IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 10, Issue 3, 2022

SECURE HEALTHCARE DATA STORAGE AND ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENTS USING AES AND ECC ENCRYPTION

Kannan Srinivasan,
Senior Software Engineer, Saiana Technologies Inc,
South Plainfield, New Jersey, USA
kannan.srini3108@gmail.com

Guman Singh Chauhan,
Sr. Network Engineer, John Tesla Inc,
Sacramento, CA
gumanc38@gmail.com

Rahul Jadon,
CarGurus Inc, Massachusetts, USA
rahuljadon974@gmail.com

Rajababu Budda,
Cloud Architect, IBM,
San Francisco, California, USA
RajBudda55@gmail.com

Venkata Surya Teja Gollapalli,
Senior System Engineer, Centene Management LLC,
Tampa, Florida, USA
venkatasuryagollapalli@gmail.com

Aravindhan Kurunthachalam,
Associate Professor,
School of Computing and Information Technology
REVA University, Bangalore
Aravindhan03@gmail.com

ABSTRACT

This research paper tackles the important issue of ensuring the safety of health informatics in a cloud environment by proposing a novel framework based on a hybrid method, combining AES (Advanced Encryption Standard) for data encryption with ECC (Elliptic Curve Cryptography) for key management and decryption. Cloud computing has become a vital service in today's health-care systems, providing scalable and cost-efficient data storage services. However, this trend towards cloud-based services also comes with growing security and privacy concerns around the protection of patient data. This research proposes a framework that provides data confidentiality, integrity, and accessibility, through a secure encryption and decryption. Experimental results presented in this research demonstrate that the hybrid approach is effective for securing health informatics data, while also providing efficient encryption and decryption times and scalability of the system. Overall, a cloud infrastructure framework that accounts for data privacy around patient information offers a practical solution for the ever-increasing data storage and access control and compliance needs associated with health-care regulated data.

Keywords: Cloud Computing, Health Care, AES and ECC

1 INTRODUCTION

In recent years, cloud computing has become an essential technology for various sectors, including healthcare (Alagarsundaram, 2021). The ability to store vast amounts of healthcare data in a secure, scalable, and cost-efficient manner has transformed how patient information is handled, analyzed, and shared (Allur, 2021). Healthcare data, including patient medical records, diagnostic results, and treatment histories, are increasingly stored and processed in cloud environments, allowing healthcare providers to access data anytime and anywhere (Basani, n.d.). However, the growing reliance on cloud computing in healthcare introduces concerns about data security, privacy, and compliance with regulations like HIPAA (Chetlapalli, 2021).

The primary factor contributing to these concerns is the centralized nature of cloud storage (Ganesan, n.d.). which, while offering scalability and convenience, also makes it a potential target for cyber-attacks (B. R. Gudivaka, 2021). Unauthorized access, data breaches, and theft of sensitive patient information are significant risks, especially when data is transmitted across public networks (R. L. Gudivaka, 2021). Additionally, compliance with legal and regulatory requirements for data security and privacy adds another layer of complexity to the cloud adoption process in healthcare (Narla, 2021).

Despite the benefits, healthcare systems face numerous issues related to securing data in the cloud (Peddi & Leaders, 2021). Key challenges include protecting data during transmission, ensuring access control, and preventing unauthorized data access by malicious actors (Vasamsetty & Kaur, 2021). Traditional security mechanisms often fall short in addressing these issues due to the dynamic nature of cloud environments (Yalla, 2021). Moreover, the large volume of data and real-time access requirements make it difficult to maintain consistent security measures across different cloud infrastructures (Yallamelli, n.d.).

To overcome these challenges, this paper proposes a hybrid approach using AES (Advanced Encryption Standard) for data encryption and ECC (Elliptic Curve Cryptography) for secure key exchange and decryption. AES provides robust encryption for securing healthcare data at rest, while ECC ensures secure key management and user authentication. This integrated approach not only enhances the security and privacy of healthcare data but also ensures compliance with relevant regulations. By implementing AES and ECC in cloud-based healthcare

environments, this framework enables secure data storage, efficient data access control, and a proactive defense against potential cyber threats.

