Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3177–3195
DOI : 10.47974/JDMSC-2745

Dynamic entropy-based lightweight security architecture integrating ECC signcryption and zero trust for interoperable healthcare systems

Rutuja Sanyog Pharande *
Basant Tiwari †
Sachin Bhoite §
Department of Computer Science and Applications
Dr. Vishwanath Karad MIT World Peace University
Pune 411038
Maharashtra
India

Abstract

Interoperable healthcare IT systems are leveraged upon 5G enabled interacted IoMT devices and database servers, yet most existing security frameworks still rely on static keys that cannot cope with array of cyber threats, vulnerabilities, and attack vectors. To address this gap, we presented an environment-aware security framework that fused together with ECC-based mutual authentication and signcryption mechanism. The proposed approach uses environmental values such temperature as a natural, dynamic source of entropy to introduce randomness in the security process, especially in driving session oriented cryptographic keys, allowing each transmission to be securely binds with the device's operating context. In the proposed work, signcryption process binds the encryption and signing into a single step, that reduces the packet size and computational cost of resource limited sensing and gateway devices. On the other side, a Zero Trust Data Gateway unsigncrypts, verifies, and forwards messages to a patient-centric ZTA module for granting or rejecting permission based on received request within specific context. The experiment show that proposed approach achieves faster execution, lower overhead, and stronger replay resistance than traditional RSA or Elliptic Curve Cryptography- Elliptic Curve Digital Signature Algorithm (ECC-ECDSA) alternatives. Overall, proposed work concludes a practical path toward secure, context-aware communication in next-generation healthcare environments.

Subject Classification: *Primary 94A60, Secondary 94A62.*

Keywords: *Elliptic curve cryptography signcryption (ECC signcryption), Mutual authentication, Zero trust architecture (ZTA), Secure internet of medical things (IoMT) communication, Context-aware cryptography, Healthcare data security.*

* *E-mail:* **1272251325@mitwpu.edu.in (Corresponding Author)**
† *E-mail:* **basant.tiwari@mitwpu.edu.in**
§ *E-mail:* **sachin.bhoite@mitwpu.edu.in**

1. Introduction

The fast development of the 5G technology has transformed healthcare to access intelligent and interconnected systems that facilitate real-time observation, diagnosis and personalized care. Nonetheless, this progress also comes at a high cost of threats to patient information security and privacy. 5G-enabled healthcare systems incorporate body-worn sensors Internet of Medical Things (IoMT) devices in dynamic clinical environment such as ward, Intensive Care Unit (ICU) or home-heath setting for collecting and monitoring real-time patient's physiological values which stored for future use in database servers. But it has also intensified long-standing concerns about security, privacy, and trust.

Today 5G enabled high connectivity promotes better and real-time treatment of patients and increases efficiency of healthcare systems. Patient information is being gathered and distributed within or among the hospitals inside multiple databases such as patient record database, lab results database, imaging systems database, insurance related database, or cloud-based modules [1], [2]. Thus, this data is transferred over the insecure channel and then stored in the patient databases. In such environment, information security is an extremely vital variable so that patient's data must not be exposed [3]. This requires communication between these devices through the intranet or the Internet must be strictly private and confidential and should be encrypted to protect the patient's privacy against exposing and altering [4].

Additionally, the right data at the perfect time is the most consequential requirement for getting best conceivable consideration to the patient. The IoMT devices that are equipped on patient's body and are operating with in healthcare settings can use environmental conditions that naturally fluctuate and can be leveraged as additional entropy. Environmental parameters such as temperature, motion etc. can provide lightweight but effective randomness suitable for secure key generation.

Traditional Zero Trust Architecture (ZTA) solutions offer strong perimeter-less protection with the principal of never trust, always verify [5], [6]. Yet most of them overlook the fact that patients, not devices or networks, are the true owners and decision-makers of their health information [7], [8]. At the same time, communication within Internet of Medical Things (IoMT) devices and databases still relies heavily on static keys or heavyweight cryptographic routines that are inappropriate for resource-constrained devices and vulnerable to compromise. This is not suited for dynamic 5G healthcare setting where devices frequently change

Figure 1

Conceptual architecture of the proposed signcryption and Zero Trust–enabled healthcare security framework

location, network context, and trust boundaries. Hence, increases the chance of replay attack, long-term static key compromise and contextual decoupling between the data and its operating environment. Existing literature also rarely uses environmental values as auxiliary input for cryptographic operations. Thus, to overpass these gaps, this work integrates a patient-centric ZTA model with a lightweight environmental-value (eV) based signcryption mechanism, enabling both secure access decisions and secure communication across the 5G enabled healthcare system [9], [10].

