SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I2P104

Volume 11 Issue 2, 33-40, February 2024

Original Article

Unified Security Paradigm: Bi-Factor Authentication and Hyper Elliptical Curve Cryptography in IoT-Enabled Cloud Data Protection (BFHECC - IoMT)

T.A. Mohanaprakash[1], K. Sivakumar[2], Nirmalrani Vairaperumal[3], M. Ramya[4], K. Cinthuja[5]

[1,5]*Department of Computer Science and Engineering, Panimalar Engineering College, Tamil Nadu, India.*
[2]*Artificial Intelligence and Data Science, Nehru Institute of Engineering and Technology, TamilNadu, India.*
[3]*Department of CSE, School of Computing, Sathyabama Institute of Science and Technology, TamilNadu, India.*
[4]*Department of Computer Science And Engineering, St. Joseph's Institute Of Technology, Tamil Nadu, India.*

[1]*Corresponding Author : tamohanaprakash@gmail.com*

Received: 25 October 2023 Revised: 02 December 2023 Accepted: 26 December 2023 Published: 02 February 2024

Abstract *- Ensuring robust security for cloud-stored sensitive information and medical data is critical in contemporary technological landscapes. Safeguarding cloud data involves encryption, access controls, and authentication methods like TLS and multi-factor authentication. Yet, vulnerabilities such as breaches or misconfigurations pose ongoing threats, necessitating continual improvements. The proposed (BFHECC-IoMT) solution integrates a two-factor authentication model and "Hyper Elliptical Curve Cryptography," presenting a formidable security infrastructure for cloud storage. This framework strengthens data encryption using conventional (password or PIN) and hyper elliptical curve-based authentication methods. It fortifies security beyond typical measures, increasing resistance to cryptographic attacks during data transmission or storage. On the other hand, integrating IoMT and cloud security, bolstered by Homomorphic Encryption and Elliptic Curve Cryptography (HECC), establishes a robust security framework for managing sensitive medical information. Addressing the oversight in existing healthcare systems, this integration ensures enhanced data confidentiality and integrity during transmission and storage. Seamlessly uniting IoMT, cloud security, Homomorphic Encryption, and ECC facilitates secure data transfer from IoT devices to cloud systems, ensuring stringent security standards for maintaining confidentiality, integrity, and availability. This comprehensive approach secures patient data transmission and provides privacy during analysis, compliance with healthcare regulations, and the overall secure handling and analysis of health data in the healthcare sector.*

Keywords *- Elliptic Curve Cryptography, Homomorphic Encryption, Internet of Medical Things, Authentication, Medical data.*

1. Introduction

Maintaining the confidentiality and integrity of cloud data is fraught with difficulties. Implementing strong encryption and access controls, including access permissions and encryption key management, is still challenging. Adhering to various data protection laws, like GDPR and HIPAA, entails fulfilling legal obligations and coordinating security protocols. The constantly evolving cyber threats increase the risks of data breaches, unauthorized access, and exploitation due to malicious attacks, human error, or system vulnerabilities. Preventing internal breaches, employee-intentioned breaches, and unauthorized access are ongoing challenges. Handling data across various locations and jurisdictions while complying with local laws and security standards presents complexity. Trusting the security of third-party services, like cloud providers, and ensuring alignment with internal security standards poses a significant challenge. Additionally, securing data during transfer and protecting it from interception remains an ongoing challenge, particularly in public networks. Addressing these issues requires a comprehensive approach involving encryption, secure access controls, continual security monitoring, user education, and implementing up-to-date security protocols and technologies. Safeguarding sensitive information in cloud storage is paramount to prevent unauthorized access or breaches. Cloud systems utilize encryption, access controls, and authentication methods such as TLS and multi-factor authentication for security. However, vulnerabilities like breaches, misconfigurations, or insider threats can compromise data integrity and confidentiality, leading to potential breaches or leaks. To address these concerns, the paper suggests integrating a two-factor authentication system in combination with "Hyper Elliptical Curve Cryptography" to fortify cloud storage security. This proposed system incorporates a standard authentication factor, such as a password or PIN, with an advanced hyperelliptical curve-based authentication

mechanism - potentially utilizing tokens or keys derived from this cryptographic algorithm. This integration enhances data encryption within the cloud storage infrastructure and introduces an additional layer of security that extends beyond typical encryption methods. Adopting this advanced cryptographic approach aims to heighten security measures by offering increased resistance to potential cryptographic attacks, making it significantly more challenging for unauthorized entities to intercept, decrypt, or manipulate data. At the same time, it's being transmitted or stored within the cloud environment. By combining multiple layers of security, this proposed system endeavors to significantly raise the barriers against potential breaches or unauthorized access to sensitive data within the cloud storage infrastructure.