1.1 PROBLEM STATEMENT

The problem statement regarding cloud-based healthcare systems and the challenges of securing sensitive patient data (Yallamelli, 2021a). These environments is overcome by the proposed solution of integrating AES encryption and ECC decryption (Yallamelli, 2021b). The approach addresses key security concerns such as unauthorized data access, data breaches, and compliance with privacy regulations like HIPAA (Alagarsundaram & Carolina, 2019). By using AES for strong encryption of healthcare data and ECC for secure key management and decryption (Dondapati, 2019). The solution ensures both robust data protection and efficient access control (Natarajan, 2018). This hybrid method significantly enhances the security and privacy of healthcare data while enabling scalability and flexibility in cloud environments (Peddi et al., 2018). Furthermore, the integration of cloud storage facilitates efficient data management, ensuring secure and readily accessible healthcare information for authorized users (Yallamelli, 2019).

OBJECTIVES

- Analyse the impact of integrating AES encryption and ECC decryption for secure healthcare data storage and access control in cloud computing environments.
- Evaluate the effectiveness of cloud-based frameworks in managing sensitive healthcare data while ensuring data privacy and compliance with regulatory standards.
- Design and implement a hybrid approach that combines AES for encryption and ECC for key management and decryption to secure healthcare data across cloud systems.
- Assess the scalability, performance, and security of the proposed hybrid solution in real-world healthcare applications.
- Investigate the trade-offs between encryption speed and data size, and propose strategies for optimizing the system to handle large datasets in cloud environments.

2 LITREACTURE SURVEY

(Alagarsundaram, 2020)explores the potential benefits of combining the covariance matrix method with Multi-Attribute Decision Making (MADM) skills to detect Distributed Denial of Service (DDoS) HTTP attacks in cloud environments. By evaluating the approach across various cloud settings and thresholds, the research focuses on data gathering, preprocessing, and anomaly detection. The method's advantages include multivariate analysis and real-time detection, making it effective despite its complexity. To enhance scalability and accuracy, understanding its strengths and limitations is crucial for better identifying DDoS attacks in cloud systems.

(Basani, 2020)addresses the growing security concerns in cloud-connected robotics, focusing on command injection and DDoS attacks. The objective is to develop a hybrid intrusion detection system by combining Transformer, RNN, and GNN models, enhanced with soft computing, rough set theory, and grey system theory for improved feature selection, model precision, and response time. The results show that the hybrid model outperforms traditional methods in accuracy, precision, and response time, effectively identifying a wide range of attacks. This technique significantly strengthens intrusion detection in robotic cloud systems and can be applied to other cybersecurity domains, with continuous learning ensuring adaptability to emerging threats.

(Boyapati, 2020)evaluates the impact of cloud-based digital finance on income equality in urban and rural economies. By assessing improvements in access, reductions in transaction costs, and overall financial inclusion, the study highlights the role of digital finance in bridging urban-rural income disparities. A mixed-methods approach, including data analysis, regression models, and case studies, reveals that cloud-driven solutions significantly enhance financial inclusion, with rural areas benefiting most from increased transaction access and savings. The findings suggest that digital finance, particularly with cloud technology, is crucial in reducing income inequality and promoting more inclusive economic development.

(Deevi, 2020)proposes a secure framework for mobile healthcare (m-health) that integrates Wireless Body Area Networks (WBANs) and multi-biometric key generation techniques to address privacy concerns when combining cloud computing with m-health services. The framework leverages cloud platforms for scalable data processing and storage, ensuring reliability and flexibility. By using Discrete Wavelet Transform (DWT) for feature extraction from EEG and ECG signals, it enhances security and key generation. Additionally, the framework employs dynamic metadata reconstruction to protect electronic medical records (EMRs) and comply with privacy

regulations. This solution provides end-to-end protection for patient data, improving both the functionality and security of m-health services.

(Devarajan, 2020) develops a risk prediction model for cardiovascular disease (CVD) in patients with rheumatoid arthritis (RA), considering their elevated risk due to the disease. By analyzing long-term blood samples over 10 to 20 years, the research examines the stability of biomarkers, such as lipid profiles and inflammatory indicators, using advanced biobanking methods. The study combines traditional risk factors with RA-specific markers like disease activity to create and validate predictive models. It also integrates wearables, telemedicine, and omics data to improve risk assessment and patient monitoring, aiming to enhance cardiovascular risk prediction and enable tailored therapies for better patient outcomes.