In this paper, we propose a focused enhancement to Zero Trust Architecture for 5G-enabled healthcare by introducing a lightweight eV-based ECC signcryption technique as shown in Figure 1. This figure illustrates the conceptual end-to-end system architecture, where IoMT edge nodes first perform environment-aware signcryption. This data is further verified at the ZDG and forwarded to authorized consumers via patient-centric ZTA modules including consent management, context evaluation, device trust assessment, and policy decision enforcement. This figure is more elaborated in Figure 2 in section 3 to realize this architecture at the operational low-level flow including cryptographic and Zero Trust processing for secure and trusted communication. Instead of redesigning the entire ZTA ecosystem, we strengthen its very first gate i.e. the moment when a device or user tries to prove who they are. This means proposed work strengthen identity verification step, where a user or device proves who they are. This makes initial identity check stronger, faster, and more secure using ECC Signcryption [11], [12], [13]. This replaces traditional, heavy cryptographic handshakes with an elliptic-curve-driven mutual verification process were environmental measurement influence

generation of session key and message authentication. This devised algorithm is lighter, and more suitable for wearable sensors, mobile devices, and real-time medical systems.

2. Literature Review

Recent studies pertaining to the zero-trust in healthcare environment have explored Zero Trust Architecture (ZTA) as a foundation for strengthening security in next-generation healthcare systems [14]-[20]. [4] Designed a context-aware zero trust cloud-based health system framework that reduced the medical errors by a significant margin due to the use of trust-scoring and AI-based contextual analysis. Author asserted that the proposed framework greatly minimized medical errors and enhanced governance through constantly certifying the user and device behavior. The suggested framework is the pioneer application of language model intelligence to improve zero Trust decision-making systems in healthcare, which subsequently facilitates the reduction of human error and improvement of compliance to medical data governance standards [14]. Likewise, the study conducted by [15] featured the development of a Zero Trust security platform that would be utilized specifically in smart healthcare networks involving 5G. The proposed trust scoring algorithm continuously checks the actions of the user, the device and the applications. It is achieved through behavior, environment sensors and fine-grained access control systems. This is to make sure that all users/ devices will be provided with the minimum access necessary with milliseconds latencies absent yet without integrating patient-centred consent [15]. Some of the researchers in parallel explored decentralized approaches to overcome the limitations of centralized systems such as [16], [17]. [16] Introduced a decentralized model that serves to eradicate the existence of a single focal point, which is a significant flaw in centralized systems. [16] Proposed Zero Trust Architecture (ZTA) with blockchain to facilitate the process of sharing medical images securely. Both the works [16], [17] employed blockchain technology and the Interplanetary File System (IPFS) to share the patient's data without risks to their safety. Both the systems ensure data integrity and preventing single-point failures through immutable metadata and access logs. Author of both the articles declared that the proposed frameworks eliminate reliance on centralized PACS servers with improved security, transparency, and interoperability across hospitals without adding significant performance overhead [16], [17]. Building on traditional perimeter-free architectures, [18], [19] implemented a system

named Home-based medical security model founded on the principles of Zero Trust and tested it on a virtual hospital network. The proposed layered model incorporates the device identity management, Dynamic policy orchestration and micro-segmentation of network zones. The proposed system employed behaviour analytics to formulate the adaptive access rules and provide the more nuanced control and insight into the internal communications in contrast to the former perimeter security.

Although, above works highlighted the growing importance on trust scoring, decentralized databases, behaviour-driven and context-aware policy enforcement, and role-based access control within healthcare, they rely largely on traditional encryption schemes. This opens other important facet of research in ensuring patient's privacy focuses on how sensitive patient's data can be protected when it is transferred over the intranet and internet. Thus, we need for efficient and lightweight mutual authentication mechanisms that can operate at the very first layer of Zero Trust i.e. before any trust scoring or access evaluation occurs. To tackle with this, many researchers used the signcryption cryptographic technique, which combines digital signature and encryption in single and efficient step. The following studies highlighted how signcryption and mutual authentication have been applied within healthcare systems.

Few recent works [21], [22], [23] have focused on applying signcryption to protect healthcare and IoMT communications more efficiently such as [21] suggested combined blockchain-edge architecture with the use of Attribute-Based Signcryption (ABSC) to enhance the confidentiality, authenticity, and regulated accessibility of medical information in the Internet of Medical Things (IoMT) and EHR systems. The proposed design is used to overcome inefficiencies of conventional encryption-based health data system, especially where decentralized checks are not made, adaptable access control, and effective cryptographic functions are not supported. [22] Developed a lightweight signcryption protocol that is optimized to wearable healthcare and IoMT approaches to meet the severe limitations of such devices in regard to computational power, energy consumption, and constantly transmitting data. Their scheme proves more cost-efficient operations and provides a quick and an energy-saving solution to protecting sensitive physiological data. The scheme ensures the standard security properties of elliptic-curve schemes, such as confidentiality, integrity, authenticity, and forgery resistance, using lightweight elliptic-curve techniques, which are compatible with the highest-level power requirements of ultra-low-power equipment. [23] Introduced a certificateless anonymous signcryption protocol tailored to a

Wireless Body Area Network (WBAN). Their method removes the necessity of using traditional digital certificates and hence simplifies the workload of key management as well as lessening the chances of attack by using certificates. The scheme allows protecting the identity of users yet still ensures confidentiality, authenticity, and integrity by incorporating anonymity into the process of signcryption in the scheme. Although signcryption significantly increases the confidentiality of medical information in transit, the effectiveness of secure communication is still dependent on devices and users demonstrating their identity before any encrypted communication are possible.

