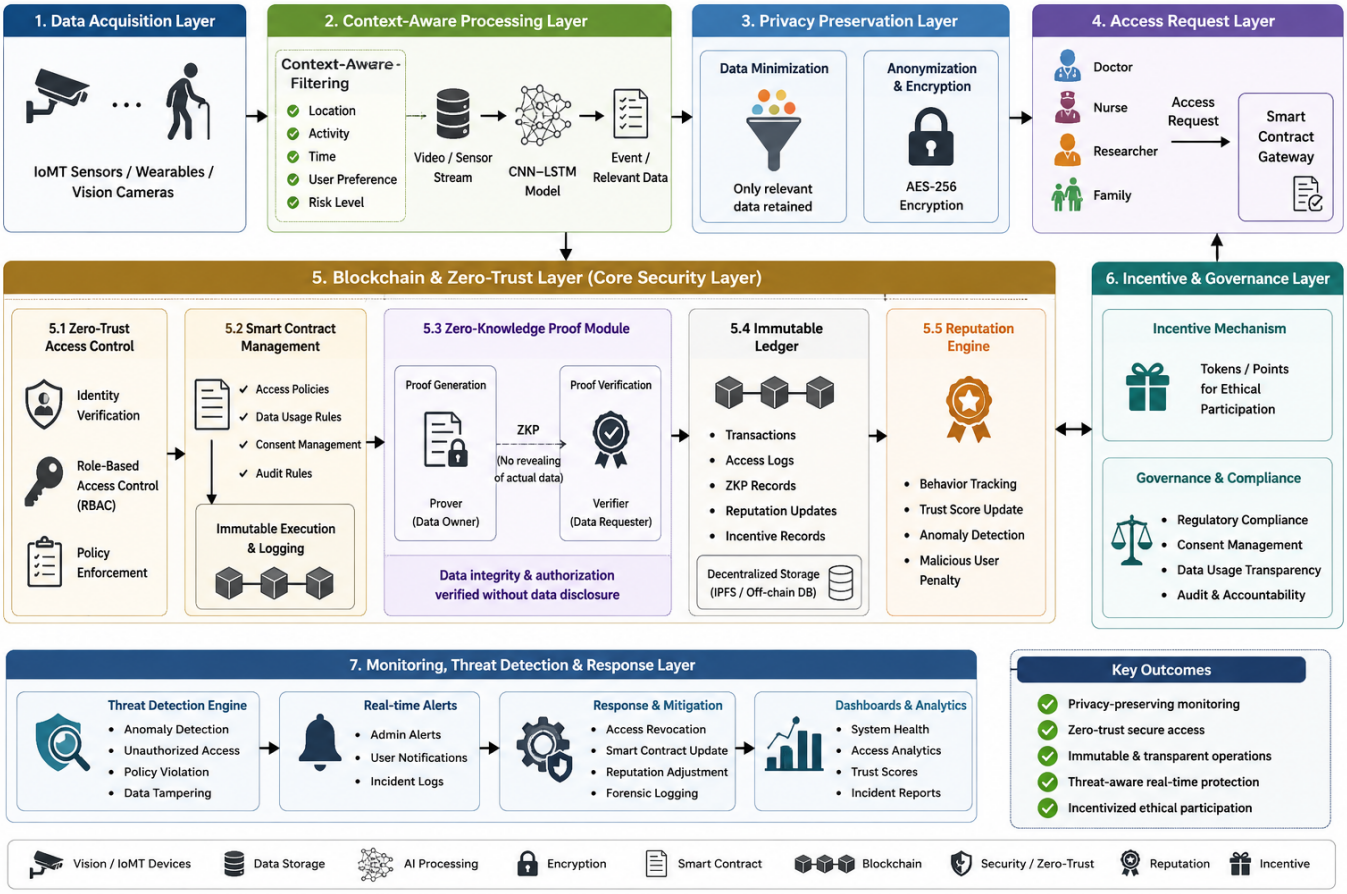

Fig. 1. Layered zero-trust privacy enforcement architecture integrating context-aware computer vision, blockchain-based decentralized access control, Zero-Knowledge Proof verification, reputation-aware trust management, incentive-driven participation, and threat-aware healthcare monitoring.

learning, data sharing, unauthorized access, blockchain authorization, incentives, or image protection separately. Few integrate contextual healthcare-event filtering, encrypted off-chain storage, blockchain auditing, ZKP authorization, reputation-aware participation, and real-time threat monitoring within one zero-trust architecture. The proposed framework addresses this gap.