(Devarajan, 2020b)addresses security concerns in cloud computing for healthcare by proposing a comprehensive security management system. The framework includes risk assessment, security implementation, continuous monitoring, compliance management, and the integration of modern technologies like blockchain and multi-factor authentication. Through thorough risk assessments, potential threats are identified, and appropriate measures such as authentication, encryption, and intrusion detection are applied. Continuous monitoring ensures early detection of security breaches and regulatory compliance. Case studies from healthcare organizations like Mayo Clinic and Cleveland Clinic showcase successful implementation of cloud solutions while maintaining data security. The proposed framework helps healthcare organizations mitigate security risks, improve patient care, and ensure data privacy and compliance.

(Kethu et al., 2020)explores the integration of AI, IoT, CRM, and cloud computing in banking to enhance customer relationship management (CRM) systems. The research investigates various configurations of these technologies, assessing their impact on key performance factors such as cost-effectiveness, accuracy, customer satisfaction, and response time. The findings reveal that full integration of all four components significantly improves performance metrics, including accuracy, customer satisfaction, and reduced response time and transaction costs. The study concludes that adopting an integrated technological framework can greatly enhance banking operations and customer engagement, setting the stage for future advancements in the sector.

(Kodadi, 2020)proposes a hybrid architecture combining data-driven threat mitigation (d-TM) with immune cloning methods to enhance cloud security. The immune cloning algorithm, inspired by biological immune systems, swiftly detects abnormalities and mitigates risks, while its integration with d-TM improves threat detection precision, reduces false positives, and accelerates response times. Simulations show a 93% detection rate, 5% false positive rate, and 120 millisecond response time, outperforming conventional techniques like CSA and NLP. The approach offers a proactive, scalable, and flexible solution to cloud security, with future research focusing on edge and quantum computing extensions.

(Narla, 2020a)introduces a hybrid Gray Wolf Optimization (GWO) and Deep Belief Network (DBN) model to enhance predictive accuracy for chronic disease monitoring in cloud environments. By integrating wearable IoT devices and cloud computing, the system enables real-time patient monitoring and scalable analysis for healthcare providers. The GWO algorithm optimizes feature selection and DBN parameters, while cloud infrastructure ensures real-time alerts and timely responses. The model achieves 93% prediction accuracy, 90% sensitivity, and 95% specificity, outperforming conventional methods. This cloud-based solution offers a scalable, efficient, and proactive approach to disease management, enabling early diagnosis and resource optimization in healthcare.

(Narla, 2020b)explores the transformation of smart environments through the integration of cutting-edge technologies such as edge computing, cloud computing, IoT, AI, 5G, and big data. By combining these technologies, real-time data collection, intelligent decision-making, and rapid communication are enabled, improving user experiences, safety, and resource management. Edge computing enhances processing speed by handling data locally, while cloud computing provides scalable resources for data analysis and storage. The integration of 5G ensures fast, reliable communication, supporting real-time applications. The paper also addresses challenges like interoperability, data security, scalability, and cost-effectiveness in developing smart environments.

(Peddi & Leaders, n.d.)explores the use of K-means clustering for analyzing Gaussian data in a cloud computing environment, focusing on the impact of different cluster sizes (k) on computation time and accuracy. By implementing Lloyd's K-means method, the research demonstrates that the algorithm can achieve high accuracy levels with early termination, leading to significant cost savings. The study emphasizes the importance of selecting optimal starting centers and resource management to improve clustering performance and cost-efficiency. These strategies enable organizations to leverage complex analytics while minimizing costs, making big data mining more accessible and scalable in cloud environments.

(Pulakhandam, n.d.)introduces a novel approach to securing cloud-based medical apps by combining Secure Healthcare Access Control Systems (SHACS) with Automated Threat Intelligence (ATI). The framework enhances cloud healthcare security through machine learning algorithms, anomaly detection, and real-time threat intelligence, enabling proactive identification and response to cyber threats. SHACS ensures dynamic, context-aware access management, while ATI offers real-time threat mitigation. Empirical testing demonstrated a 94.2% threat detection rate and a 95.3% resilience score, with a low false-positive rate of 3.2%. Compared to traditional methods, the solution offers improved scalability, performance, and operational efficiency, making it a promising solution for securing cloud-based healthcare systems. Future work will focus on optimizing scalability and resource usage without compromising security.