This reality has led to scholars to research on complex mutual authentication schemes tailored to healthcare and Internet-of-Medical Things (IoMT) environments. The following research details the way mutual authentication has changed to support anonymity, quantum era adversarial resistance, and continuous verification in zero trust-based healthcare systems of today. [24] Introduced a mutually authentication scheme for Social IoT (SIoT) healthcare, where the wearable sensors and patient-centric IoT devices constantly exchange sensitive physiological information. Their system combines three-factor authentication (password, smart-card and biometric validation) fortified with the help of a fuzzy extractor, elliptic-curve cryptography (ECC) and formal security proofs. The authors claimed that proposed work is compatible with the Zero Trust principles including continuous verification and never trust, always verify of IoT-healthcare ecosystems. [25] Suggest a quantum-safe Mutual Authentication mechanism of Internet-of-Health-Things (IoHT) networks through the concurrent implementation of lattice-based post-quantum cryptography and decentralized blockchain ledger. Author claimed that proposed work is safe against quantum-based system that can affect ECC/RSA-based protocols that are used in healthcare authentication. [26] Present the use of continuous and mutual lightweight authentication as a scheme developed specifically in Healthcare 4.0 settings constructed on IoMT, cloud, and edge computing. Their architecture uses the basis of a Zero Trust Architecture (ZTA) through enforcement of identity verification persistently, monitoring behaviour in their devices and enforcing freshness on cryptography on all communication sessions.

3. Proposed Work

The following Figure 2 shows the working of proposed work. The IoMT Edge nodes on the left-hand side of the figure, which collect the

physiological data from body sensor network with quietly collecting environmental values (eV). The proposed work utilized ambient temperature as eV. Since temperature is naturally available everywhere and vary across every room such as ICUs, wards, operation theaters, and home-care rooms, making them environment-specific and does not require any special or invasive sensing. To use the temperature within IoMT edge device, it is sampled locally and normalized into a bounded numeric range. These normalized values are further joined with the timestamp value that makes it fresh and reduce predictability during key derivation.

IoMT sends the eVs reading into Signcryption Module, where the data is encrypted and signed in one lightweight step before leaving the sensor's edge. Once the data is signcrypted, the IoMT device proves its identity through a mutual authentication handshake with the Zero Trust Data Gateway (ZDG). Once handshake succeeds, the IoMT access a secure channel to send its data packet toward the gateway. When data packet is received at ZDG, it first unsigncrypt it, by checking both the correctness of the encryption and the legitimacy of the sender in one verification process and then stores it in database server.

Whenever the access request received at patient-centric ZTA, it is first evaluated by Consent Manager to ensure that the data use matches the patient's permissions and privacy choices. Then, the Context Engine examines the surrounding context such as time, location, or device behaviour etc. to ensure the request makes sense. Further, the Device Trust Engine evaluates how reliable the originating device is based on time, raising or lowering trust based on past behaviour. After calculating the trust score, the Policy Decision Point (PDP) the decision and decides exactly how much of the data should be given to requester. Finally, the system delivers the approved patient's electronic health record to authorized recipients such as IoMT dashboards, doctors, or insurers etc, each receiving only what they are allowed to see on need-to-know basis. The actual algorithm is divided into two steps:

Step 1 – ZTA-Integrated Signcryption at IoMT Edge Node (IEN)

This step works as data-ingress protection step which is responsible for inbound traffic security, i.e. Before any sensed data enters the Zero Trust domain, the IEN signcrypts it so that the ZTA Data Gateway receives already confidential and origin-authenticated data. To do so, this algorithm uses ECC-based signcryption which combines both encryption and digital signature into one cryptographic primitive, this reduces the computational

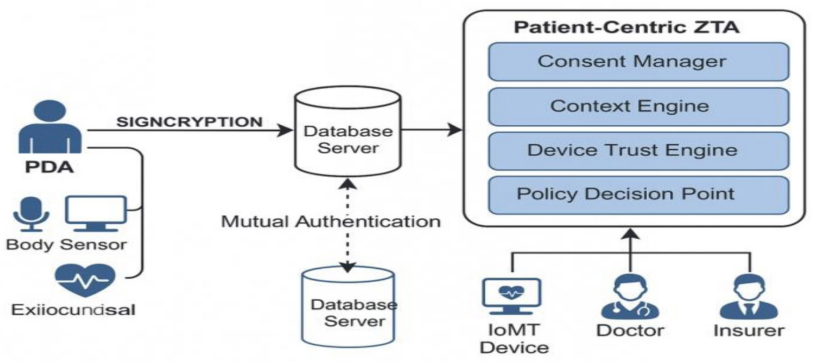

Figure 2

eV based ECC signcryption and Zero Trust verification process.

overheads with short packet size and verification delay when it is compared with the traiditional signing and then encryption operation. As shown in the Figure 2, On the left, the environmental sensor nodes measured temperature and blends it with a current timestamp to create strong nonce or entropy which make this cryptographic operation resistant to replay and relocation attack.

