Security and Privacy of E-Health Solutions in Cloud

[1]Puchala Manju Reddy, [2]Chitirala Sravanthi

[1]PG Scholar, [2]Assistant Professor

[1]Information Technology,

[1]G. Narayanamma Institute of Technology and Science, Hyderabad, India

[1]manjureddypuchala@gmail.com, [2]sravanthi.cvr@gnits.ac.in

Abstract: Since more and more electronic health systems use cloud computing, it is very important to ensure that group data sharing is safe and works well. Identity-based encryption (IBE), Ciphertext-Policy Attribute-Based Encryption (CP-ABE)- and proxy re-speaking are examples of traditional public key cryptographic systems that provide good access and privacy control. In order to do this problem, a light encryption model is designed to use symmetrical key cryptography. This makes mathematics much easier. However, symmetrical encryption is weak because it uses the same key for both encryption and decrypting. If the key is published, it can be interrupted. This work improves symmetrical encryption by adding a key distribution method based on an ex-or key that divides the key into two parts: one is safely held in the cloud and the other is shared among group members. This architecture ensures that no one has the entire decryption key. This makes data more private and reduces the chance of exposing keys. The design makes it easier to regulate the approach, has minimal latency and can grow, so it is good for cloud applications in real time, especially in areas where privacy such as e-Healthcare is important.

"Index Terms *-Symmetric Encryption, EX-OR Operation, Cloud Security, Key Splitting, E-Health, Access Control, Group Data Sharing, Confidentiality".*

1. INTRODUCTION

Cloud Computing has become a technology changing the game in digital ecosystem of health care. It allows scalable storage, real -time data access and cooperation services in a wide range of health organizations. Since more people use cloud platforms for electronic health, safe and private solutions are needed even more important. It is very important that any infrastructure of electronic health protects the privacy and accuracy of patient medical information, diagnosis, regulations and diagnostic findings [1]. Identity-Based Encryption (IBE), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), and proxy re-load are examples of traditional cryptographic schemes that offer strong access control. However, they can be very demanding on resources, especially in the settings of multiple users, where key generation processes, pairing and re-evacuation can slow things down and make them more complicated [2]. [3].

People are interested in symmetrical key cryptography because it is fast and works well in real -time situations. However, its dependence on a single key for encryption and decryption is very weak; If the key is stolen, all data are revealed [4]. Healthcare applications need not only fast encryption, but also better ways to manage keys that reduce the danger of one -point failure and make it easier to share data sharing in groups [5] [6].

The aim of this project is to provide a lightweight and efficient encryption frame that uses symmetrical key encryption with distribution of keys based on ex-or keys to share data in cloud e-resort systems safely and fast. The aim is to make calculations as simple as possible and maintain private data and only allow certain people to view them [7].

2. RELATED WORK

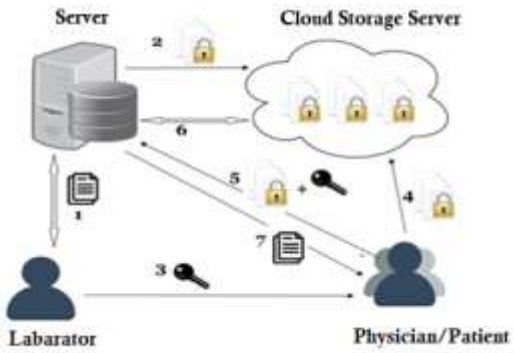
Many studies have come to keep sensitive medical data safe in health care cloud systems. There are many proposals to improve privacy, integrity and management of electronic health systems. Manicandan et al. [8] they performed a thorough review of literature, which focused on the greatest problems with security and privacy in cloud electronic systems. They emphasized the need for light but strong cryptographic methods that allow application in real time. Karthikeyan et al. [9] they came up with a hybrid cloud architecture that is aware of privacy and well protects patient data while increasing more flexible and scalable health care operations. Their method uses many levels of protection to prevent someone from entering without permission and theft of data.

Dhinakaran et al. [10] The SpectraSafe encryption scheme, which works with the dynamic anonymity of K-Anonymity, has been able to set up health care in the cloud. This method reduces the risk of detecting someone's identification while taking quick answers to questions. Kumar et al. [11] He was concerned with how cloud and IoT technologies could cooperate on providing intelligent health services. They said that intelligent city infrastructure must have safe ways to share data to help health care. Raghav et al. [12] He came up with an intelligent health -based health frame that improves patient monitoring and health with safe data sharing methods.

Satpathy et al. [13] they wrote about safety models for Cloud Healthcare that use ML. They also talked about how important it is to have algorithms that protect privacy in analysis of patients. Kothai et al. [14] they proposed a concept used by blockchain, encryption and cloud to improve health monitoring systems more scalable and credible. Their study shows that multi -layer design can be much more durable. ALAHMARI et al. [15] He created a decentralized framework to maintain electronic health information by blockchain. This system provides privacy and transparency without dependence on centralized authority. All these studies provide a clear direction for research in creating cloud solutions for health care that are safe, scalable and focus on privacy. This shows that the need for light encryption approaches with improved key control.