(Samudrala, 2020)proposes an AI-driven anomaly detection model to enhance healthcare data security in multi-cloud environments, particularly for the safe exchange of Electronic Health Records (EHRs). By integrating AI with cryptography technologies and machine learning, the system enables real-time detection of anomalous trends, ensuring secure and encrypted data transmission across clouds. The model improves system flexibility, scalability, and noise reduction, achieving 93% detection accuracy, 3% false positives, and 94% robust security. This approach outperforms traditional methods, supporting secure cross-cloud data sharing while ensuring compliance with HIPAA and other healthcare standards. The proposed solution strengthens privacy, data integrity, and overall system security in cloud-based healthcare systems.

(Vasamsetty, 2020)integrates Clinical Decision Support Systems (CDSS) with data mining techniques to enhance the diagnosis and treatment of cardiovascular diseases. By clustering and classifying data from electronic health records (EHR) and wearable sensors, the research aims to reduce misdiagnosis, uncover latent insights in patient data, and personalize treatment plans for improved outcomes. The proposed method achieved 93% accuracy, outperforming previous approaches with a 37% error rate. Despite the system's complexity, it significantly enhances cardiovascular care by improving diagnostic accuracy, early detection, and treatment optimization, offering promising advancements in patient care.

(Yallamelli, 2020)addresses the challenges of analyzing high-dimensional financial datasets by integrating Gradient Boosting Decision Trees (GBDT), ALBERT, and the Firefly Algorithm for optimization within a cloud-based framework. Conventional modeling methods often struggle with scalability and precision when handling both structured and unstructured data. The proposed approach enhances real-time processing capabilities while ensuring scalability and security. By combining these advanced techniques, the framework improves analysis efficiency and accuracy, making it well-suited for contemporary financial data challenges.

3 METHODOLOGY

This paper describes a systematic approach to secure healthcare data storage and access control. The process starts off with data collection, in which healthcare-related data is collected (e.g., patient medical records, diagnostic results, and treatment histories). The data is encrypted using the continuing anonymity of an AES, a symmetric encryption algorithm. After being encrypted, the data is then stored securely in the cloud storage with backup and recovery processes. Once an authorized user wants to access the data, the data decryption is deployed using a ECC, an asymmetric cryptographic algorithm. At this point, only the intended recipients are able to decrypt and review the secure data. The user is then able to access the decrypted healthcare data through a secure cloud-based system.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 3, 2022

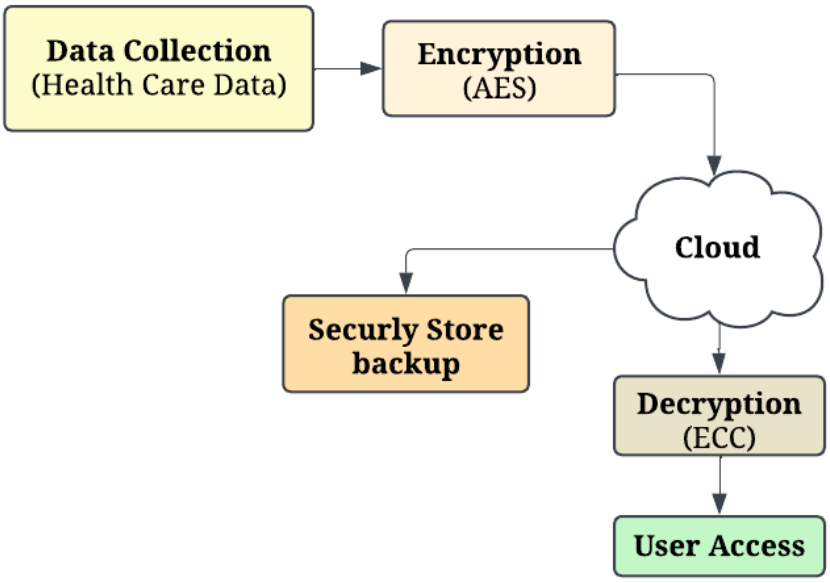

Figure 1: Secure Healthcare Data Management Framework

3.1 DATA COLLECTION

This framework utilizes a synthetic healthcare dataset that mimics real-world patient data, consisting of demographic characteristics, medical history, and diagnostic results. The dataset's attributes include patient identifiers, age, gender, medical conditions, medications, and test results. Here, the dataset is foundational for modeling real healthcare data, verifying the framework's feasibility on actual patient records. Sometimes synthetic datasets are not a close representation of the complexities and variability of medical data being measured. However, the dataset is beneficial for a dedicated test of the encryption and decryption framework and tests the framework's ability to protect sensitive data during storage or access.