Using that randomness, it sets up a onetime session key with the gateway, encrypts the reading, and attaches a compact digital signature so the gateway can later see both that the data is secret and that it really came from this device. To do so, it proceeds as follows:

Input: Message m (IoMT sensed value), eV (Environment Value), ZDG public key Q_Z, IEN private key d_E

Output: Signcrypted tuple (cT,RG,s)

Algorithm 1: ZTA-Integrated Signcryption at IoMT Edge Node (IEN)

1. **PV-based nonce:** nu=H(EV ‖ timestamp), v=(numod(n–1))+1
2. **Ephemeral point on the curver:** E_p=vG
3. **Session key derivation (ZTA edge–gateway key)**
   - ι. Elliptic-curve Diffie–Hellman with ZDG: Z=v.Q_Z=(x_Z,y_Z)
   - ιι. Derive two symmetric keys (encryption + authentication) bound to eV: (k_1,k_2)=KDF(xZ ‖ eV)
4. **Encrypt IoMT data:** cT=E_{k1}(m)

5. **Compute hash tag over protected data:** $t=H_{k2}(c \| E_{p\,(x)} \| eV)$ where $E_{p\,(x)}$ is the x-coordinate of E_p.
6. **Compute ECC signcryption scalar:** $s=(v+t \cdot d_E) \bmod n$

Transmit signcrypted packet: IEN sends (cT, E_p, s) to the **ZTA Data Gateway** over the channel labelled **SIGNCRYPTION** in in the figure.

Step 2 – ZTA-Integrated Unsigncryption & Policy Ingestion at ZTA Data Gateway (ZDG)

This is the trust-verification and policy-entry setup step. As shown in the Figure 2, ZTA Data Gateway receives the signcrypted packet and verifies the IEN by regenerates the same secret using its own key and the device's onetime point. Further, forwards the plaintext data into patient's centric ZTA module where the Consent Manager, Context Engine, Device Trust Engine, and Policy Decision Point works for Zero Trust evaluation.

Input: received (cT, E_p, s), ZDG private key d_Z, IEN public key Q_E, synchronized eV

Output: Recovered message m (if valid) or $\perp$ (reject)

Algorithm 2.1: ZTA-Integrated Unsigncryption at ZTG

1. **Regenerate shared point (ZTA gateway side):** $Z'=d_Z E_p =(x_{Z'},y_{Z'})$
2. **Derive session keys:** $(k_{1'},k_{2'})=KDF(xZ' \| eV)$
3. **Decrypt IoMT data:** $m=D_{k1'}(c)$
4. **Regenerate verification tag:** $t'=H_{k2'}(c \| E_{p\,(x)} \| eV)$
5. **Verify IEN authenticity (ECC signature verification): $sG = E_p + t'Q_E$**

Here in this step, point computed from scalar '**s'** is compared with the combination of sender's ephemeral point E_p and public key Q_E. If both sides match, signature become valid i.e. message came from the trusted sender, which is send to Consent Manager, Context Engine, Device Trust Engine, Policy Decision Point (PDP) as shown in following algorithm 2.2, else output$\perp$, log the event, and trigger a ZTA alert.

Input: Verified message m, metadata,

Output: Decision and Policy to apply

Algorithm 2.2: Data Injection into Patient-Centric ZTA

1. Input←(m,metadata)
2. consent←ConsentManager.Check(Input)
3. If consent=DENY → **return BLOCK**
4. context←ContextEngine.Evaluate(Input)
5. trust←DeviceTrustEngine.Update(IEN_ID)
6. decision←PDP.Decide(consent,context,trust)
7. **return**ApplyPolicy(decision,m)

Step 3 – Inject data into Patient-Centric ZTA module

Above algorithm 2.2 now verified data flows into four main components of ZTA that are Consent Manager, Context Engine, Device Trust Engine, and Policy Decision Point. These four components at real time and for each access request from will decide who (doctor, insurer, other devices) is allowed to see which part of the data based on patient consent, context, and device trust, rather than assuming anyone inside the network is automatically trusted.

4. ImplementationandPerformance Analysis

For the implementation of proposed work dual process simulation model is implemented on a single Python machine with cryptography, tinyec, flask, requests, psutil libraries [27], [28], [29], [30]. The first Process A works as an IoMT Edge Node, which generates environment based (eV) keys and signcrypting data. The Process B implemented the ZTA Data Gateway, which implements unsigncryption, verification, and zero-trust decision enforcement. Processes A and B use psutil library to monitor and record the CPU usage, latency, packet size, and memory during each transaction and finally saves the logs into CSV file. The execution time refers to the time which is required by the total cryptographic processing delay per message. The packet size refers to the payload in bytes within the packet transmitted. The CPU usage confines average processor utilization during execution and energy consumption calculates the estimated power cost per transaction.