2. Related Work

A comprehensive view of security considerations encompassing the Internet of Things (IoT), cloud computing, and related technological landscapes. Haque et al. [1] investigate IoT security and privacy, exploring cognitive computing and intelligent IoT systems. Meanwhile, Vijayakumar and Shiny Angel [2] focus on identifying IoT security threats and botnet attacks, stressing the urgency of addressing security issues within this domain.

Boumait et al. [3] delve into IoT systems security, specifically leveraging machine learning applications to bolster security measures. Gupta et al. [4] emphasize enhancing security in e-healthcare applications using blockchain technology. Several studies, including Dedeoglu et al. [5], Mohanta et al. [6], and Wazid et al. [7], investigate trust and privacy in IoT systems, proposing various architectures, solutions, and trust-based authentication schemes.

Additionally, Xie et al. [8] emphasize privacy-preserving authentication methods for wireless sensor networks in IoT environments. Pasumponpandian [9] highlights secure cloud storage using Elgamal Hyper Elliptic Curve Cryptography, while Mendonca [11] discusses data security in the cloud utilizing AES.

Table 1. Comparative analysis of tools and concepts used in current IoMT and cloud security systems

Reference	Tools / Methods / Concepts	Focus
1	IoT Security, Privacy Measures	Privacy and Security in the Internet of Things
2	Botnet Analysis, IoT Security Threats	IoT Security Survey: Examination of Botnet Attacks on IoT
3	Machine Learning in IoT Security	A Survey on Machine Learning-Based IoT System Security
4	Blockchain in e-Healthcare IoT	Blockchain-Based IoT-Based e-Healthcare Application Security
5	Trust Architecture, Blockchain in IoT	Blockchain-Based Trust Architecture for IoT
6	Blockchain in IoT, Security Measures	Resolving IoT Security and Privacy Concerns with Blockchain Technology
7	Certificate-Based Authentication Scheme	TACAS-IoT: Authentication Scheme for Edge-Enabled IoT Systems Based on Trust Aggregation Certificates
8	Anonymous Authentication, Wireless Sensor Networks	Anonymous Authentication Scheme for Wireless Sensor Networks in the Internet of Things: Safe and Privacy-Preserving
9	Elgamal Cryptography, Cloud Security	Elgamal Hyper Elliptic Curve Cryptography with Fuzzy Logic for Secure Cloud-Based Storage
10	Cloud Computing Security Challenges	Services, Deployment Models, and Security Issues in Cloud Computing
11	AES	Cloud Data Security with AES
12	ECC	Elliptic Curve Cryptography-Based Secure User Authentication Protocol
13	AES	An Overview of AES, or the Advanced Encryption Standard
14	Security of Edge Computing	Group Security and Multi-Cloud Load Distribution for Information in Edge-Based Computing Uses
15	Encrypting Data in Cloud Storage through Cryptographic Techniques	Utilizing Cryptographic Mechanisms for Data Security and Privacy Preservation in Cloud Storage Environments

Moreover, Kumari et al. [12] specifically focus on secure user authentication through Elliptic Curve Cryptography (ECC). Papers like Conrad et al. [13] offer an overview of security mechanisms like AES. Furthermore, Dornala [14] and Kaaniche and Laurent [15] address multi-cloud load balancing, ensemble security, and privacy preservation in cloud storage, respectively. Each paper contributes significantly to understanding and implementing diverse security strategies within IoT, cloud computing, and related technological domains, covering a wide spectrum of security approaches from fundamental encryption protocols to intricate trust-based architectures.

3. Materials and Methods

3.1. Methodology

Integrating advanced security measures in cloud storage and medical data management represents a significant leap in fortifying information security. Specifically, the proposed solution amalgamates a two-factor authentication model with "Hyper Elliptical Curve Cryptography" (HECC), resulting in a robust and sophisticated security infrastructure tailored for cloud-based storage systems. This approach (BFHECC-IoMT) innovatively combines traditional authentication methods, such as passwords or PINs, with the advanced encryption capabilities of hyper elliptical curve cryptography. This fusion creates a multi-layered defense mechanism bolsters data encryption beyond standard security measures.