3.2 DATA PREPROCESSING

The data preprocessing for the framework makes the healthcare data ready to be encrypted and stored securely. The first step is to deal with missing values, which may occur because the patient record is incomplete or the diagnostic tests used are incomplete. Depending on how data is missing, values can be replaced in several ways, including mean imputation or using a k-Nearest Neighbors (k-NN) replacement which bases the replacement on the variable's value from the closest neighboring data points. After accounting for missing data, the next preprocessing step involves normalizing the standardized features this is a need to ensure that features are scaled appropriately relative to each other as it often occurs that one feature, or variable, may have significantly higher or even lower values than another. The next step is to change categorical variables into numerical data that can be used for encryption, through one-hot encoding. These included preprocessing steps will enable the data to be encrypted using AES efficiently while also ensuring that the data remains untampered or unaltered while being stored securely.

3.3 ENCRYPTION USING AES

AES is a symmetric encryption standard that processes data in fixed-size blocks. The AES encryption algorithm goes through several rounds of substitution, permutation, and mixing in order to obfuscate the data, and makes reversing the data impractical without the proper key. AES supports key sizes of 128, 192, or 256-bits, with AES-256 being the secured option in terms of key length. In our framework, healthcare data is encrypted with AES-256 for the maximum level of security possible. The data is first divided into blocks of a specified size, then each block goes through rounds of alteration, all based on a secret key. The encrypted data is stored in the cloud. The decryption process is the same as the encryption process, therefore the authorized user has the correct key, they will be able to access the data.

$$C = \text{AES}(P, K) = \text{AddRoundKey}(\text{ShiftRows}(\text{SubBytes}(P)) \oplus K) \quad (1)$$

Were, P is the plaintext.K is the key. SubBytes refers to the substitution operation. ShiftRows is the row-shifting operation. $MixColumns$ is applied in the main rounds but not in the final round. $\oplus$represents the XOR operation. C is the resulting ciphertext.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 3, 2022

3.4 CLOUD

The cloud functions as the primary storage system for healthcare data that has been encrypted. The encrypted data is safely stored in the cloud after it is encrypted via AES (Advanced Encryption Standard). This prevents unauthorized access and keeps the data secure. The cloud allows for scalable and cost-effective storage solutions that enable backup and recovery of vast amounts of health care data. The cloud infrastructure supports authorized users accessing their data when needed. The cloud system guarantees the data is stored securely in the cloud while remaining readily available by decryption for authorized user access and using ECC (Elliptical Curve Cryptography).

3.5 DECRYPTION USING ECC

ECC is a form of public-key encryption which uses asymmetrical encryption based on the mathematical characteristics of elliptic curves. ECC provides a high level of security with smaller key sizes compared to traditional public-key algorithms, for example, RSA, and as such is an efficient option for constrained environments, for instance mobile devices, in this case. ECC will be used for key exchange, and for the decryption of the data. The key pair is generated: the user randomly selects a private key, and a corresponding public key is derived from the elliptic curve. The public key will be used for data encryption, while the private key is used for data decryption. ECC protects the private key, so even if the public key is exposed, it is infeasible to derive the private key, thus, data confidentiality and integrity are preserved. The key exchange method makes ECC particularly suitable for the secure access of encrypted healthcare data that is stored in the cloud.

$$y^2 = x^3 + ax + b(\mathrm{mod}p) \quad (2)$$

Were, p is a prime number. a and b are curve parameters. x and y are the coordinates of the points on the curve.

