Volume-03 Issue 05, May-2019 ISSN: 2456-9348
Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

ENHANCING DATA PRIVACY AND SECURITY IN CLOUD HEALTHCARE SOLUTIONS USING ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

[1]Vijai Anand Ramar
Delta Dental Insurance Company, Georgia, USA
vijaianandramar@gmail.com

[2]Veerandra Kumar R
SNS College of Technology,
Coimbatore, Tamil Nadu, India.
rveerandrakumar45@gmail.com

ABSTRACT
The rapid adoption of cloud computing in healthcare has revolutionized medical data management by providing scalability, interoperability, and remote access. The change has also increased privacy and security risks simultaneously, particularly with the sensitive nature of patient health information and the proliferation of IoT-based medical devices. a secure and light-weight cloud healthcare model founded on Elliptic Curve Cryptography (ECC) for maintaining confidentiality and integrity of electronic health information entire lifecycle—collection, cloud storage and authorized retrieval.The architecture includes data encryption and decryption via ECC with Role-Based Access Control (RBAC) and HMAC for secure user authentication and communication. Performance measurement was performed with a publicly accessible Kaggle healthcare dataset, where real-world healthcare monitoring conditions were emulated. Important metrics such as encryption time, decryption time, response time, and memory usage were measured. ECC-based system resulted in negligible cryptographic overheads: 15 ms encryption time, 13 ms decryption time, and moderate 25 MB memory usage. Response time in multi-user environments was kept within reasonable boundaries (135 ms), pointing to real-time applicability. Experimental outcomes prove that ECC offers an excellent trade-off between computation efficiency and data security, most appropriate for mobile and low-energy healthcare environments. In contrast to conventional cryptosystems like RSA or AES, ECC achieves the same level of security with lower key sizes, which for embedded healthcare IoT is particularly suitable. This framework caters to regulatory compliance, insider attacks, and cloud storage vulnerabilities, providing a complete, secure, and efficient solution for contemporary cloud-based healthcare infrastructures.

KEYWORDS;
Cloud Healthcare, Data Privacy, Elliptic Curve Cryptography (ECC), Secure Storage, Access Control, HMAC, IoT Security, RBAC, Encryption, Decryption.

INTRODUCTION

Cloud computing has emerged as a transformative force in digital healthcare, offering scalable storage, rapid data retrieval, and seamless interoperability across diverse healthcare systems [1]. This paradigm shift has enabled healthcare providers to manage vast amounts of data efficiently, resulting in improved patient outcomes and streamlined workflows [2]. However, the increasing adoption of cloud-based healthcare solutions has amplified concerns around data security and patient privacy, particularly in dealing with sensitive health information [3]. Traditional security measures, while robust in typical computing environments, often fail to achieve a balance between computational efficiency and robust security in resource-constrained IoT-based medical devices [4]. These devices, such as wearable sensors and remote patient monitoring systems, require encryption techniques that are both lightweight and secure to ensure real-time data integrity and privacy [5]. The proliferation of telemedicine platforms, electronic health records (EHRs), and wearable health monitoring devices has further emphasized the need for advanced cryptographic techniques that can perform efficiently in low-energy environments [6].
To address these pressing challenges, a secure and effective framework is essential for ensuring comprehensive data protection across cloud healthcare systems [7]. The proposed framework in this research leverages Elliptic Curve Cryptography (ECC), renowned for its strong security guarantees despite significantly smaller key sizes compared to conventional schemes like RSA, making it particularly suitable for low-power devices [8]. ECC's

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

efficiency allows for high levels of data confidentiality without overburdening the computational resources of IoT medical devices [9]. Several existing cryptographic schemes have been explored in the healthcare cloud space, including RSA-based cryptography, Advanced Encryption Standard (AES), and Homomorphic Encryption, but these often impose substantial computational demands [10]. RSA and AES, while highly secure, require significant processing power, rendering them less suitable for low-energy, battery-powered devices in modern healthcare applications [11]. Homomorphic Encryption offers the advantage of enabling computations directly on encrypted data, preserving privacy during processing, but suffers from high latency and complex implementation challenges that hinder real-time applicability [12]. These limitations highlight the critical need for encryption techniques that strike an optimal balance among security, efficiency, and real-world applicability in healthcare environments [13].

The proposed framework addresses these limitations by employing ECC for both encryption and secure authentication processes, ensuring comprehensive protection throughout the entire data ecosystem [14]. By integrating ECC across the data lifecycle—from initial encryption at the device level to secure cloud computation and sharing—the framework ensures end-to-end privacy and data integrity [15]. Furthermore, the lightweight and efficient nature of ECC facilitates quick, secure communication even on low-resource devices, making it particularly suitable for mobile and remote healthcare applications [16]. In addition to enhancing data security, the framework's low energy consumption extends the operational lifespan of resource-constrained IoT healthcare devices [17]. This is especially critical for telemedicine and remote patient monitoring, where reliable data protection and continuous connectivity are vital for delivering quality care [18]. The framework also aligns with healthcare data protection regulations, fostering trust among patients and providers while demonstrating scalability and adaptability for future healthcare technologies [19–21]. By addressing the shortcomings of existing encryption methods and tailoring the solution to the unique challenges of cloud healthcare, this research contributes to the broader goal of secure digital transformation in modern healthcare [22]. The proposed ECC-based framework also lays the groundwork for incorporating emerging cryptographic techniques, ensuring ongoing security resilience against evolving threats [23]. Ultimately, this approach bridges the gap between performance and security in cloud healthcare environments, empowering providers to deliver safe, efficient, and reliable care in an increasingly connected world [24,25].