III. Proposed Architecture

The proposed framework introduces a zero-trust, threat-aware healthcare monitoring architecture integrating context-aware computer vision, blockchain-based access control, zero-knowledge proof (ZKP) verification, reputation management, and incentive-driven participation. Unlike traditional centralized systems, the framework processes only contextually relevant healthcare events while enforcing decentralized authorization and cryptographic security. The overall architecture is illustrated in Fig. 1.

A. Overview

IoMT devices, wearable sensors, and video cameras continuously collect healthcare-related data streams. Instead of retaining all captured information, the proposed framework applies context-aware filtering to identify security-critical and healthcare-relevant events. Raw video, sensor streams, and encrypted healthcare records remain in authorized off-chain storage, whereas record hashes, access decisions, consent states, reputation updates, and audit logs are recorded on a consortium blockchain. ZKPs validate authorization without revealing confidential attributes, while smart contracts automate access control and incentive distribution.

Let x denote the public statement, w the confidential witness, and π the generated proof. The ZKP interaction is represented as

$$\pi \leftarrow \mathrm{Prove}(pk, x, w), \tag{1}$$

where pk denotes the proving key. The verifier evaluates

$$\mathrm{Verify}(vk, x, \pi) \in \{0, 1\}, \tag{2}$$

where vk is the verification key. In the proposed framework, x contains the encrypted-record hash, access-policy identifier, and requested operation, while w contains confidential credentials or authorization attributes.

B. Context-Aware Vision and Blockchain Security

To reduce unnecessary surveillance exposure, the framework performs context-aware filtering before forwarding event metadata to the blockchain layer. Let $\theta(x)$ denote the contextual

relevance score of healthcare input x, and let τ represent the minimum relevance threshold:

$$C(x) = \begin{cases} 1, & \theta(x) \geq \tau, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

Here, $C(x) = 1$ identifies a healthcare-relevant event. Only the encrypted event record is retained off-chain, while its hash and associated authorization metadata are submitted to the blockchain.

The framework employs a consortium blockchain to balance decentralization, confidentiality, and regulatory control:

$$B_{\text{type}}(a, c) = \begin{cases} \text{public}, & a = \text{open},\ c = \text{low}, \\ \text{private}, & a = \text{restricted},\ c = \text{high}, \\ \text{consortium}, & a = \text{regulated},\ c = \text{moderate}. \end{cases} \tag{4}$$

where a denotes the access-control requirement and c represents the confidentiality level. Healthcare records are protected as

$$D_e = \text{Encrypt}(D, K), \qquad h_D = H(D_e), \tag{5}$$

where D_e is retained off-chain and h_D is recorded on-chain for integrity verification.

C. ZKP Verification and Access Control

The proposed framework uses ZKPs to verify healthcare-record integrity and requester authorization without disclosing confidential information. The authorization decision is defined as

$$A_d = \begin{cases} \text{grant}, & \text{Verify}(vk, x, \pi) = 1 \wedge r_u \in P_d, \\ \text{deny}, & \text{otherwise}, \end{cases} \tag{6}$$

where r_u denotes the requesting user's role and P_d represents the permissions associated with healthcare resource d. The ZKP-verification delay contributes to the access-time measurements reported in Section V.

D. Trust, Incentive, and Threat Management

The framework balances privacy preservation, trustworthy participation, and decentralized enforcement under dynamic monitoring conditions. Policy-compliant actions receive incentives according to

$$I_u = \begin{cases} \gamma, & a_u = \text{valid}, \\ 0, & \text{otherwise}, \end{cases} \tag{7}$$

where γ denotes the assigned incentive value. User reputation is updated as

$$R_u = \frac{1}{n} \sum_{i=1}^{n} q_i, \tag{8}$$

where q_i represents the assessed quality of the i-th healthcare-data contribution.