Utilizing these enhanced cryptographic protocols fortifies the overall security posture, ensuring a higher resilience against potential cryptographic attacks during cloud systems' data transmission and storage phases. Furthermore, integrating the Internet of Medical Things (IoMT) and cloud security, supported by Homomorphic Encryption and Elliptic Curve Cryptography (HECC), establishes an authoritative and influential framework tailored explicitly for managing highly sensitive medical information. This integration aims to ensure the protection and integrity of medical data throughout its lifecycle, addressing the healthcare sector's intricacies and stringent security demands. Homomorphic encryption enables secure computation and analysis of encrypted medical data without decryption, ensuring heightened privacy.

Simultaneously, Elliptic Curve Cryptography offers robust encryption techniques ideally suited for Internet of Things (IoT) devices, thus preserving the confidentiality and integrity of the transmitted and stored medical information. This comprehensive approach emphasizes secure data transmission and adheres to patient privacy standards, ensuring compliance with vital healthcare regulations like HIPAA (Health Insurance Portability and Accountability Act). The aim is to create a secure, privacy-preserving, and integrity-upholding environment for medical data within the healthcare sector. The proposed system (BFHECC-IoMT) Bi-Factor Authentication and Hyper Elliptical Curve Cryptography in IoT-Enabled Cloud Data Protection, which consists of four entities - the data generator, signcrypter, certificate authority, and server - as well as the verifier or unsigncrypter, is shown in Figure 1 of our proposed model. The certificate authority publishes all public parameters, including m, $\hbar 1$, $\hbar 2$, $\hbar 3$, $\mathscr{E}/\mathcal{D}$, HEC($\oint q$), $\oint q$, and q, before starting communication.

After verifying the verifier's public key received from the certificate authority, the data generator signs using a new nonce and continues the encryption process. The data generator creates the signcryptext, uploads it to the server, and the server sends it to the intended recipient or verifier. The unsigncryption procedure is then carried out by the verifier after confirming the data generator's or signcrypter's public key.

3.2. Key Generation

There are several steps in the critical generation process. A key generator is first used to generate an AES key, initializing the required size and then developing the secret key. A standard algorithm is used for data encryption and decryption using AES while the data is at rest. This entails establishing a cipher, setting it up for encryption, and then carrying out the encryption or decryption operation on the file. Regarding the cloud's second layer of security, Hyper Elliptic Curve Cryptography (ECC) uses two generated keys - a public key and a private key-typical of asymmetric keys.

The specification of the finite field, represented as P, the coefficients a and b for defining the curve, the generator point G, where the operations start, the order of G (n), and the ratio between the total points on the curve and the order of G (h) are among the fundamental components of the HECC system parameters that define the system. Algorithm 1 uses the signcrypter's private key, divisor, the public key of the unsigncrypter, and the message represented by ($\mathcal{J}u,, ds, m$). The algorithm produces the cipher text and corresponding signature based on this input. After that, Bob or the unsigncrypter receives the output ω = ($\boldsymbol{\mathcal{C}}$,,) for additional processing.

Algorithm 1 ($\mathcal{J}u,,$).

1. Select a number γ randomly from the set {1,..., q-1}.
2. Select a nonce number.
3. Calculate $\mathcal{Z} = \gamma.\mathcal{D} \ mod \ \boldsymbol{\varepsilon}$, in which $\mathcal{D}$ represents a hyperelliptic curve's divisor.
4. Split $\mathcal{Z}$ into xz and $y\boldsymbol{\xi}$.
5. Determine $\mathscr{b} = \hbar 1(O//xz.\mathrm{Nr})$.
6. Determine that $\mathcal{K} = \hbar 2((\gamma + \mathcal{X}.\ ds).\ \mathcal{J}u)$.
7. Divide $\mathcal{K}$ into $x\mathcal{K}$ and $y\mathcal{K}$.
8. Calculate $\mathscr{M} = O.\mathcal{D}$.
9. Determine $\boldsymbol{\mathcal{C}} = ((\mathscr{M},\mathrm{Nr}))$.
10. Determine $v = \hbar 3(\boldsymbol{\mathcal{C}})$.
11. Determine that $\boldsymbol{\mathcal{S}} = \gamma^{-1}(ds\mathcal{X} - \mathcal{T}) mod\ q$.

Send ω = ($\boldsymbol{\mathcal{C}}$, $\mathcal{X}$, $\mathcal{S}$) to Unsigncrypter or Bob.