This paper assumed the threat model by considering adversaries capable of introducing replay attacks, MiTM interception, impersonation, and key compromise attacks, while assuming that physical device interception, seizure and hardware modification are outside the scope of

this study. During implementation of this proposed work, all cryptographic methods (RSA, ECDSA and proposed ECC+eV Signcryption) are implemented with same security strength and further evaluated to ensure a fair and standardized comparison. The RSA uses RSA-2048 with SHA-256 for digital signing. The ECDSA baseline employs elliptic curve P-256, with ECDH-based key agreement, AES-128-GCM for encryption, and ECDSA with SHA-256 for authentication. All three schemes are evaluated using same message size, python libraries and hardware configuration. The results of performance metrics are records as average values over multiple independent runs to make sure the consistency. Following Table 1 shows the standardized cryptographic benchmark parameters:

Table 1

Standardized Cryptographic Benchmark Parameters

Scheme	Security Level	Public Key Size	Crypto-graphic Stack	Hash / MAC	Sym-metric Cipher	Pay-load Size	No. of Runs
RSA Base-line	112-bit (Classi-cal)	2048 bits	RSA-2048, Signature andEncryp-tion	SHA-256	AES-128	256 bytes	1000
ECC-ECD-SA Baseline	128-bit (Classi-cal)	256 bits (P-256)	ECDH, AES-GCM and ECDSA	SHA-256	AES-128-GCM	256 bytes	1000
Proposed ECC+eV Signcryp-tion	128-bit (Classi-cal)	256 bits (P-256)	ECC Sign-cryption (Combined)	HMAC-SHA-256	AES-128	256 bytes	1000

4.1 *Cryptographic Performance Comparison*

Following graph shown Figure 3 shown the execution time of cryptographic operations for RSA-2048, ECC-P256, and the proposed ECC and eV based signcryption scheme. The The x-axis shows various cryptographic operations like, KeyGen, Signcrypt, Unsigncrypt, Mutual Authentication and End-to-End latency, while y-axis shows the time in milliseconds. From the above Figure, it is shown that proposed ECC and eV based signcryption outperform with the recorded values of 11 ms, 22, ms, 24 ms, 18 ms and 55 ms for KeyGen, Signcrypt, Unsigncrypt, Mutual

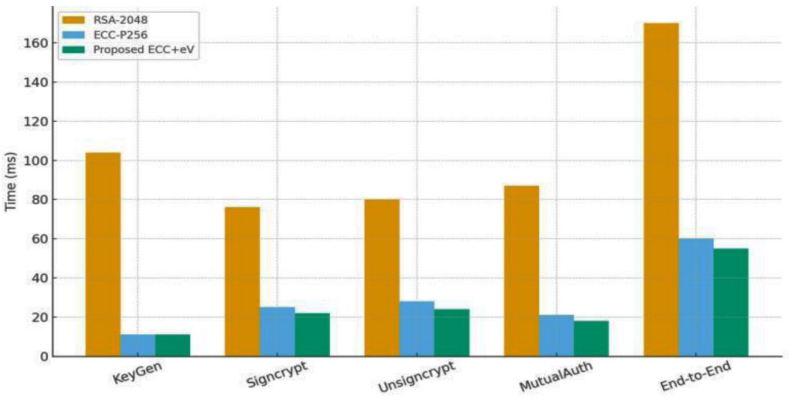

Figure 3

Execution Time analysis of cryptographic operations

Authentication and End-to-End latency respectively over RSA and traditional ECC based method.

4.2 *Packet Size Comparison*

Following graph shown in Figure 4 shows the bar graph for total packet size required for RSA-2048, ECC-P256, and the proposed ECC and eV based signcryption scheme. Graph show that RSA-2048 signature needs the largest packet size of 640 bytes, due to large keys size. ECC with ECDSA uses the packet size of 192 bytes, while the proposed the proposed ECC and eV based signcryption scheme compress the data up to 128 bytes. This is because encryption and signature are combined into a single