The threat model includes unauthorized access, insider misuse, replay attacks, malicious nodes, anomalous transactions, and privacy leakage. Threat status is determined as

$$\text{Threat}(A) = \begin{cases} 1, & A \in \mathcal{A}_{\text{malicious}}, \\ 0, & \text{otherwise}, \end{cases} \tag{9}$$

where $\mathcal{A}_{\text{malicious}}$ contains predefined policy violations, replay attempts, invalid proofs, and anomalous blockchain transactions. These conditions are used in the threat scenarios evaluated in Section V.

Blockchain transactions are verified through

$$\text{VerifyTx}(t) = \begin{cases} \text{true}, & H(t) = h_{\text{expected}}, \\ \text{false}, & \text{otherwise}, \end{cases} \tag{10}$$

thereby supporting tamper-resistant auditability, integrity preservation, and continuous zero-trust enforcement.

IV. Implementation Details

The framework was implemented using blockchain, computer vision, zero-knowledge proof (ZKP) verification, and deep learning. Smart contracts were developed in Remix IDE, while simulations and machine-learning experiments were conducted in Python on a 12th-generation Intel Core i7 system with 16 GB RAM. Raw healthcare records and video streams were stored off-chain, whereas hashes, authorization decisions, consent states, reputation updates, and audit logs were recorded on the consortium blockchain.

The UR Fall Detection Dataset [25] was used for fall and posture analysis. HeightWidthRatio, MajorMinorRatio, BoundingBoxOccupancy, MaxStdXZ, H, and D were normalized, while temporal height and distance variations were generated to improve abnormal-event sensitivity.

A. CNN-LSTM-Based Healthcare Event Detection

A CNN-LSTM model was used to capture spatial posture features and temporal activity patterns. The CNN representation is

$$F_{\text{cnn}} = \text{Conv}(X, W) + b, \tag{11}$$

and the temporal representation is

$$h_t = \text{LSTM}(F_{\text{cnn}}, h_{t-1}). \tag{12}$$

The output probabilities are

$$Y = \text{Softmax}(W_h h_t + b_h), \tag{13}$$

where Y represents fall, abnormal-posture, and normal-activity probabilities. The CNN-LSTM detects clinical events, while cybersecurity threats are identified separately through policy evaluation, transaction validation, blockchain-log analysis, and behavioral monitoring.

B. Training and Statistical Evaluation Protocol

The dataset was divided into 70% training, 15% validation, and 15% testing subsets. Training used Adam with a learning rate of 0.001, batch size 32, and 50 epochs. Accuracy, precision, recall, and F1-score were used for evaluation.

The baseline and proposed configurations were each executed 30 times using seeds 42–71 under identical workloads, user roles, traffic levels, and threat scenarios. Performance comparisons were based on mean values across the 30 runs. Paired differences were tested for normality using Shapiro–Wilk; paired t-tests were used for normal data and Wilcoxon signed-rank tests otherwise. Holm–Bonferroni correction was applied with $\alpha = 0.05$, and effect sizes were measured using paired Cohen's d or rank-biserial correlation.

ZKP proof generation and verification were performed for each protected access request, and their delay was included in data-access time. Blockchain latency included transaction validation, policy execution, and audit-log recording.

C. Privacy-Preserving Data Management

Algorithm 1 describes encrypted storage, confidential authorization, blockchain logging, and reputation updating.

Algorithm 1 Privacy-Preserving Data Management

Require: Record D, key K, requester u, role r_u, policy P, proving key pk, verification key vk, blockchain B
Ensure: D_e, π, T_x, A_d, R_u, I_u

$D_e \leftarrow \mathrm{Encrypt}(D, K)$, $h_D \leftarrow H(D_e)$
$x \leftarrow (h_D, P, \mathrm{request})$, $w \leftarrow (r_u, \mathrm{credential}_u)$
$\pi \leftarrow \mathrm{Prove}(pk, x, w)$
$R_u \leftarrow B.\mathrm{GetReputation}(u)$
if $\mathrm{Verify}(vk, x, \pi) = 1 \wedge r_u \in P$ **then**
  $A_d \leftarrow \mathrm{grant}$
  Update R_u and assign I_u
else
  $A_d \leftarrow \mathrm{deny}$, $I_u \leftarrow 0$
  Deny access and record the failed request
end if
$T_x \leftarrow B.\mathrm{Store}(h_D, H(\pi), u, A_d)$
return $(D_e, \pi, T_x, A_d, R_u, I_u)$

D. Secure Drug Distribution and Reputation Management

Algorithm 2 validates shipment records, updates supplier reputation, and triggers dispute handling for invalid transactions.