The first algorithm ($\mathcal{J}u$,, ds,m) involves several steps. Initially, a number γ is randomly chosen from the set {1,…,q -1}, followed by selecting a nonce Nr. Subsequently, $\mathcal{Z}$ is computed as γ multiplied by $\mathcal{D}$ modulo q, where $\mathcal{D}$ represents the divisor on a hyper-elliptic curve, and this resulting value is divided into xz and yz.

Further steps involve calculating $\mathcal{X}$ using $\hbar 1$ based on specific parameters, the computation of $\mathcal{K}$ utilizing $\hbar 2$ with additional factors and breaking down $\mathcal{K}$ into $x\mathcal{K}$ and $y\mathcal{K}$. The algorithm then proceeds to determine $\mathcal{M}$ as the product of m and $\mathcal{D}$, followed by the computation of $\boldsymbol{\mathcal{C}}$ using specific encryption operations.

It evaluates $\boldsymbol{\mathcal{T}}$ and $\boldsymbol{\mathcal{S}}$ based on different mathematical calculations using the previously obtained parameters. Eventually, the resulting data, represented as ω = ($\boldsymbol{\mathcal{C}}$, $\mathcal{X}$,), is transmitted to either Bob or the Unsigncrypter, completing the sequence of operations defined by the algorithm.

3.3. Encryption, Decryption, and Verifying the Signature

The encryption, decryption, and signature verification algorithms describe a set of actions taken during secure communication between a sender and a recipient in an encrypted communication environment. Message'm' is converted to cipher text for safe transmission to start the encryption process. At first, the message, 'm,' is recognized as a point on an elliptic curve, M. The sender then selects a random number, 'k,' from the range of [1, n-1]. This section is essential to producing the cipher text, which comprises two points, C1 and C2. Multiplying 'k' by a base point, G, yields C1, while the product of k*G and the sum of M yield C2.

After receiving the encrypted text, the recipient applies the decryption algorithm to recover the original plain text. The receiver uses its private key to calculate the product of C1 in this process. The receiver then recovers the original message, M, by subtracting this product from the second point, C2. Verifying the signature's authenticity involves several critical steps. The receiver must know the sender's public key, PA, which remains readily available within the cloud space. The verification commences with the receiver ensuring that the pairs (r, s) are within the array of [1, 1-n].

Subsequently, the receiver calculates the hash function' e,' similar to the process during signature generation. Further calculations involve determining 'w' as s-1 mod(n), computing u1 as e * w (mod n), u2 as r * w (mod n), and calculating (x1, y1) = u1 * G + u2 * PA. Ultimately, the validity of the signature is confirmed by evaluating if x1 is equivalent to r (mod n). This comprehensive framework of encryption, decryption, and signature verification algorithms ensures secure, authenticated, and confidential communication between the sender and the receiver, ensuring the integrity and authenticity of transmitted messages. Integrating these cryptographic methodologies establishes a robust, secure foundation for data transfer and communication integrity.

Algorithm SenderReceiver Communication (m, k, dB, r, s, n, G, M, C1, C2, PA, e):

Encryption Algorithm 2

- M = m # Assigning message m to a point M on the elliptic curve
- k = random([1, n-1]) # Sender generates a random number k
- C1 = k * G # Computation of the first cipher text component C1
- C2 = M + (k * G) # Computation of the second cipher text component C2

Decryption Algorithm 3

- M = C2 - (dB * C1) # Receiver decrypts the cipher text to retrieve the original message

Algorithm 4 for Signature Verification

- if (r, s) ∈ [1, 1-n]:
- # Verifying that (r, s) falls inside the given range e = hash(r, s)
- # The hash function' e' is calculated by the recipient: w = s^(-1) mod n
- # The recipient computes w: u1 = (e * w) mod n
- For u1, the formula is u2 = (r * w) mod n.
- For u2, the formula is (x1, y1) = (u1 * G) + (u2 * PA). # (x1, y1) computation
- if x1 ≡ r (mod n): # Verifying that x1 equals r (mod n) for the signature to be valid #The signature is still enforceable.

The integration of advanced security measures for cloud storage and medical data management, emphasizing the proposed integration of two-factor authentication with hyper elliptical curve cryptography, aimed at fortifying data security in cloud systems and managing sensitive medical information in a robust security framework. Algorithm 1 details the essential generation process, creating a robust system for cryptographic operations. Furthermore, the content describes the Encryption, Decryption, and Verifying Signatures process, outlining specific steps for encryption and decryption, followed by signature verification in a secure communication environment.