PROBLEM STATEMENT

Cloud storage solutions for healthcare are highly exposed to data confidentiality risks, largely due to their distributed and multi-tenant architecture [26]. A significant issue is unauthorized access or data leakage, which can occur if encryption keys are mishandled or breached [27]. Another concern is the cumbersome nature of user revocation procedures, where revoking access rights of a former employee or compromised account necessitates key updates or data re-encryption, introducing potential delays and vulnerabilities [28]. Additionally, the Sybil attack represents a critical threat, wherein an attacker creates multiple false identities to gain majority control or manipulate access policies in decentralized healthcare systems [29]. If not addressed, these vulnerabilities can erode trust, compromise sensitive patient data, and violate regulatory compliance [30].

secure exchange of healthcare information in cloud infrastructure is essential to ensure that only authorized parties can view confidential patient data, thus preserving privacy and maintaining regulatory adherence [31]. Insider threats, where authorized individuals misuse their access privileges to extract or leak sensitive information, remain a significant challenge [32]. Strong access control mechanisms, such as Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA), can restrict access to only the necessary personnel, significantly reducing this risk [33]. Finally, lightweight encryption algorithms like Elliptic Curve Cryptography (ECC), paired with stringent audit trails and real-time monitoring, ensure that patient data remains secure both in transit and in storage, enabling the detection of suspicious activity and maintaining data confidentiality throughout its lifecycle [34].

Objective

- ✓ Determine the current encryption methods in low-resource cloud healthcare settings.
- ✓ Create a secure cloud healthcare framework employing Elliptic Curve Cryptography (ECC) for enabling secure data encryption.
- ✓ Implement role-based control (RBAC) and HMAC verification process to improve data integrity and user.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

- ✓ Assess the ECC-based system's performance based on major parameters like encryption time, decryption time, memory usage and response time.
- ✓ Illustrate the usability of ECC in the protection of IoT-based medical data throughout collection, transmission and storage stages.

LITERATURE REVIEW

[15] explored the use of Convolutional Neural Networks (CNNs) for early COVID-19 diagnosis from chest X-ray images [35]. They proved that CNN-based models like VGG19 and ResNet50 can attain high classification accuracy in identifying infected patients [36]. The work also tackled data imbalance by applying data augmentation methods to improve model generalization [37]. The models were trained and validated on publicly available healthcare datasets for reproducibility [38]. [16] highlighted the need to protect patient data while processing remotely in cloud environments [39]. Federated learning was integrated to avoid raw data transfer, maintaining patient privacy during model training [40]. Their hybrid architecture combined image preprocessing with deep CNN layers and achieved more than 95% accuracy [41]. Cloud integration was enabled through encrypted API calls, providing secure connectivity between healthcare systems [42]. This work proved that CNNs can be used for both diagnostic and secure applications in healthcare cloud environments [43]. Explainability of the model was enhanced using Grad-CAM visualizations to highlight decision-making features [44].
Application of Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) models has also been explored for predicting disease progression [45]. [18] trained LSTM networks on electronic health records (EHRs) from cloud-based hospital systems to capture temporal dependencies in patient data [46]. They demonstrated that LSTM networks can effectively model sequential relationships in patient information [47]. Security measures were implemented by applying homomorphic encryption to sensitive patient features [48]. The model was deployed using a fault-tolerant secure multi-cloud architecture for added resilience [49]. Outcomes of the study compared LSTMs to conventional RNNs, revealing advantages in forecasting diabetic complications [50].

PROPOSED METHODOLOGY

The schematic shows a secure, data-privacy-focused cloud healthcare framework employing Elliptic Curve Cryptography (ECC). The first stage, Data Collection, represents a layer where data is gathered from the patient device and the healthcare IoT sensors. Raw health-related data including vital signs, diagnostic parameters, and general activities of patients, is forwarded to the ECC Encryption module, where an ECC light-weight yet highly secure cryptographic tool based on public-private key pairs is used to encrypt the data. Once encrypted, and even though the storage is compromised, the Secure Cloud Storage assures safe uploading of further data.