3. METHODOLOGY

This article suggests a safe way to share data based on the cloud-based e-residential systems by combining symmetrical encryption AES-128 with a key distribution method based on ex-or keys. The symmetrical key is divided into two parts: one is given by authorized users and the other is held in the cloud. This ensures that the entire key is never displayed, which improves access security and control. This strategy reduces the amount of computing performance and reduces the chances of a key compromise in critical healthcare settings. [9] [10] [14].



"Fig. 1. System Architecture"

The diagram (Fig. 1) shows how to safely share data. The local server sends encrypted data from the laboratory to the cloud server. Doctors and patients can use the key to get and decode their own private and secure information that is stored in the cloud.

i) Symmetric Encryption Using AES-128:

The AES-128 is a strong and rapid symmetrical encryption technique used to protect electronic health data from its storage in the cloud. The AES-128 provides great privacy with less processing, so it is ideal for health care applications that need to be quickly performed. 128 -bit key length is strong enough for cryptography and does not slow down processing. This method enables rapid encryption and decryption of data, allowing health workers to access patients and diagnostic findings in real time without threatening security. This is in line with the needs of the current cloud -based healthcare systems [10].

ii) EX-OR-Based Key Splitting:

An EX-OR-based approach or is used to divide the AES-128 key to ensure symmetrical encryption. The key is divided into two parts that can work on their own. One part is kept on a cloud server, while the other is shared with users who have permission. This two -storey method ensures that no one can get to the entire key, which will reduce it to be exposed. Ex-or access is a lightweight and low latent way of splitting keys without adding further cryptographic work. This makes it easier to maintain private health care when they are stored in several places [14].

iii) Secure Data Access Control:

To save access control, the user's data must be checked and a partial key on the user's side must be present. When authorized users ask for data, their partial key is connected to the segment stored cloud, which is related to the original AES key. This system ensures that only authorized users can decrypt and access electronic health data. This prevents unauthorized users from entering and maintaining personal data protection for patients within cloud infrastructure in accordance with healthcare data security rules [9].

iv)Cloud Integration and Performance Optimization:

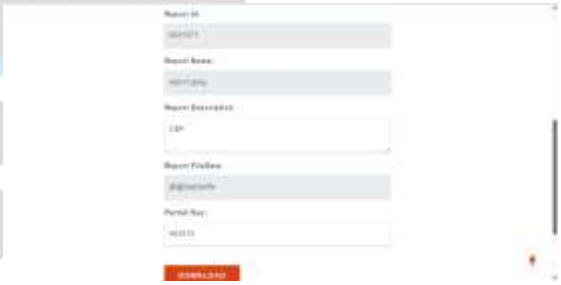
The system is closely linked to the cloud infrastructure, allowing the processing of electronic health data with high scalability and performance. Encryption and decryption methods are improved to reduce processing delay, ensuring that encrypted medical data can be quickly and reliably accessed. The design provides real-time data transactions in healthcare situations with multiple users and maintains high safety, efficiency of resources and low computational loads by AES-128 integration and good key management with cloud storage [12].

4. RESULTS AND DISCUSSIONS

Using the AES-128 encryption with an ex-or key distribution, the system performs a good job to protect healthcare based on cloud. Test cases show that the key reconstruction works, access control is safe and the system cannot be decrypted by anyone who should not be able to. Power testing shows that the encryption time has fallen and the scalability has increased. This method maintains very private data with very small extra work, so it is ideal for setting up electronic health that has to work in real time.

"Fig. 2. Report History"

Fig. 2 it displays the interface of the message history where users can see medical records that have been submitted and viewed in the past.



"Fig. 3. By using partial key can download reports"

Fig. 3 it illustrates how to safely download a message using a partial key that ensures that only some people can get to encrypted content.

"Fig. 4. By symmetric key we can upload reports"

Fig. 4 It shows how to submit an encrypted message using the AES-128 and ex-or logic to make the data more private.

"Fig. 5. By getting key we can view reports"

Fig. 5 Displays the following key reconstruction message and make sure that decryption and access permissions were made correctly.

5. CONCLUSION

The symmetric encryption of the AES-128 and the key splitting mechanism with use of the EX-OR operation have been done to ensure that cloud-based e-health environments are secure and convenient to share information. This is very efficient in reducing computational overhead, and it ensures that the entire encryption key has never been beheld by a mere individual, which enhances key secrecy. Its group based access control is another strength as only authorized party is allowed to rebuild the key and gain access to sensitive information. The encryption time was found to be less, one could exchange the files securely, and the system was not at risk of key compromise. The real-time healthcare applications can be accommodated by the system because it is quick, efficient, and scalable to the business requirements. Its capability can interface easily with present cloud systems due to its modular and web-based structure. This means that it is a privacy-respecting solution that can be of great use to industries handling sensitive data, such as the healthcare and banking.