Finally, an algorithm is provided to represent the overall process for secure communication. The summary encompasses the text's fundamental content and critical elements, emphasizing the integration of advanced security methods, key generation, encryption, decryption processes, and signature verification steps in a secure communication framework.

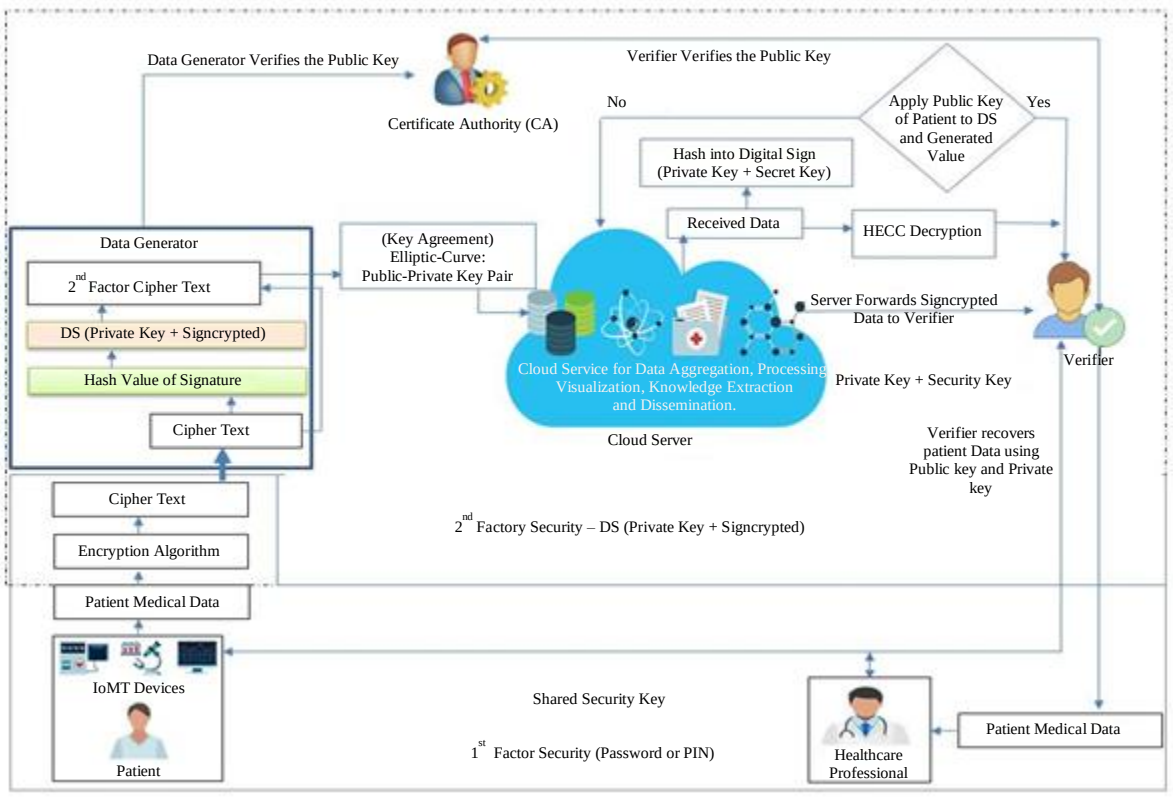

Fig. 1 Proposed system model

4. Results and Discussion

The comparative analysis between the existing system utilizing two-factor authentication with hyper elliptical curve cryptography and the proposed system reveals key disparities in their performance parameters. This comparison emphasizes the proposed system's distinct advantages in fortifying data security within cloud systems and managing sensitive medical information. The existing system relies on conventional authentication and encryption methods, potentially leaving vulnerabilities against sophisticated cyber threats.

Table 2. Result and discussion of various parameters with the existing method

Parameters	[16] Signcryption Method	[17] Certificateless Key-Insulated Scheme	[18] Public Verifiability Signcryption Technique	[19] Secured Signcryption Method	Proposed Method (BFHECC-IoMT)
Computational Cost	5 - Elliptic Curve Point Multiplication	5 - Elliptic Curve Point Multiplication	5 - Elliptic Curve Point Multiplication	6 - Elliptic Curve Point Multiplication	6 - Elliptic Curve Point Multiplication
	4.45 (ms)	4.3 (ms)	4.5 (ms)	5.2 (ms)	3.1 (ms)
Communication Cost	$\mathcal{C}+\|\mathcal{H}\|+2\|\rho\|$	$\mathcal{C}+\|\mathcal{H}\|+2\|\rho\|$	$\mathcal{C}+\|\mathcal{H}\|+2\|\rho\|$	$\mathcal{C}+\|\mathcal{H}\|+\|\rho\|$	$\mathcal{C}+\|\mathcal{H}\|+\|\rho\|$
128 bits-	602	602	414	288	240
256 bits-	731	731	566	410	400
1024 bits-	1500	1500	1500	1300	1100