V. Simulations and Results Discussion

The proposed framework was evaluated under varying workloads, user roles, traffic levels, and threat scenarios. Baseline and proposed configurations were each executed 30 times using seeds 42–71 under identical paired conditions. Reported values are means across all runs, and statistical comparisons followed the procedure in Section IV with $\alpha = 0.05$.

Algorithm 2 Secure Drug Distribution

Require: Shipment S, supplier s, metadata M_s, policy P_s, blockchain B
Ensure: Validation V_s, transaction T_s, reputation R_s, dispute flag D_s

$h_S \leftarrow H(S, M_s)$
$R_s \leftarrow B.\mathrm{GetReputation}(s)$
$C_s \leftarrow B.\mathrm{Validate}(h_S, s, P_s)$
if $C_s = \mathrm{valid}$ **then**
  $V_s \leftarrow \mathrm{valid}$, $T_s \leftarrow B.\mathrm{Store}(h_S, s)$
  Increase R_s and set $D_s \leftarrow 0$
else
  $V_s \leftarrow \mathrm{invalid}$, $T_s \leftarrow \varnothing$
  Decrease R_s and set $D_s \leftarrow 1$
  Trigger dispute-handling procedure
end if
return (V_s, T_s, R_s, D_s)

TABLE II
CNN-LSTM Healthcare-Event Classification Performance

Metric	Mean (%)
Accuracy	92.1
Precision	91.3
Recall	90.7
F1-score	91.0

A. Performance Evaluation

The framework was compared with a conventional centralized architecture using direct database access, static role-based authorization, and centralized logging. Fig. 2 compares access delay, breach-response time, and privacy incidents.

The proposed architecture reduced healthcare data-access time by 54.5% and breach-response time by 52.4% compared with the conventional architecture. These improvements resulted from contextual filtering, decentralized authorization, and cryptographic verification.

B. CNN-LSTM Classification Performance

Table II presents the mean CNN-LSTM performance for healthcare-event classification across the repeated runs.

The model captures spatial posture features and temporal activity patterns for fall and abnormal-posture detection. Cybersecurity threats were evaluated separately through authorization failures, replay attempts, policy violations, malicious transactions, and blockchain-log anomalies.

C. Participation and Reputation Analysis

Fig. 3 compares healthcare data-sharing activity before and after incentive deployment.

The proposed framework increased simulated participation by 43.7% across the 12 monthly scenarios, indicating that reputation and incentive mechanisms improved engagement while discouraging invalid contributions.

The relationship between reputation and integrity incidents is shown in Fig. 4.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2026.3723896