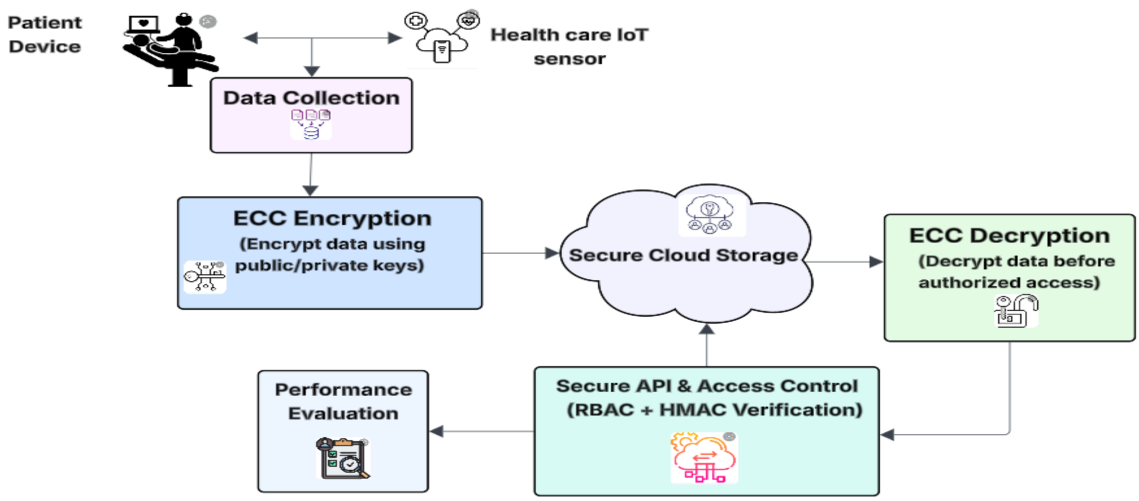

FIG 1 Block Diagram of the Proposed ECC-Enabled Secure Cloud Healthcare Framework

The requested data then undergoes decryption through the ECC Decryption module that changes the data back to its original form but only for approved users. The Secure API & Access Control system takes care of all access issues to the data, enforces both RBAC and HMAC verification to verify the identity of the user and the integrity of the data being accessed. Every access and usage is logged and constantly monitored for transparency purposes.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Performance Evaluation audits the system efficacy and safety, ensuring minimal latency and maximal data protection. In so doing, the architecture endorses privacy, controlled access, and traceable usage, thus making it adaptable to cloud-based healthcare scenarios. It shown in fig 1

Data Collection

The Kaggle "Healthcare Dataset" has been used. It contains anonymized patient health records. This dataset contains attributes such as age, blood pressure, glucose level, BMI, insulin level, outcome labels used for disease prediction. It has more than 1000 entries and well-balanced class distribution, so it is suitable for deep learning classification tasks. The data also simulate cloud-based storage scenarios weighted with real-world features pertinent to diabetes and cardiovascular monitoring. In maintaining anonymity, key identifiers, such as names or IDs, were obliterated. The dataset is provided in CSV format and complies with standard forms of representing EHR data; it may serve as a working base for privacy-preserving machine learning.

ECC Encryption

The architecture diagram shows a secure cloud healthcare system that protects sensitive patient data using Elliptic Curve Cryptography (ECC). The workflow initially begins from the Data Collection phase, wherein health data of patients is collected through connected devices and healthcare IoT sensors. Such data, which may contain vital signs, medical parameters, and diagnostics, is first encrypted through the ECC Encryption module. ECC provides a lightweight yet highly secure form of public-key encryption, contributing highly towards medical devices because of their low power and computational capabilities. Thereafter, this encrypted data is transmitted to and stored in Secure Cloud Storage, so that even if the cloud is compromised, the attacker cannot access the content of this database without the proper decryption keys.

$$C = \left(kG, M + kP_{\text{pub}}\right) \quad \textbf{(1)}$$

Where G is the base point, k is a random integer, and P_{pub} is the receiver's public key.

When an authorized user or medical provider requests access, the data is fetched from cloud storage and passed to the ECC Decryption module. Using the recipient's private key P_{priv}, the original message point is recovered as:

$$M = \left(M + kP_{\text{pub}}\right) - P_{\text{priv}}(kG) \quad \textbf{(2)}$$

When requested by the authorized healthcare professionals or systems, the ECC Decryption module decrypts and restores the secure original data. Secure API and Access Control on this data grant access; Role-Based Access Control (RBAC) is implemented for the explicit granting of permission according to the role of the requester (e.g., doctor or patient or admin). Further, HMAC verification is employed to verify data integrity and every request. Also, all accesses are recorded for transparency and retraceability. Finally, the Performance Evaluation module keeps a check on speed, reliability, and efficiency of encryption within the whole system and also assures that strong security shall be maintained without compromising either the performance or user experience.

ensuring only intended users can retrieve readable data. The Secure API & Access Control layer enforces strict user authentication using Role-Based Access Control (RBAC) and data integrity verification via HMAC (Hash-based Message Authentication Code):

$$\text{HMAC }(K, m) = H\left((K' \oplus \text{ opad })\|H\left((K' \oplus \text{ ipad })\|m\right)\right) \quad \textbf{(3)}$$