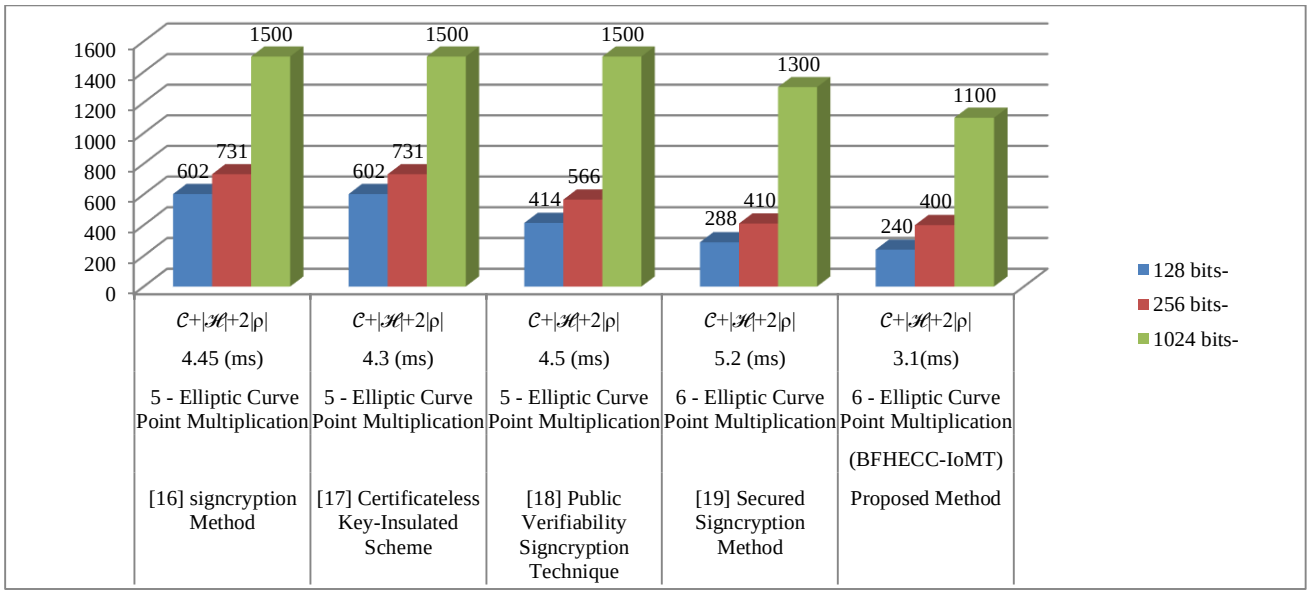

Fig. 2 Result and discussion of various parameters with the existing method

In contrast, the proposed system integrates advanced two-factor authentication with hyper elliptical curve cryptography, significantly bolstering data encryption and overall security. By employing HECC, the proposed system offers superior protection against potential breaches and cryptographic attacks, ensuring higher resistance to unauthorized access.

Moreover, the proposed system effectively ensures data integrity, confidentiality, and compliance with healthcare regulations. While the existing system maintains a certain level of integrity and privacy, it might be more vulnerable to unauthorized access due to reliance on conventional security measures. The proposed system, specifically designed for managing sensitive medical data, integrates advanced security techniques to guarantee enhanced data integrity and confidentiality.

It significantly reduces the risk of potential breaches, leaks, and unauthorized access. The proposed system complies more with stringent healthcare regulations like HIPAA, ensuring better patient data privacy and security. Additionally, the proposed system shows superior resilience against evolving cyber threats. While the existing system could be susceptible to vulnerabilities in the face of advancing threats, the proposed system, fortified by HECC and advanced authentication mechanisms, showcases adaptability and robustness against a broad spectrum of potential risks.

This comprehensive comparison emphasizes the substantial advantages of the proposed system over the existing one, particularly in terms of security, data integrity, healthcare regulation compliance, and resilience to evolving cyber threats.