Multi-factor authentication would be the enhancement to include in cloud-based healthcare systems to strengthen user-level access management even further in the future. You can make the current symmetric key and EX-OR based splitting technique even better by including the biometric based key generation to make verification of identities still better. Besides, blockchain technology could introduce audit trails that are immutable and non-centralized trust in data exchange. Making the system optimized to distributed cloud system could also increase the availability and fault tolerance of the data which is crucial in large scale use of the health industry. It may also be a good idea to add anomaly detection powered by AI which can help identify attempts to gain access to data without authorization in real-time. The model can be modified to support dynamic revocation and rekeying by the user. The future research may also focus on machine learning the privacy-preserving technique that can be analyzed encrypted health data to ensure that patient confidentiality does not get breached.

REFERENCES

[1]. Chen. Y and W. Tzeng, "Efficient and provably-secure group key management scheme using key derivation," in Proc. IEEE 11th Int. Conf. TrustCom, 2012, pp. 295–302.

[2]. Hua Deng, Zheng Qin, Qianhong Wu, Zhenyu Guan, Hui Yin, "Revocable Attribute-based Data Storage in Mobile Clouds", IEEE Transactions on Services Computing,02 April 2020.

[3]. Leyou Zhang, Yilei Cui, Yi Mu, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing", IEEE Systems Journal, Volume: 14, Issue: 1, 06 May 2019.

[4]. Liming Fang, Ge Chunpeng, Zhe Liu, Jinyue Xia, "Revocable Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds", IEEE Transactions on Dependable and Secure Computing, Volume: 18, Issue: 3, 14 February 2019.

[5]Nicolas Sarvamathu Silambarasan Elkana Ebinazer, S. Mary SairaBhanu, "ESKEA: Enhanced Symmetric Key Encryption Algorithm Based Secure Data Storage in Cloud Networks with Data Deduplication", Springer Transactions on Wireless Personal Communications, volume: 117, pages: 3309–3325, 19 November 2020.

[6] Manikandan, A., Sanjay, T., Menon, G., Aswin, R., Bhaskar, P. B., Govind, R. M., &Ramprasad, O. G. (2025). Issues and challenges in security and privacy with e-Healthcare: A thorough literature analysis. *Internet of Things enabled machine learning for biomedical applications*, 222-247.

[7] Karthikeyan, M.P., Bareja, L., Gupta, M., Malviya, A., Dev, S., & Iqbal, M. A. (2025). Revolutionizing healthcare: data privacy based on novel approach in hybrid cloud networks. *International Journal of System Assurance Engineering and Management*, 1-9.

[8] Dhinakaran, D., Kumar, N. J., &Ponnuviji, N. P. (2025). Safeguarding confidentiality and privacy in cloud-enabled healthcare systems with spectrasafe encryption and dynamic k-anonymity algorithm. *Expert Systems with Applications*, *279*, 127584.

[9] Kumar, A., Bag, A., Anand, A., Saha, S., Mohapatra, H., &Kolhar, M. (2025). Examining healthcare services utilizing cloud technology in intelligent urban environments. In *Revolutionizing healthcare systems through cloud computing and iot* (pp. 77-98). IGI Global.

[10] Raghav, Y. Y., Choudhary, S., Pandey, P., Singh, S., &Varshney, D. (2025). Smart Healthcare: Cloud-IoT Solutions for Enhanced Patient Well-Being. *African Journal of Biomedical Research*, *28*(1), 14-28.

[11] Satpathy, S., Mohapatra, S., Swain, P. K., &Paikaray, B. K. (2025). Securing healthcare in the cloud: a machine learning erspective. International Journal of Internet Manufacturing and Services, 11(2), 114-131.

[12] Kothai, G., Harish, P., Ajinesh, D., &Sathyanarayanan, V. (2025). Optimizing data privacy and scalability in health monitoring: Leveraging, encryption, blockchain, and cloud technologies. In *Critical Phishing Defense Strategies and Digital Asset Protection* (pp. 245-270). IGI Global Scientific Publishing.

[13] Alahmari, S., Alshardan, A., Al-Wesabi, F. N., Sorour, S., Alghushairy, O., Alsini, R.,& Al Duhayyim, M. (2025). A decentralized and privacy-preserving framework for electronic health records using blockchain. *Alexandria Engineering Journal*, *126*, 196-203.

[14] NS Lockhart, E. (2025). Privacy and data security in digital health: Implications for family therapy. *Contemporary Family Therapy*, 1-3.

[15] Georgiou, D., Katsaounis, S., Tsanakas, P., Maglogiannis, I., &Gallos, P. (2025). Towards a secure cloud repository architecture for the continuous monitoring of patients with mental disorders. *Frontiers in Digital Health*, *7*, 1567702.