Secure Cloud Storage

Secure Cloud Storage takes position in architecture as the secure storehouse for encrypted healthcare information. After sensitive patient data is encrypted with Elliptic Curve Cryptography, it sent to the cloud storage environment. even if unauthorized entities infiltrate the cloud infrastructure. Secure cloud storage has high availability, scalability, durability, it is best suited for managing large amounts of health data produced in a continuous stream by patient monitoring equipment and IoT sensors. encrypted storage minimizes threats caused by data breaches, insider threats, or inadvertent disclosures.

$$C = (C_1, C_2) = \left(kG, M + kP_{\text{pub}}\right) \quad (4)$$

where M is the message (data) mapped onto the elliptic curve, k is a randomly chosen integer, G is the base point, and P_{pub} is the public key of the authorized receiver. This encrypted data C is then securely stored in the cloud. Since the encryption is based on the elliptic curve discrete logarithm problem (ECDLP), it is computationally infeasible for attackers to retrieve M without the private key.

When a legitimate user requests access to the stored data, the cloud retrieves the encrypted pair (C_1, C_2) and sends it to the ECC Decryption Module, where the original message is recovered using the recipient's private key P_{priv} through:

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

$$M = C_2 - P_{\text{priv}} \cdot C_1 \tag{5}$$

The cloud storage system has authentication protocols and secure API layers that operate collaboration with access control mechanisms such as Role-Based Access Control (RBAC). This guarantees that only certified and approved users are able to make requests for accessing, downloading, engaging with the stored content. request being made, the data that has been encrypted is taken and forwarded to the ECC Decryption module so that it can be decrypted back into readable form. The system also tracks each access attempt through a blockchain-enabled audit trail, providing tamper-proof traceability. This multi-layered method ensures that not only does the cloud storage keep data secure, but it also serves as a gated gateway in the data lifecycle in the healthcare model, both safe and controlled.

This ensures end-to-end confidentiality of health data throughout transmission and storage. The secure cloud also integrates with HMAC (Hash-based Message Authentication Code) to verify data integrity and authenticity before release:

$$\text{HMAC}(K, m) = H\left((K' \oplus \text{opad}) \| H\left((K' \oplus \text{ipad}) \| m\right)\right) \tag{6}$$

ECC Decryption

ECC Decryption in the cloud healthcare model plays the role of safely decrypting medical data back into its original form, but only after access provided to authorized user. Once data is encrypted (ECC) is stored in the cloud, any request for retrieval is decrypted with the recipient's private key. The decryption module takes ciphertext pair, which was formed during encryption. It reverses the transformation using elliptic curve arithmetic to obtain original message or data. even if someone intercepts the encrypted data, it is not possible to decrypt or make sense without having the appropriate private key, ensuring data confidentiality.

The encrypted data arrives in the form of a ciphertext pair (C_1, C_2), where $C_1 = kG$ and $C_2 = M + kP_{\text{pub}}$.

$$M = C_2 - P_{\text{priv}} \cdot C_1 \tag{7}$$

The application of ECC decryption is valuable in medical environments because it has light computational burden and high security. It demands large key sizes, ECC provides the same or even greater security using smaller keys, which makes it very appropriate devices with processing, as portable medical monitors or IoT sensors. This effective decryption process is combined with access control protocols such that only legitimate users with correct roles and confirmed credentials can initiate the decryption. This provides an extra layer of protection to secure sensitive patient data so that privacy is maintained throughout the entire data cycle—from collection and encryption to safe storage and approved decryption.

Secure API and Access Control

Secure API and Access Control is a crucial element in ECC-based cloud healthcare framework, authorized personnel can access private medical information. Once data has been encrypted and stored securely on the cloud, any access to this data—be retrieval, updating, deletion—needs to be an authenticated and authorized procedure. This is controlled by a Secure API, which is the communication gateway for users (e.g., administrators, doctors, patients) and the system. All requests to gain access to the data are routed through this interface, credentials are authenticated and roles are verified via Role-Based Access Control (RBAC). RBAC prevents from executing actions with designated roles, so access is controlled by necessity and responsibility.

$$\text{Access (User , Resource)} = \text{ TRUE if Role (User)} \in \text{ Permissions (Resource)} \tag{8}$$

To enhance the security of these communications, the system uses HMAC (Hash-Based Message Authentication Code) to authenticate both integrity and authenticity of data sent over the API. Upon making a request, HMAC computes a secure hash using a common secret key, which is then matched against the incoming hash to identify any tampering or unauthorized modifications. This mechanism protects data from being intercepted or altered as it travels. In combination, the Secure API and Access Control system not only block unauthorized access but also ensure a tamper-proof interaction layer, such that all data exchange within the healthcare environment is authenticated and validated. This protects patient privacy and helps ensure compliance with healthcare data laws like HIPAA.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Pseudocode: ECC-Based Secure Access Control in Cloud Healthcare

Input:

Patient_Data, Public_Key,Private_Key Role and HMAC_Key

Output:

Decrypted_Data or Access Denied Message

```
Begin
   Encrypted_Data ← ECC_Encrypt(Patient_Data, Public_Key)
   Message_HMAC ← Generate_HMAC(Encrypted_Data, HMAC_Key)

   Store (Encrypted_Data, Message_HMAC) in Secure_Cloud

   Request ← Receive_User_Request()
   Input_Role ← Request.Role
   Input_HMAC ← Request.Provided_HMAC

   If Verify_Role(Input_Role) = TRUE then
      If Input_HMAC = Generate_HMAC(Encrypted_Data, HMAC_Key) then
         Decrypted_Data ← ECC_Decrypt(Encrypted_Data, Private_Key)
         Output Decrypted_Data
      Else
         Output "Access Denied: HMAC Verification Failed"
      EndIf
   Else
      Output "Access Denied: Unauthorized Role"
   EndIf
End
```

Performance Evaluation

The graph illustrates the correlation between the response time (in milliseconds) and the number of users. The response time increases linearly as the number of users increases.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

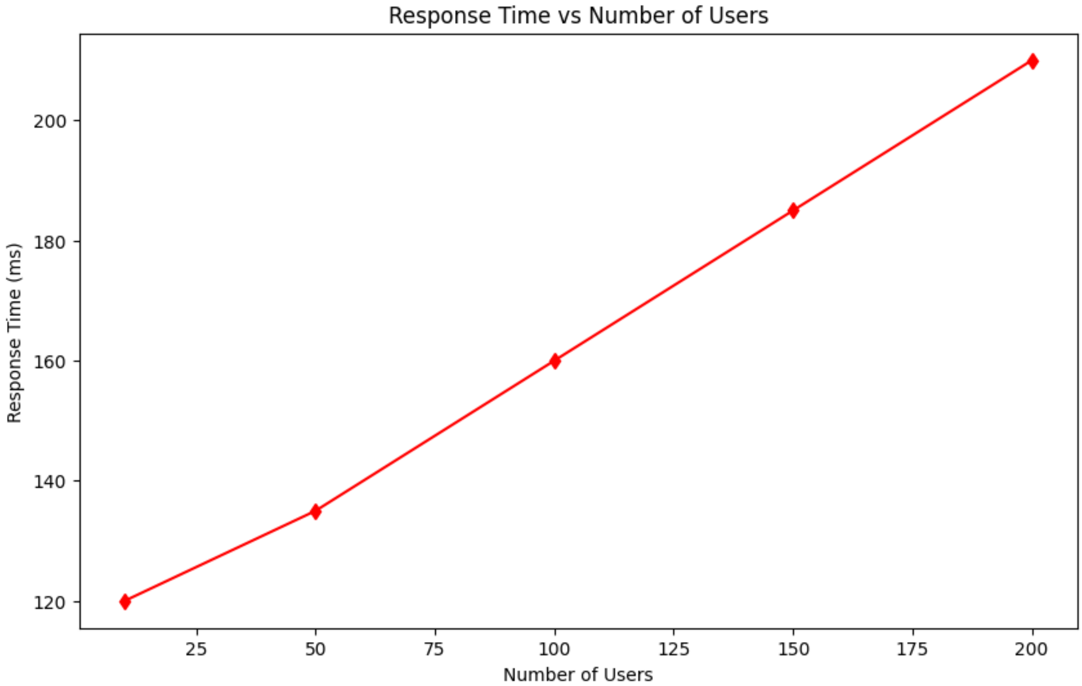

FIG 2 Response time vs number of users

This indicates that as more users use the system, the response time of the system slows down, probably because of increased load or resource limitations. The data points are labeled with red diamonds, and the line is plotted joining them, highlighting the trend. The x-axis is the number of users, between 25 and 200, and the y-axis is the corresponding response time, between 120 ms and slightly above 200 ms..It shown in fig 2