Table 3. Security level comparison of various methods with BFHECC-IoMT

Security Level (bit)	[16] Signcryption Method Key Size (bit)	[17] Certificateless Key-Insulated Scheme Key Size (bit)	[18] Public Verifiability Signcryption Technique Key Size (bit)	[19] Secured Signcryption Method Key Size (bit)	Proposed Method (BFHECC-IoMT) Key Size (bit)
256	200	224	255	240	96
512	285	290	298	290	128
1024	365	365	370	404	176
2048	425	420	422	462	236

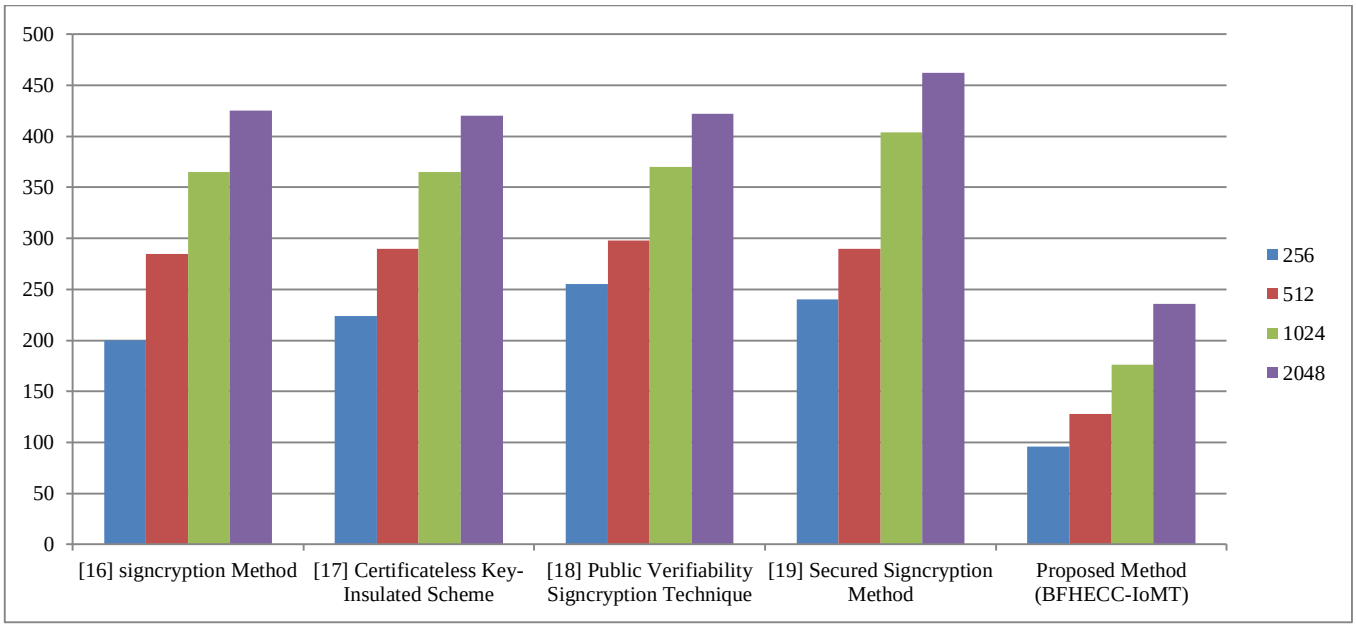

Fig. 3 Security level comparison of various methods with BFHECC-IoMT

5. Conclusion

The significance of robust security measures for cloud-stored sensitive information and medical data reflects the contemporary technological landscape. While established methods like TLS, multi-factor authentication, and access controls provide a degree of security, they often encounter vulnerabilities like misconfigurations or breaches, necessitating continual enhancements.

The proposed BFHECC-IoMT solution combines two-factor authentication and hyperelliptical curve cryptography, offering a potent security framework for cloud storage. This framework strengthens data encryption by amalgamating traditional and hyper-elliptical curve-based authentication methods. It fortifies security beyond typical measures, increasing resistance to cryptographic attacks during data transmission and storage. Moreover, integrating IoMT and cloud security, reinforced by Homomorphic Encryption and Elliptic Curve Cryptography (HECC), establishes a robust security framework specifically designed for managing sensitive medical information. Addressing existing healthcare system gaps, this integration ensures enhanced data confidentiality and integrity during transmission and storage.