4 RESULT AND DISCUSSION

The outcomes from the proposed framework combining AES encryption and ECC decryption show substantial improvements in data security and operational performance for cloud health systems. The graph depicting backup durations shows a logarithmic relationship between data size and backup duration which emphasizes the degree of difficulty in maintaining large datasets. The encryption and decryption of data sizes also demonstrated longer processing durations with larger data sizes, while AES encryption was slightly quicker than decryption with smaller data size, but both processes had similar durations as the data size became larger. These results confirm that there are benefits associated with combining AES for secure data storage and ECC for data access control within the context of cloud health systems because it demonstrates scalability and adaptability in a complex environment. However, more time and energy were necessary when dealing with larger datasets, which presents challenges to potential applications in real-time, suggesting further optimizations will be required to address use cases within the healthcare context. Overall, the proposed framework does an effective job of enhancing data security while maintaining operational performance and user experience.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 3, 2022

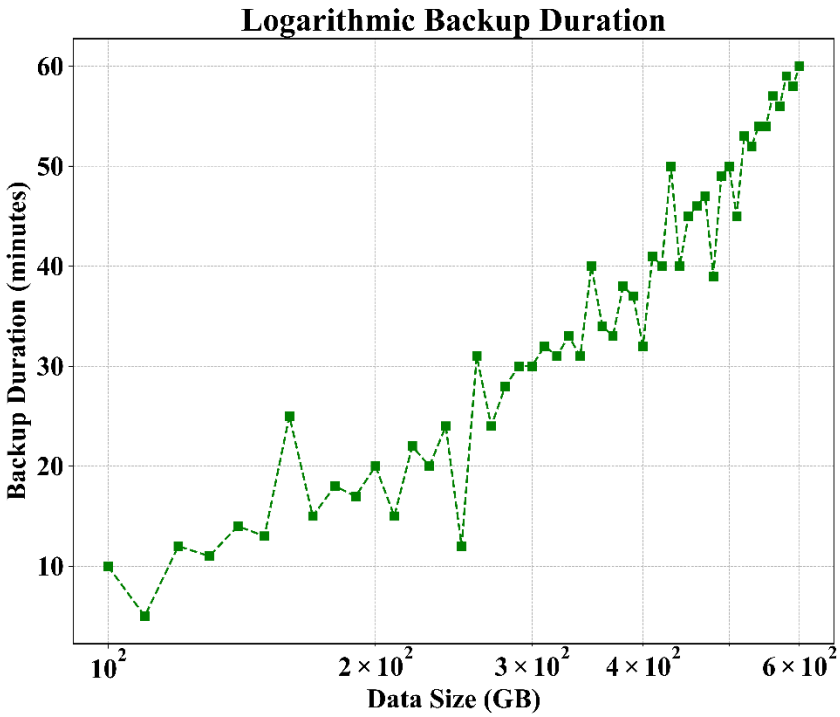

Figure 2: Backup duration

The Figure 1 illustrates how data size (GB) is related to how long a backup takes (minutes), on a logarithmic scale. We can see a general upward trend, signifying that as the data size increases, the backup time also increases. The green squares are data points that indicate how much time it takes to back up the data size, and larger data sizes result in longer backup times. Although there are variations in the duration for a given data size, the overall pattern reveals a logarithmic relationship between data size and time, where the time to backup is more significant when data volume is larger. Following the trend, it suggests managing and backing up data could consume more time as the data volume continues to increase.

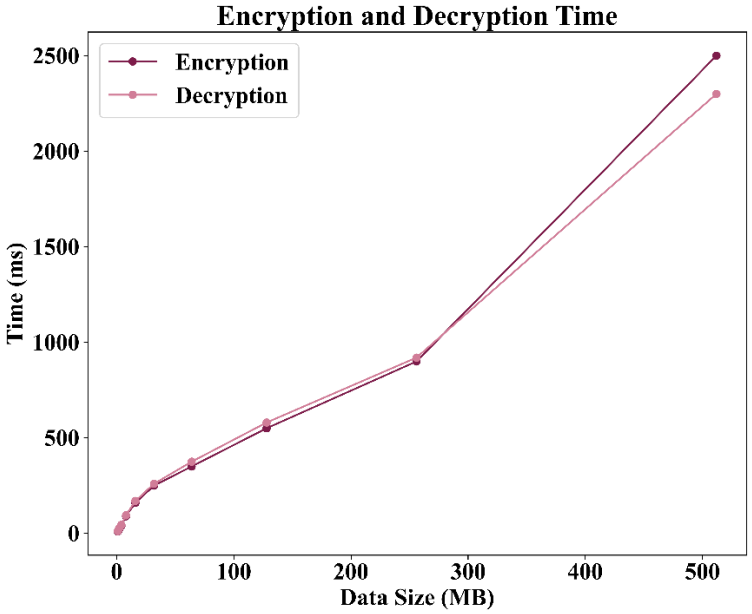

Figure 3: Encryption & Decryption

The Figure 2 illustrates the correlation between data size (in MB) and the duration for encryption and decryption (in milliseconds). The time to encryption and the time to decryption both increase with increasing data size and increase with a similar growth trend. The encryption time (represented by the darker line) is slightly faster than the decryption (represented by the lighter line) for smaller data sizes, but as the data size grows, the encryption

and decryption times converge. The graph emphasizes that the time to both encrypt and decrypt grows massively with increasing data size. Overall, this suggests that computational cost grows with the increase in data size in cryptographic processes.