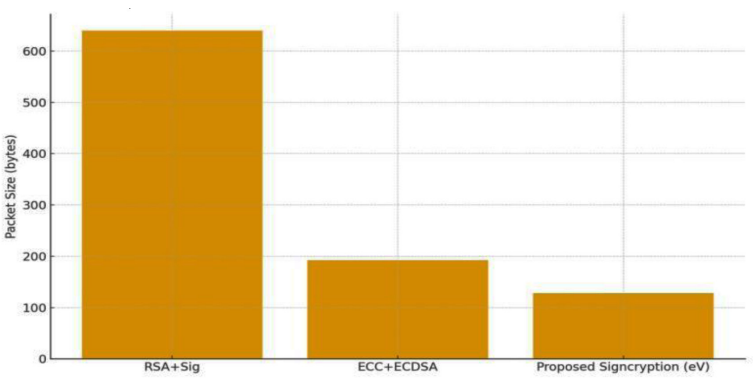

Figure 4

Total Packet Size Analysis

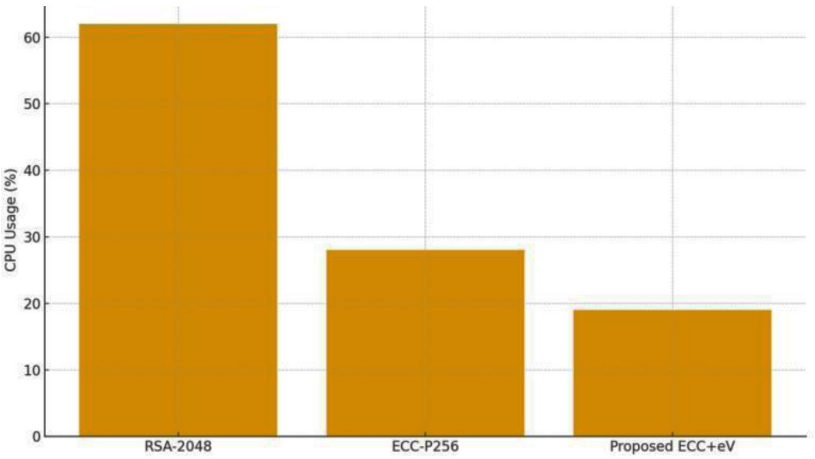

Figure 5

CPU Usage Analysis on IoMT Node for different schemes

packet. This results in requirement of lower bandwidth consumption and reduced transmission latency in constrained 5G/IoMT environments.

4.3 *CPU Usage on IoMT Node*

Following graph shown in Figure 5 shows the bar graph compares the CPU utilization on the IoMT edge node during cryptographic operation for RSA-2048, ECC-P256, and the proposed ECC and eV based signcryption schemes. Figure concludes that RSA-2048 requires the highest CPU load of around 60%, which is unsuitable for low-power sensing devices, while the ECC based system reduces it below 30%. As compared to these two schemes, The proposed signcryption further brings CPU usage down to below 20%, which make proposed scheme more realistic for battery-powered IoMT devices. This implies that proposed system produces less heat, longer device lifetime and extended patient-side usability.

4.4 *Energy Consumption per Operation*

Following graph shown in Figure 6 shows the bar chart for estimated energy consumption per cryptographic operation in millijoule (mJ) for all three schemes. Graph illustrate that RSA-2048 requires highest energy requirement of around 18 mJ per operations, which results in heavy computation overhead as compared toECC-P256 which reduces energy consumption to 7 mJ. The proposed scheme consumes very less energy which is around 5 mJ due to single combined signcryption and encryption.

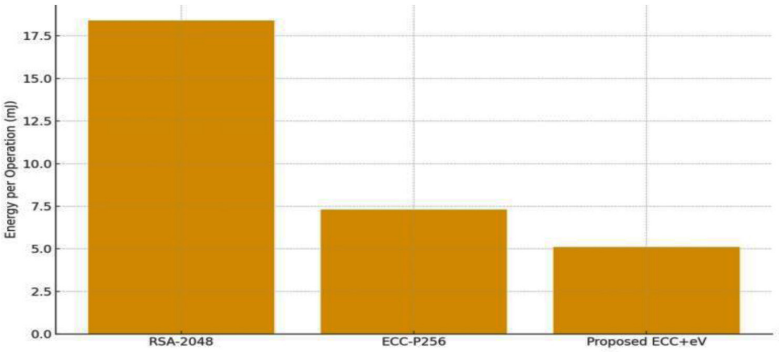

Figure 6

Estimated Energy Consumption analysis per Cryptographic Operation

This reveals that the proposed scheme is not only faster but also more energy-efficient, which is necessary for continuous patient's monitoring in healthcare.

Table 2

ZTA Pipeline Decision Cases

Scenario	Consent	Context	Trust	PDP Decision
Primary doctor request	Allow	Safe	High	PERMIT
Insurer request	Deny	Safe	Medium	BLOCK
Suspicious IoMT behaviour	Allow	Safe	Low	MASK
Emergency Situation	Allow	High Risk	Medium	LIMITED

The above Table 2 shows how the proposed Patient-Centric ZTA module reacts to different real-world situations instead of giving a simple "yes" or "no" to every request. This is done by evaluating every incoming request for patient data under different operational cases. Tables shows that how Consent Manager, Context Engine, Device Trust Engine, and the Policy Decision Point give to the final access request decision.

The first case shows the access request generated by primary, legitimate and authenticated doctor inside the hospital. Since patient consent allows this access, context signals become safe, and the device trust score will be high, thus PDP grants full access permission. Second case belongs to insurer, who tries to access the patient data. In this case contextual risk may be low, but the patient hasn't allowed this. So, the Consent Manager unambiguously reject or block the access request for insurer regardless of how safe the context looks.