Uniting IoMT, cloud security, Homomorphic Encryption, and ECC facilitates secure data transfer from IoT devices to cloud systems, ensuring stringent security standards for maintaining confidentiality, integrity, and availability. This comprehensive approach secures patient data transmission and provides privacy during analysis, compliance with healthcare regulations, and the overall secure handling and analysis of health data within the healthcare sector.

References

[1] Md. Alimul Haque et al., "Security and Privacy in Internet of Things," *International Conference on Emerging Technologies in Computer Engineering*, Switzerland, pp. 226-235, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] M. Vijayakumar, and T.S. Shiny Angel, "A Survey on IoT Security: Security Threads and Analysis of Botnet Attacks over IoT and Avoidance," *Cyber Security, Privacy and Networking*, pp. 141–154, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] El Mahdi Boumait et al., "Survey IOT Systems Security Based on Machine Learning," *International Conference on Digital Technologies and Applications*, Fez, Morocco, pp. 251-258, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Sachin Gupta, Babita Yadav, and Bhoomi Gupta, "Security of IoT-Based e-Healthcare Applications Using Blockchain," *Advances in Blockchain Technology for Cyber Physical Systems*, pp. 79–107, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Volkan Dedeoglu et al., "A Trust Architecture for Blockchain in IoT," *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, Houston, USA, pp. 190–199, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Bhabendu Kumar Mohanta et al., "Addressing Security and Privacy Issues of IoT Using Blockchain Technology," *IEEE Internet Things Journal*, pp. 881-888, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Mohammad Wazid, Ashok Kumar Das, and Sachin Shetty, "TACAS-IoT: Trust Aggregation Certificate-Based Authentication Scheme for Edge Enabled IoT Systems," *IEEE Internet Things Journal*, vol. 9, no. 22, pp. 22643–22656, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Qi Xie, Zixuan Ding, and Bin Hu, "A Secure and Privacy-Preserving Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things," *Security, Privacy and Reliability in Cloud-Based Internet of Things*, vol. 2021, pp. 1-12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] A. Pasumpon Pandian, "Development of Secure Cloud Based Storage Using the Elgamal Hyper Elliptic Curve Cryptography with Fuzzy Logic Based Integer Selection," *Journal of Soft Computing Paradigm*, vol. 2, no. 1, pp. 24-35, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Shubham Gupta, Anand Gupta, and Gori Shankar, "Cloud Computing: Services, Deployment Models and Security Challenges," *2nd International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, pp. 414-418, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Smitha Nisha Mendonca, "Data Security in Cloud Using AES," *International Journal of Engineering Research & Technology (IJERT)*, vol. 7, no. 1, pp. 205-208, 2018. [Google Scholar] [Publisher Link]

[12] Adesh Kumari et al., "A Secure User Authentication Protocol Using Elliptic Curve Cryptography," *Journal of Discrete Mathematics and Cryptography*, vol. 22, pp. 521-530, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[13] Eric Conrad, Seth Misenar, and Joshua Feldman, *Advanced Encryption Standard- An Overview*, Eleventh Hour CISSP:: Study Guide, 3rd Ed, pp. 1-221, 2016. [Google Scholar] [Publisher Link]

[14] Raghunadha Reddi Dornala, "Ensemble Security and Multi-Cloud Load Balancing for Data in Edge-Based Computing Applications," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 14, no. 8, pp. 7-13, 2023. [Google Scholar] [Publisher Link]

[15] Nesrine Kaaniche, and Maryline Laurent, "Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms," *Computer Communications*, vol. 111, pp. 120-141, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ren-Junn Hwang, Chih-Hua Lai, and Feng-Fu Su, "An Efficient Signcryption Scheme with Forward Secrecy Based on Elliptic Curve," *Applied Mathematics and Computation*, vol. 167, no. 2, pp. 870-881, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[17] Caixue Zhou et al., "Certificateless Key-Insulated Generalized Signcryption Scheme without Bilinear Pairings," *Security and Communication Networks*, vol. 2017, pp. 1-17, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[18] Hassan M. Elkamchouchi, Mohamed H. El-Atiky, and Eman Abouelkheir, "A Public Verifiability Signcryption Scheme without Pairings," *International Journal of Computer Applications*, vol. 157, no. 9, pp. 35–40, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[19] Insaf Ullah et al., "A Novel Provable Secured Signcryption Scheme: A Hyper-Elliptic Curve-Based Approach," *Mathematics*, vol. 7, no. 8, pp. 1-16, 2019. [CrossRef] [Google Scholar] [Publisher Link]