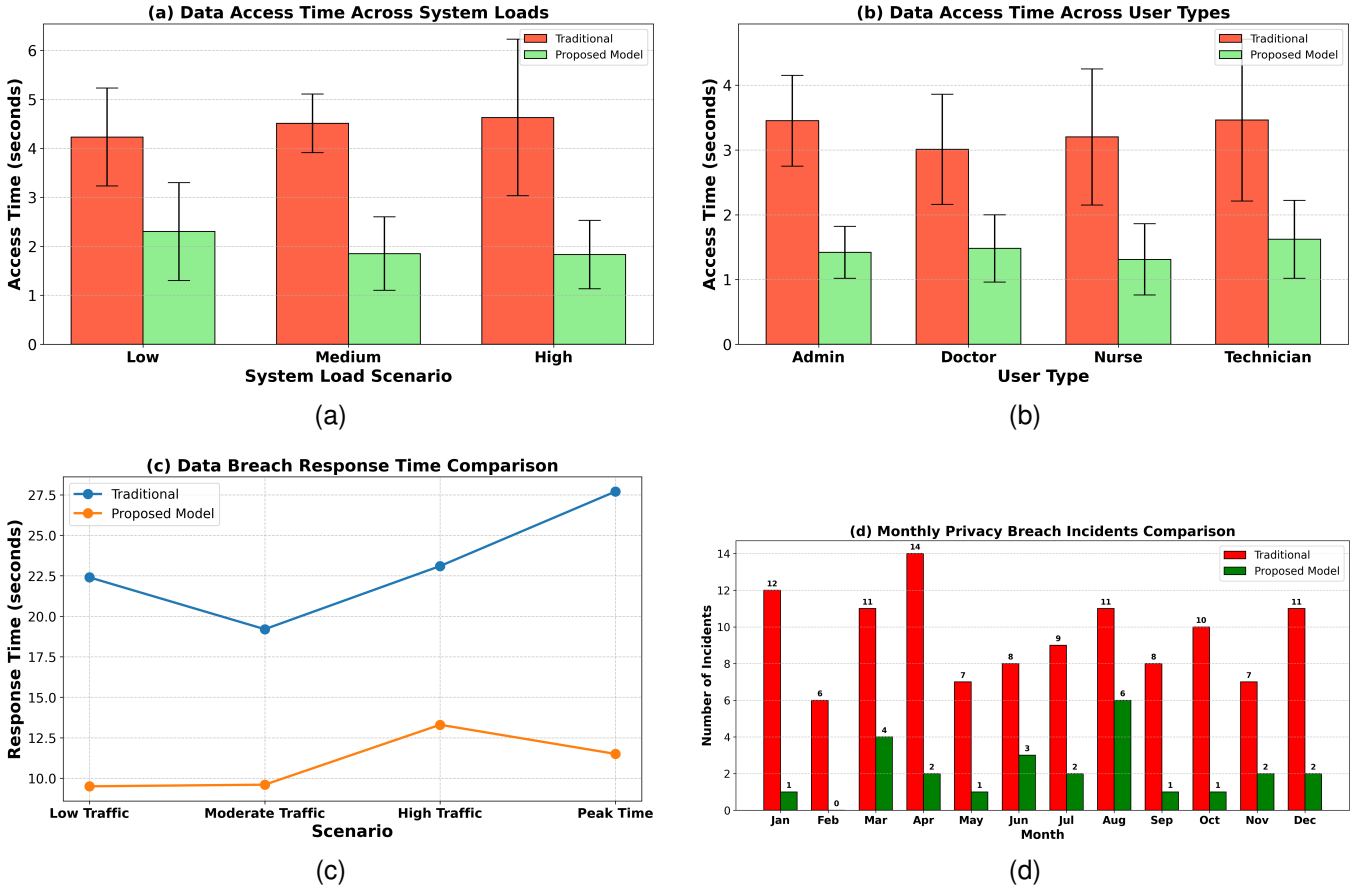

Fig. 2. Comparative performance of the traditional and proposed healthcare architectures: (a) data-access time under low, medium, and high workloads; (b) access delay for administrator, doctor, nurse, and technician roles; (c) breach-response time under low, moderate, high, and peak traffic; and (d) monthly privacy incidents. Values are averaged over 30 seeded runs, error bars denote one standard deviation, and the proposed framework consistently reduces access delay, response time, and privacy incidents.

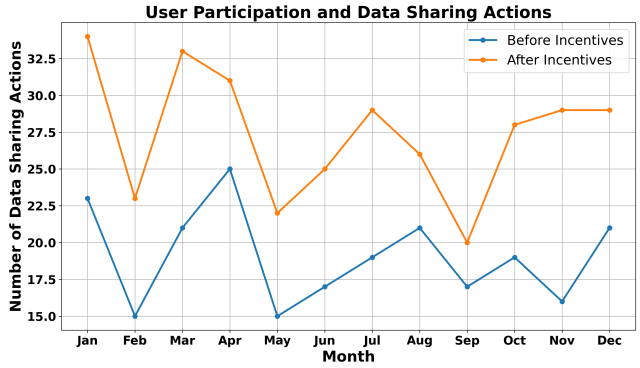

Fig. 3. Monthly healthcare data-sharing activity before and after incentive deployment, averaged over 30 seeded runs. The post-incentive condition shows greater participation across most months, indicating improved policy-compliant data sharing.

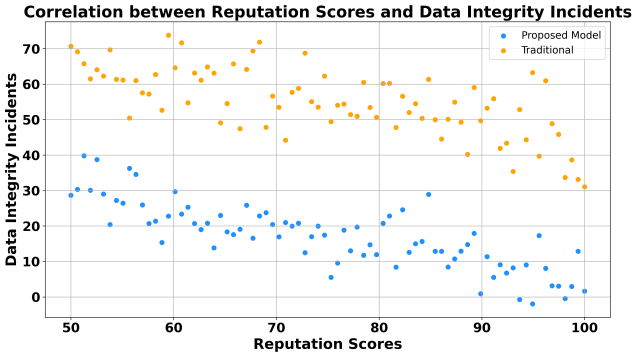

Fig. 4. Relationship between user reputation scores and healthcare-data integrity incidents across repeated simulations. Higher reputation scores are associated with fewer integrity incidents in the proposed framework than in the traditional architecture.