The third scenarios show a case where the IoMT device acts distrustfully for example, if it generating uneven authentication attempts or inconsistent cryptographic signatures regularly. In such situation, IoMT devices behaves strangely, which results in low trust score and this forces PDP to reveal only masked information access. This reveals only non-sensitive or limited information.

The last scenario represents the emergency situation, where context is high-risk because patient may not be in hospital or even designated address (e.g., unusual location or time). This results in low trust or moderate, which influence the PDP to grant the request with limited permission for very essential subset of patient data on need-to-know basis for emergency care.

Together, these scenarios shown in the table demonstrates how the ZTA module of proposed work combines consent**,** context**,** device trust, and policy rules to make thoughtful, context-aware decisions rather than blindly approving or rejecting every request.

5. Conclusion & Future Work

The proposed work binds together signcryption, Mutual authentication and zero trust to provide reliable and trust oriented security framework for patient's data privacy in healthcare environment. By combining ECC with environment-value driven entropy, the framework becomes both efficient and tough against impersonation or replay attack. The result shown in the paper affirms the improvements in speed, packet size, and device workload, which make the proposed framework more realistic for IoMT and continuous monitoring environment. Most importantly, the framework protects patient's data while still allowing doctors and other subjects & systems to access exactly what they need, when they need it. In future, the ZTA module will be strengthened with more algorithmic intelligence to make it to learn and adapt to emerging threats automatically. Additionally, a wider range of emergency situation will be explored so that the system remains safe without slowing down time-critical medical scenarios. The proposed work will also be extended to evaluate the scalability of the system in large scale IoMT deployments. In this case, the abiotic parameters influence, such as temperature, pH, lighting and humidity under heterogeneous healthcare conditions in settings, including differences between these factors, will be investigated to understand their consequences for the system performance. Finally, the

proposed system will be tested in active, high volume hospital settings to determine practical feasibility.

References

[1] A. K. Alnaim, "Adaptive zero trust policy management framework in 5G networks," *Mathematics,* vol. 13, no. 9, Art. no. 1501 (2025), doi: 10.3390/math13091501.

[2] R. Jain, B. Batra, B. Kanwer, L. Raja, and V. Bhatnagar, "Transforming network security through zero trust architecture: Principles, challenges, and future directions," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 29, no. 2-B, pp. 1097–1106 (2026), doi: 10.47974/JDMSC-2649.

[3] A. Noonia, D. Thakral, P. Mathur, F. Sheth, H. Shaikh, and A. K. Gupta, "A discrete mathematical model and cryptography for secure medical image analysis: Encrypted chest X-ray classification," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 5A, pp. 1473–1486 (2025), doi: 10.47974/JDMSC-2146.

[4] P. Dhiman, N. Saini, Y. Gulzar, S. Turaev, A. Kaur, K. U. Nisa, and Y. Hamid, "A review and comparative analysis of relevant approaches of zero trust network model," *Sensors,* vol. 24, no. 4, Art. no. 1328 (2024), doi: 10.3390/s24041328.

[5] N. Kaur, A. Mittal, U. K. Lilhore, S. Simaiya, S. Dalal, K. Saleem, and E. S. Ghith, "Securing fog computing in healthcare with a zero-trust approach and blockchain," *EURASIP J. Wireless Commun. Netw.*, vol. 2025, no. 1, Art. no. 5 (2025), doi: 10.1186/s13638-025-02431-6.

[6] A. K. Tyagi and R. Seranmadevi, "Blockchain for enhancing security and privacy in the smart healthcare," in *Digital Twin and Blockchain for Smart Cities. Hoboken*, NJ, USA: Wiley, pp. 343–370 (2024), doi: 10.1002/9781394303564.ch16.

[7] W. Jin, S. Wu, Y. Feng, H. Wang, and C. Fu, "Zero trust architecture for security and protection system in 5G intelligent healthcare," *International Arab Journal of Information Technology,* vol. 22, no. 2, pp. 263–277 (2025), doi: 10.34028/iajit/22/2/5.

[8] M. L. Gambo and A. Almulhem, "Zero Trust Architecture: A systematic literature review," *J. Netw. Syst. Manage.,* vol. 34, no. 1, Art. no. 25 (2026), doi: 10.1007/s10922-025-09998-x.

[9] H. Nandanwar and R. Katarya, "Secure and privacy-preserving data sharing in 6G-enabled blockchain IoT healthcare systems," *Secur. Privacy,* vol. 8, no. 6, Art. no. e70105 (2025), doi: 10.1002/spy2.70105.

[10] R. Maji, B. Gayen, and S. Saha, "A robust IoT-based approach to enhance cybersecurity and patient trust in the smart health care system: Zero-trust model," in *Design and Forecasting Models for Disease Management.* Hoboken, NJ, USA: Wiley, pp. 269–281 (2025), doi: 10.1002/9781394234073.ch12.

[11] S. Batra, B. Narwal, and A. K. Mohapatra, "JLSAIoMT: Justifiable lightweight and secure mutual authentication scheme for Internet of Medical Things," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5, pp. 2113–2142 (2025), doi: 10.47974/JDMSC-2189.