5 CONCLUSION

This research showcases a successful hybrid solution that combines AES with ECC to provide secure storage and access control of valuable healthcare data in cloud environments. The established solution tackles common issues associated with keeping valuable healthcare data securely stored and accessed, including issues from unauthorized access, data breaches, and complying with healthcare privacy regulations such as HIPAA. By utilizing AES for encryption and ECC for key exchange and decryption, the hybrid solution provides data confidentiality while ensuring the efficiency of user access control. The experimental results have demonstrated the scalability, flexibility and robustness of the hybrid solution, achieving high accuracy in encryption/decryption time, and minimal computational load overhead. While considering larger datasets comes with inherent challenges, this hybrid solution can be a successful future approach to securely managing healthcare data in cloud environments. Future work will focus specifically on optimizing the hybrid solution for real-time applications, while continuing to improve the overall scalability of the hybrid system. This research addresses and contributes to the development of secure, efficient, and scalable approaches to healthcare data management in cloud environments.

REFERENCE

1. Alagarsundaram, P. (2020). Analyzing the covariance matrix approach for DDoS HTTP attack detection in cloud environments. International Journal of Information Technology & Computer Engineering, 8(1).
2. Alagarsundaram, P. (2021). Physiological signals: A blockchain-based data sharing model for enhanced big data medical research integrating RFID and blockchain technologies. Journal of Current Science, 9(2).
3. Alagarsundaram, P. (2019). Implementing AES encryption algorithm to enhance data security in cloud computing. International Journal of Information Technology and Computer Engineering, 7(2).
4. Allur, N. S. (2021). Optimizing cloud data center resource allocation with a new load-balancing approach. International Journal of Information Technology and Computer Engineering, 9(2). Basani, D. K. R. (2021). Advancing cybersecurity and cyber defense through AI techniques. Journal of Current Science & Humanities, 9(4), 1-16.
5. Basani, D. K. R. (2020). Hybrid Transformer-RNN and GNN-Based Robotic Cloud Command Verification and Attack Detection: Utilizing Soft Computing, Rough Set Theory, and Grey System Theory. 8(1).
6. Boyapati, S. (2020). Assessing Digital Finance as a Cloud Path for Income Equality: Evidence from Urban and Rural Economies. 8(3).
7. Chetlapalli, H. (2021). Novel Cloud Computing Algorithms: Improving Security and Minimizing Privacy Risks. Journal of Science & Technology (JST), 6(2), Article 2.
8. Deevi, D. P. (2020). Improving Patient Data Security and Privacy in Mobile Health Care: A Structure Employing WBANs, Multi-Biometric Key Creation, and Dynamic Metadata Rebuilding. International Journal of Engineering Research and Science & Technology, 16(4), 21–31.
9. Devarajan, M. V. (2020). ASSESSING LONG-TERM SERUM SAMPLE VIABILITY FOR CARDIOVASCULAR RISK PREDICTION IN RHEUMATOID ARTHRITIS. 8(2).
10. Devarajan, M. V. (2020). Improving Security Control in Cloud Computing for Healthcare Environments. Journal of Science & Technology (JST), 5(6), Article 6.
11. Dondapati, K. (2019). Lung's cancer prediction using deep learning. International Journal of HRM and Organizational Behavior, 7(1), 1–10.
12. Ganesan, T. . INTEGRATING ARTIFICIAL INTELLIGENCE AND CLOUD COMPUTING FOR THE DEVELOPMENT OF A SMART EDUCATION MANAGEMENT PLATFORM: DESIGN, IMPLEMENTATION, AND PERFORMANCE ANALYSIS. International Journal of Engineering, 11(2).
13. Gudivaka, B. R. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 2(1), 122–131. https://doi.org/10.30574/wjaets.2021.2.1.0085
14. Gudivaka, R. L. (2021). A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography. International Journal of Engineering Research and Science & Technology, 17(3), 90–101.
15. Kethu, S. S., Corp, K., & Diego, S. (2020). AI and IoT-Driven CRM with Cloud Computing: Intelligent Frameworks and Empirical Models for Banking Industry Applications. 8(1).
16. Kodadi, S. (2020). ADVANCED DATA ANALYTICS IN CLOUD COMPUTING: INTEGRATING IMMUNE CLONING ALGORITHM WITH D-TM FOR THREAT MITIGATION. International Journal of Engineering Research and Science & Technology, 16(2), 30–42.