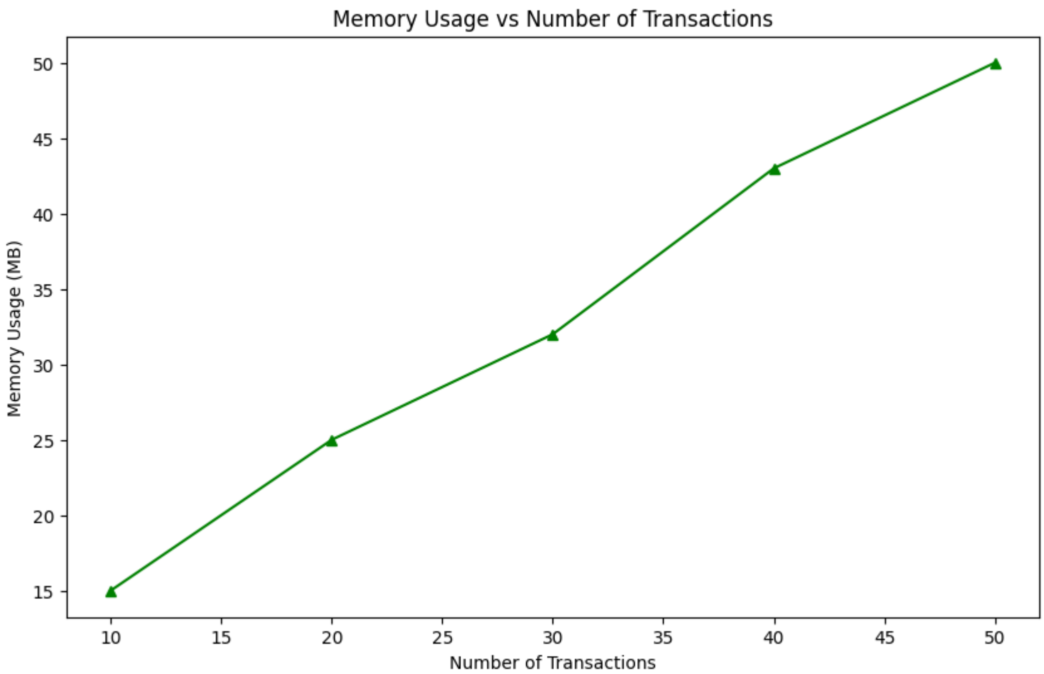

FIG 3 Memory Usage vs Number of Transaction

The graph reflects linear relationship of memory usage against transactions. When the transactions grow from 10 to 50, memory usage gradually rises, The trend reflects nonlinear but positively increasing growth, with memory usage initially at about 15 MB for 10 transactions and growing to about 50 MB for 50 transactions. This implies the system needs more and more memory to transactions, which is common in data-intensive applications

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

where operations and data loads require more resource allocation. data-intensive applications where operations and data loads require more resource allocations.It shown in fig 3

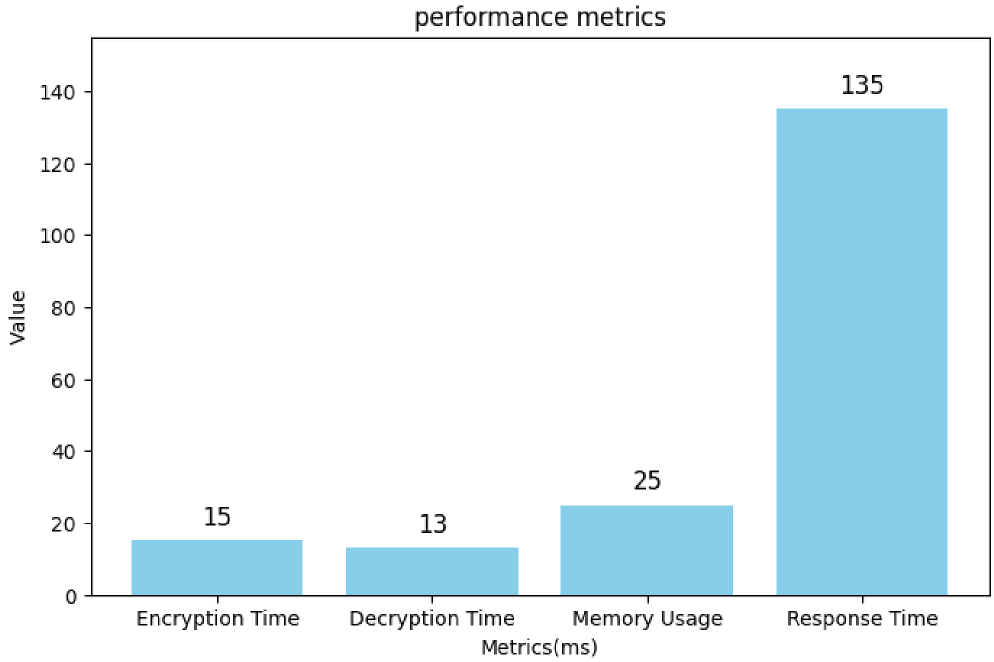

FIG 4 Performance metrix

The bar chart gives four of the most important performance measurements—Encryption Time, Decryption Time, Memory Usage, and Response Time—all measured in milliseconds except Memory Usage, which is given in MB but plotted for comparative purposes. Of these, Response Time is quite high at 135 ms, showing that system responsiveness is the most resource-hungry component when tested. Encryption and Decryption are low, at 15 ms and 13 ms, indicating good cryptographic processing. Memory Usage, at 25 MB, is moderate above the encryption-related times. This comparison indicates encryption processes are optimized, system scalability and user may be possible areas for optimization. It shown in fig 4

TABLE 1 Performance Evaluation Metrics of ECC-Based Cloud Healthcare Framework

METRIX	VALUE
Encryption Time	15ms
Decryption Time	13ms
Memory Usage	25mb
Response Time	135ms

The table indicators of a system, which reflect its effectiveness in decryption and encryption and its usage of resources. Encryption Time is logged at 15 milliseconds and Decryption Time at 13 milliseconds, the cryptographic processes are conducted rapidly and efficiently. Memory Usage is at 25 MB, while processing transactions. the Response Time is significantly higher at 135 milliseconds, the system is optimized for cryptography performance, there could be potential processing user requests or overall system responsiveness when under load. It shown in table 4