Higher reputation scores were associated with fewer integrity incidents. Overall, the proposed framework reduced healthcare privacy and integrity incidents by 78.1%, indicating improved behavior-aware monitoring and decentralized trust enforcement.

D. Comparative Analysis and Discussion

The results indicate that contextual filtering, blockchain-based authorization, ZKP verification, and reputation-aware participation improve healthcare-event processing, privacy enforcement, and threat response. Across 30 seeded runs, the framework reduced data-access time by 54.5%, breach-response time by 52.4%, and privacy and integrity incidents

by 78.1%, while simulated participation increased by 43.7%. These findings demonstrate improved efficiency, privacy, and security under dynamic healthcare-monitoring conditions.

VI. Conclusion

The proposed zero-trust healthcare framework improves privacy preservation, operational efficiency, and threat responsiveness compared with a conventional centralized architecture. Across 30 independently seeded runs, the framework reduced data-access time by 54.5%, breach-response time by 52.4%, and privacy and integrity incidents by 78.1%, while simulated participation increased by 43.7% across 12 monthly scenarios. These outcomes result from contextual event filtering, blockchain-based authorization, zero-knowledge proof verification, and reputation-aware trust management. The architecture also limits unnecessary surveillance by retaining encrypted healthcare records off-chain and recording hashes, authorization decisions, consent states, and audit logs on-chain. Overall, the findings support a secure and privacy-aware approach for AI-enabled healthcare monitoring. Future work will investigate real-world deployment, federated edge learning, predictive threat analytics, and lightweight blockchain optimization for resource-constrained IoMT environments.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research and Graduate Studies at King Khalid University, KSA, for funding this work through the Small Research Group under grant number RGP.1/39/46.

References

[1] A. Gupta and A. Singh, "Healthcare 4.0: Recent advancements and futuristic research directions," *Wireless Personal Communications*, vol. 129, no. 2, pp. 933–952, 2023.

[2] O. Ali, W. Abdelbaki, A. Shrestha, E. Elbasi, M. A. A. Alryalat, and Y. K. Dwivedi, "A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities," *Journal of Innovation & Knowledge*, vol. 8, no. 1, p. 100333, 2023.

[3] M. Mijwil, M. Aljanabi, and A. H. Ali, "ChatGPT: Exploring the role of cybersecurity in the protection of medical information," *Mesopotamian Journal of Cybersecurity*, vol. 2023, pp. 18–21, 2023.

[4] H. Pang and Y. Ruan, "Can information and communication overload influence smartphone app users' social network exhaustion, privacy invasion and discontinuance intention? a cognition–affect–conation approach," *Journal of Retailing and Consumer Services*, vol. 73, p. 103378, 2023.

[5] V. Natalucci, F. Marmondi, M. Biraghi, and M. Bonato, "The effectiveness of wearable devices in non-communicable diseases to manage physical activity and nutrition: Where we are?" *Nutrients*, vol. 15, no. 4, p. 913, 2023.

[6] W. Zhang, S. Wang, P. Wang, Q. Fu, and X. Li, "Design of accelerometer-based PUF for internet of things security," *IEEE Sensors Journal*, p. 1, 2025.

[7] J. Hu, H. Jiang, D. Liu, Z. Xiao, S. Dustdar *et al.*, "A wireless self-service system for library using commodity RFID devices," *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 4998–5010, 2024.

[8] Y. Xia, R. Yu, Y. Li, A. P. Zhao, Z. Liu, L. Shi *et al.*, "Cyber-physical-social insights into barriers to transactive energy market development in power systems," *Cyber-Physical Energy Systems*, 2026.

[9] Y. Lu, S. Wang, R. Chen, H. Dui, J. Gao, and C. Zhang, "Human-centric reliability prediction for IoT-enabled human–machine systems considering component hierarchical dependency," *International Journal of Human–Computer Interaction*, pp. 1–26, 2026.