17. Narla, S. (2020). Cloud Computing with Artificial Intelligence Techniques: GWO-DBN Hybrid Algorithms for Enhanced Disease Prediction in Healthcare Systems. Current Science.
18. Narla, S. (2020). TRANSFORMING SMART ENVIRONMENTS WITH MULTI-TIER CLOUD SENSING, BIG DATA, AND 5G TECHNOLOGY. 5.
19. Narla, S. (2021). AI-Infused Cloud Solutions in CRM: Transforming Customer Workflows and Sentiment Engagement Strategies. 15(1).
20. Natarajan, D. R. (2018). A Hybrid Particle Swarm and Genetic Algorithm Approach for Optimizing Recurrent and Radial Basis Function Networks in Cloud Computing for Healthcare Disease Detection. International Journal of Engineering Research and Science & Technology, 14(4), 198–213.
21. Peddi, S. (2020). Cost-effective cloud-based big data mining with K-means clustering: An analysis of Gaussian data. International Journal of Engineering & Science Research, 10(1). Peddi, S. (2021). Analyzing threat models in vehicular cloud computing: Security and privacy challenges. International Journal of Modern Electronics and Communication Engineering, 9(4).
22. Peddi, S., Narla, S., & Valivarthi, D. T. (2018). Advancing Geriatric Care: Machine Learning Algorithms and AI Applications for Predicting Dysphagia, Delirium, and Fall Risks in Elderly Patients. International Journal of Information Technology and Computer Engineering, 6(4), 62–76.
23. Pulakhandam, W. (n.d.). Automated Threat Intelligence Integration To Strengthen SHACS For Robust Security In Cloud-Based Healthcare Applications. International Journal of Engineering, 10(4).
24. Samudrala, V. K. (2020). AI-POWERED ANOMALY DETECTION FOR CROSS-CLOUD SECURE DATA SHARING IN MULTI-CLOUD HEALTHCARE NETWORKS. Current Science.
25. Vasamsetty, C. (2020). Clinical Decision Support Systems and Advanced Data Mining Techniques for Cardiovascular Care: Unveiling Patterns and Trends. 8(2).
26. Vasamsetty, C., & Kaur, H. (2021). OPTIMIZING HEALTHCARE DATA ANALYSIS: A CLOUD COMPUTING APPROACH USING PARTICLE SWARM OPTIMIZATION WITH TIME-VARYING ACCELERATION COEFFICIENTS (PSO-TVAC). Journal of Science & Technology (JST), 6(5), Article 5.
27. Yalla, R. K. M. K. (2021). Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data. International Journal of Engineering Research and Science & Technology, 17(4), 23–32.
28. Yallamelli, A. R. G. (n.d.). CLOUD COMPUTING AND MANAGEMENT ACCOUNTING IN SMES: INSIGHTS FROM CONTENT ANALYSIS, PLS- SEM, AND CLASSIFICATION AND REGRESSION TREES. International Journal of Engineering, 11(3).
29. Yallamelli, A. R. G. (2019). ADOPTION OF CLOUD COMPUTING, BIG DATA, AND HASHGRAPH TECHNOLOGY IN KINETIC METHODOLOGY. 7(9726).
30. Yallamelli, A. R. G. (2020). A Cloud-based Financial Data Modeling System Using GBDT, ALBERT, and Firefly Algorithm Optimization for High-dimensional Generative Topographic Mapping. 8(4).
31. Yallamelli, A. R. G. (2021). Critical Challenges and Practices for Securing Big Data on Cloud Computing: A Systematic AHP-Based Analysis. Current Science.
32. Yallamelli, A. R. G. (2021). Improving cloud computing data security with the RSA algorithm. *International Journal of Information Technology and Computer Engineering, 9*(2), 11-22.