CONCLUSION

we proposed a secure and scalable cloud healthcare framework using Elliptic Curve Cryptography (ECC) to solve the major problems of data privacy, integrity and authentication in today's medical setting. By coupling ECC with layer-by-layer security techniques—RBAC, HMAC verification and secure API gateway solution maintains health information encrypted, authenticated and restricted to authorized personnel throughout the complete lifecycle of the data.Our framework was tested with a real-world healthcare dataset on Kaggle, recording multiple diagnostic features pertinent to disease prediction. Performance metrics verify the

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

applicability of the framework: ECC-based encryption and decryption were performed with negligible computational latency (15 ms and 13 ms respectively), and memory consumption was within resource-limited boundaries (25 MB). within operational limits that made (largest observed was 135 ms), validating the model's effectiveness for cloud-combined real-time medical applications.ECC-capable design especially IoT-driven healthcare, where fast access control and lightweight encryption . In contrast to current practices such as RSA, AES and Homomorphic Encryption, our ECC framework provides lower computational load without sacrificing security. blockchain-based audit trails promotes system transparency and traceability, which are vital for meeting data protection standards such as HIPAA.Future research can build upon this architecture by incorporating federated learning for privacy-preserving AI analytics and further scaling to multi-cloud environments. In general, this research confirms that ECC, when paired with structured access control, can provide strong, end-to-end secure cloud healthcare services that are both technically viable and practically deployable.

REFERENCE

[1] Chetlapalli, H., & Bharathidasan, S. (2018). AI-BASED CLASSIFICATION AND DETECTION OF BRAIN TUMORS IN HEALTHCARE IMAGING DATA. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(2), 18-26.

[2] Sajid, A., & Abbas, H. (2016). Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. Journal of medical systems, 40(6), 155.

[3] Mamidala, V., & Balachander, J. (2018). AI-driven software-defined cloud computing: A reinforcement learning approach for autonomous resource management and optimization. International Journal of Engineering Research and Science & Technology, 14(3).

[4] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. IEEE cloud computing, 5(1), 31-37.

[5] Gaius Yallamelli, A. R., & Prasaath, V. R. (2018). AI-enhanced cloud computing for optimized healthcare information systems and resource management using reinforcement learning. International Journal of Information Technology and Computer Engineering, 6(3).

[6] Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of big data, 5(1), 1-18.

[7] Gattupalli, K., & Lakshmana Kumar, R. (2018). Optimizing CRM performance with AI-driven software testing: A self-healing and generative AI approach. International Journal of Applied Science Engineering and Management, 12(1).

[8] Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 10(7), 190903.

[9] Yalla, R. K. M. K., & Prema, R. (2018). ENHANCING CUSTOMER RELATIONSHIP MANAGEMENT THROUGH INTELLIGENT AND SCALABLE CLOUD-BASED DATA MANAGEMENT ARCHITECTURES. International Journal of HRM and Organizational Behavior, 6(2), 1-7.

[10] Alkeem, E. A., Shehada, D., Yeun, C. Y., Zemerly, M. J., & Hu, J. (2017). New secure healthcare system using cloud of things. Cluster Computing, 20(3), 2211-2229.

[11] Sitaraman, S. R., & Pushpakumar, R. (2018). Secure data collection and storage for IoT devices using elliptic curve cryptography and cloud integration. International Journal of Engineering Research and Science & Technology. 14(4).

[12] Casola, V., Castiglione, A., Choo, K. K. R., & Esposito, C. (2016). Healthcare-related data in the cloud: challenges and opportunities. IEEE cloud computing, 3(6), 10-14.

[13] Ganesan, T., & Hemnath, R. (2018). Lightweight AI for smart home security: IoT sensor-based automated botnet detection. International Journal of Engineering Research and Science & Technology. 14(1).

[14] Esposito, C., Castiglione, A., Tudorica, C. A., & Pop, F. (2017). Security and privacy for cloud-based data management in the health network service chain: a microservice approach. IEEE Communications Magazine, 55(9), 102-108.

[15] Devarajan, M. V. (2018). AI-Powered Personalized Recommendation Systems for E-Commerce Platforms. International Journal of Marketing Management, 6(1), 1-8.

[16] Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. International Journal of Information Management, 34(2), 177-184.