[10] J. Jin, M. Wu, A. Ouyang, K. Li, and C. Chen, "A novel dynamic hill cipher and its applications in medical IoT," *IEEE Internet of Things Journal*, vol. 12, no. 10, pp. 14 297–14 308, 2025.

[11] F. Ding, Z. Liu, Y. Wang, J. Liu, C. Wei, A. Nguyen *et al.*, "Intelligent event-triggered lane-keeping security control for autonomous vehicles under DoS attacks," *IEEE Transactions on Fuzzy Systems*, pp. 1–13, 2025.

[12] N. Khalid, A. Qayyum, M. Bilal, A. Al-Fuqaha, and J. Qadir, "Privacy-preserving artificial intelligence in healthcare: Techniques and applications," *Computers in Biology and Medicine*, p. 106848, 2023.

[13] X. Zhang, H. Zheng, J. Li, Z. Xie, H. Sun, and H. Wang, "Safety decision-making for autonomous vehicles integrating passenger physiological states by fNIRS," *Cyborg and Bionic Systems*, vol. 6, p. 0205, 2025.

[14] S. Aminizadeh, A. Heidari, S. Toumaj, M. Darbandi, N. J. Navimipour, M. Rezaei, S. Talebi, P. Azad, and M. Unal, "The applications of machine learning techniques in medical data processing based on distributed computing and the internet of things," *Computer Methods and Programs in Biomedicine*, p. 107745, 2023.

[15] J. Shi, R. Yuan, X. Yan, M. Wang, J. Qiu, X. Ji, and G. Yu, "Factors influencing the sharing of personal health data based on the integrated theory of privacy calculus and theory of planned behaviors framework: Results of a cross-sectional study of chinese patients in the yangtze river delta," *Journal of Medical Internet Research*, vol. 25, p. e46562, 2023.

[16] S. Mikuletič, S. Vrhovec, B. Skela-Savič, and B. Žvanut, "Security and privacy-oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees," *Computers & Security*, vol. 136, p. 103489, 2024.

[17] P. Verma, V. Tripathi, and B. Pant, "ZeroMedChain: Layer 2 security and zero-knowledge proof integration for decentralized identity and access management in healthcare," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2024, pp. 1023–1027.

[18] Y. Liu, Z. Liu, Q. Zhang, J. Su, Z. Cai, and X. Li, "Blockchain and trusted reputation assessment-based incentive mechanism for healthcare services," *Future Generation Computer Systems*, vol. 154, pp. 59–71, 2024.

[19] X. Deng, S. Ding, H. Lin, L. Jiang, H. Sun *et al.*, "Privacy-preserving online medical image exchange via hyperchaotic memristive neural networks and DNA encoding," *Neurocomputing*, vol. 653, p. 131132, 2025.

[20] K. Sangeethalakshmi, U. Preethi, S. Pavithra *et al.*, "Patient health monitoring system using IoT," *Materials Today: Proceedings*, vol. 80, pp. 2228–2231, 2023.

[21] J. Zhao, J. Du, B. Zhu, J. Han, D. Song *et al.*, "Cognitive risk-aware hierarchical trajectory planning for adaptive regulation of driving caution," *IEEE Transactions on Intelligent Transportation Systems*, vol. 27, no. 2, pp. 2331–2349, 2026.

[22] R. Sprague, "Privacy self-management: A strategy to protect worker privacy from excessive employer surveillance in light of scant legal protections," *American Business Law Journal*, vol. 60, no. 4, pp. 793–836, 2023.

[23] A. B. Whitford and J. Yates, "Surveillance and privacy as coevolving disruptions: Reflections on "notice and choice"," *Policy Design and Practice*, vol. 6, no. 1, pp. 14–26, 2023.

[24] J. Liu, C. Ma, M. Li, J. He, C. Hua, L. Wang *et al.*, "Physics-informed hybrid digital twin framework integrating fractal contact modeling and edge–cloud artificial intelligence for dynamic thermal contact conductance prediction," *International Journal of Heat and Mass Transfer*, vol. 264, p. 128736, 2026.

[25] B. Kwolek and M. Kepski, "Human fall detection on embedded platform using depth maps and wireless accelerometer," *Computer Methods and Programs in Biomedicine*, vol. 117, no. 3, pp. 489–501, 2014.