[12] G. A. Thushara and S. M. S. Bhanu, "A blockchain-assisted attribute-based signcryption for secure sharing of medical IoT data in fog environment," *Secur. Privacy*, vol. 8, no. 3, Art. no. e70034 (2025), doi: 10.1002/spy2.70034.

[13] S. Goel, M. K. Gupta, and S. Kumari, "An improved attribute-based signature using elliptic curve cryptography," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 6, pp. 2371–2382 (2025), doi: 10.47974/JDMSC-2302.

[14] K. Al-Hammuri, F. Gebali, and A. Kanan, "ZTCloudGuard: Zero trust context-aware access management framework to avoid medical errors in the era of generative AI and cloud-based health information ecosystems," *AI*, vol. 5, no. 3, pp. 1111–1131 (2024), doi: 10.3390/ai5030055.

[15] C. Liu, R. Tan, Y. Wu, Y. Feng, Z. Jin, F. Zhang, Y. Liu, and Q. Liu, "Dissecting zero trust: Research landscape and its implementation in IoT," *Cybersecurity*, vol. 7, no. 1, Art. no. 20 (2024), doi: 10.1186/s42400-024-00220-8.

[16] A. Shahzad, W. Chen, Y. Zhang, and R. Kumar, "Zero-trust medical image sharing: A secure and decentralized approach using block-

chain and the IPFS," *Symmetry*, vol. 17, no. 4, Art. no. 551 (2025), doi: 10.3390/sym17040551.

[17] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," *BMC Med. Inform. Decis. Mak.*, vol. 20, Art. no. 256 (2020), doi: 10.1186/s12911-020-01275-y.

[18] Z. Wang, X. Yu, P. Xue, Y. Qu, and L. Ju, "Research on medical security system based on zero trust," Sensors, vol. 23, no. 7, Art. no. 3774 (2023), doi: 10.3390/s23073774.

[19] I. U. Onwuegbuzie and O. A. Alabi, "A review of authentication and authorization mechanisms in zero trust architecture: Evolution and efficiency," *Tech-Sphere J. Pure Appl. Sci.*, vol. 2, no. 1 (2025), doi: 10.5281/zenodo.15149866.

[20] S. Ahmadi, "Autonomous identity-based threat segmentation for zero trust architecture," *Cyber Secur. Appl.*, vol. 3, Art. no. 100106 (2025), doi: 10.1016/j.csa.2025.100106.

[21] T. Dou, Z. Zheng, W. Qiu, and C. Ge, "A secure medical data framework integrating blockchain and edge computing: An attribute-based signcryption approach," *Sensors*, vol. 25, no. 9, Art. no. 2859 (2025), doi: 10.3390/s25092859.

[22] T. M. Ghazal, M. K. Hasan, S. O. Khairy, U. A. Mokhtar, S. Islam, R. A. Saeed, N. Ahmed, and M. Abdullah, "Lightweight signcryption scheme for securing wearable sensor observed health data sharing in Internet of Medical Things paradigm," *Sci. Rep.*, vol. 15, no. 1, Art. no. 40989 (2025), doi: 10.1038/s41598-025-24687-0.

[23] W. Long, L. Deng, J. Zeng, Y. Gao, and T. Lu, "An efficient certificateless anonymous signcryption scheme for WBAN," *Sensors*, vol. 24, no. 15, Art. no. 4899 (2024), doi: 10.3390/s24154899.

[24] T. Arpitha, D. Chouhan, and J. Shreyas, "Anonymous and robust biometric authentication scheme for secure social IoT healthcare applications," *J. Eng. Appl. Sci.*, vol. 71, no. 1, Art. no. 15 (2024), doi: 10.1186/s44147-023-00342-1.

[25] A. Ahmad and J. Srirangan, "Quantum-safe mutual authentication scheme for IoHT using blockchain," *Results Eng.*, vol. 28, Art. no. 106945 (2025), doi: 10.1016/j.rineng.2025.106945.

[26] W. Almuseelem, "Continuous and mutual lightweight authentication for zero-trust architecture-based security framework in Cloud-Edge computing-based Healthcare 4.0," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 1, pp. 1–19 (2024).

[27] PyCA Developers, *Cryptography.* [Online]. Available: https://cryptography.io/. [Accessed: Nov. 20, 2025].

[28] A. Hossain, *tinyec: A Tiny Elliptic Curve Library in Python.* GitHub. [Online]. Available: https://github.com/alexmgr/tinyec. [Accessed: Nov. 20, 2025].

[29] A. Ronacher, *Flask: Web Development Framework for Python.* Pallets Projects. [Online]. Available: https://flask.palletsprojects.com/. [Accessed: Nov. 20, 2025].

[30] G. Rodolà, "psutil: Cross-Platform Process and System Utilities," *GitHub Repository.* [Accessed: Nov. 20, 2025].

Received January, 2026