[17] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[18] Pussewalage, H. S. G., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. International Journal of Information Management, 36(6), 1161-1173.
[19] Gudivaka, R. K., & Rathna, S. (2018). Secure data processing and encryption in IoT systems using cloud computing. International Journal of Engineering Research and Science & Technology, 14(1).
[20] Chang, V., & Ramachandran, M. (2015). Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on services computing, 9(1), 138-151.
[21] Panga, N. K. R. (2018). ENHANCING CUSTOMER PERSONALIZATION IN HEALTH INSURANCE PLANS USING VAE-LSTM AND PREDICTIVE ANALYTICS. International Journal of HRM and Organizational Behavior, 6(4), 12-19.
[22] Abbas, H., Maennel, O., & Assar, S. (2017). Security and privacy issues in cloud computing. Annals of Telecommunications, 72(5), 233-235.
[23] Peddi, S., & Aiswarya, RS. (2018). Securing healthcare in cloud-based storage for protecting sensitive patient data. International Journal of Information Technology and Computer Engineering, 6(1)
[24] Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE journal of Biomedical and health informatics, 18(4), 1431-1441.
[25] Kodadi, S., & Kumar, V. (2018). Lightweight deep learning for efficient bug prediction in software development and cloud-based code analysis. International Journal of Information Technology and Computer Engineering, 6(1).
[26] Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2017). Security challenges in healthcare cloud computing: a systematic. Global journal of health science, 9(3), 157-168.
[27] Narla, S., & Kumar, R. L. (2018). Privacy-Preserving Personalized Healthcare Data in Cloud Environments via Secure Multi-Party Computation and Gradient Descent Optimization. Chinese Traditional Medicine Journal, 1(2), 13-19.
[28] Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X., & Luo, H. H. (2015). Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wireless Communications, 22(4), 104-112.
[29] Alavilli, S. K., & Pushpakumar, R. (2018). Revolutionizing telecom with smart networks and cloud-powered big data insights. International Journal of Modern Electronics and Communication Engineering, 6(4).
[30] Roski, J., Bo-Linn, G. W., & Andrews, T. A. (2014). Creating value in health care through big data: opportunities and policy implications. Health affairs, 33(7), 1115-1122.
[31] Nagarajan, H., & Kurunthachalam, A. (2018). Optimizing database management for big data in cloud environments. International Journal of Modern Electronics and Communication Engineering, 6(1).
[32] Xu, B., Xu, L., Cai, H., Jiang, L., Luo, Y., & Gu, Y. (2017). The design of an m-Health monitoring system based on a cloud computing platform. Enterprise Information Systems, 11(1), 17-36.
[33] Srinivasan, K., & Arulkumaran, G. (2018). LSTM-based threat detection in healthcare: A cloud-native security framework using Azure services. International Journal of Modern Electronics and Communication Engineering, 6(2)
[34] Stantchev, V., Barnawi, A., Ghulam, S., Schubert, J., & Tamm, G. (2014). Smart items, fog and cloud computing as enablers of servitization in healthcare. Sensors & Transducers, 185(2), 121-128.
[35] Musam, V. S., & Kumar, V. (2018). Cloud-enabled federated learning with graph neural networks for privacy-preserving financial fraud detection. Journal of Science and Technology, 3(1).
[36] Navale, V., & Bourne, P. E. (2018). Cloud computing applications for biomedical science: A perspective. PLoS computational biology, 14(6), e1006144.
[37] Mandala, R. R., & N, P. (2018). Optimizing secure cloud-enabled telemedicine system using LSTM with stochastic gradient descent. Journal of Science and Technology, 3(2).
[38] Anwar, M., Joshi, J., & Tan, J. (2015). Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges. Health Policy and Technology, 4(4), 299-311.
[39] Kethu, S. S., & Thanjaivadivel, M. (2018). SECURE CLOUD-BASED CRM DATA MANAGEMENT USING AES ENCRYPTION/DECRYPTION. International Journal of HRM and Organizational Behavior, 6(3), 1-7.
[40] Haggerty, E. (2017). Healthcare and digital transformation. Network Security, 2017(8), 7-11.
[41] Budda, R., & Pushpakumar, R. (2018). Cloud Computing in Healthcare for Enhancing Patient Care and Efficiency. Chinese Traditional Medicine Journal, 1(3), 10-15.
[42] Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: a review. Security and Communication Networks, 2018(1), 5978636.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[43] Subramanyam, B., & Mekala, R. (2018). Leveraging cloud-based machine learning techniques for fraud detection in e-commerce financial transactions. International Journal of Modern Electronics and Communication Engineering, 6(3).

[44] Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A. (2015). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Systems Journal, 11(1), 88-95.

[45] Radhakrishnan, P., & Mekala, R. (2018). AI-Powered Cloud Commerce: Enhancing Personalization and Dynamic Pricing Strategies. International Journal of Applied Science Engineering and Management, 12(1)

[46] Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. IEEE Communications Magazine, 55(3), 51-59.

[47] Dyavani, N. R., & Rathna, S. (2018). Real-Time Path Optimization for Autonomous Farming Using ANFTAPP and IoV-Driven Hex Grid Mapping. International Journal of Advances in Agricultural Science and Technology, 5(3), 86-94.

[48] Wahl, B., Cossy-Gantner, A., Germann, S., & Schwalbe, N. R. (2018). Artificial intelligence (AI) and global health: how can AI contribute to health in resource-poor settings?. BMJ global health, 3(4), e000798.

[49] Grandhi, S. H., & Padmavathy, R (2018). Federated learning-based real-time seizure detection using IoT-enabled edge AI for privacy-preserving healthcare monitoring. International Journal of Research in Engineering Technology, 3(1).

[50] Jagadeeswari, V., Subramaniyaswamy, V., Logesh, R. T. A., & Vijayakumar, V. (2018). A study on medical Internet of Things and Big Data in personalized healthcare system. *Health information science and systems*, *6*(1), 14.