International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 03 | Mar 2024 www.irjet.net p-ISSN: 2395-0072

Implementing Data Security on EHR Using Hybrid Cryptography

Mr. Dipak Bisht[1], Mr. Deepak Sharma[2], Mr. Meet Todankar[3], Ms. Sneha Sankhe[4]

[1,2,3] Student, Department of Information Technology, Theem College of Engineering, Boisar, Maharashtra, India
[4]Professor, Department of Information Technology, Theem College of Engineering, Boisar, Maharashtra, India

---

Abstract - *The development of electronic health records (EHR's) for patient monitoring is a concept widely adopted in the field of healthcare industry. Through this considerable web app patients can communicate with respective doctors and consult them for their disease diagnosis. This helps them to keep a track of their medical records in a digital and electronic form. However, the data uploaded on the EHR is huge in terms of volume, as multiple patients might try to access them. In such a scenario the data so collected might undergo certain attacks and breaches due to the vulnerability of the system model which might even lead to power failure of data stored on the respective EHR. Therefore, in this report, we propose the implementation of two encryption algorithms that would help to secure the data being transferred on the EHR. For this purpose, a Hybrid Cryptographic Technique (HCT) is used that includes the execution of AES, RSA and Serpent Algorithm. Using the mentioned HCT, the informational exchange is expected to be secured on cloud. The Advanced Encryption Standard (AES) is lauded for its efficiency in protecting data through its symmetric encryption approach. RSA, an asymmetric encryption scheme, enhances security by leveraging complex mathematical relationships This innovative amalgamation safeguards medical records from unauthorized access, cyberattacks, and potential power-related incidents, reinforcing the confidentiality and integrity of sensitive healthcare data. The marriage of encryption methodologies thus presents a significant stride toward ensuring the safety and privacy of patient information in the evolving landscape of healthcare technology*

Key Words: **AES, cryptography, RSA, encryption, EHR**

1.INTRODUCTION

The aim of the proposed research study is to develop a web app that would run on a server and keep track of patient health records. The health records and respective patient information is expected to be shared between the patient and his respective doctor. An added feature in the proposed web app is that the file of the patient can also be shared between multiple doctors if the patient wishes to do so. To accomplish the aim of this study; the author of the research has put forward the concepts of encryption techniques and cryptography so that secured transfer of information exchange can occur between the patient and the doctor. Since the webserver is deployed on cloud using MS Azure, patient data is at risk to exposure and data loss.

For this purpose, a hybrid cryptographic technique (HCT) that combines the fundamentals of RSA and AES encryption are used. The deployment of the web server occurs on cloud using MS Azure and can thereby be accessed by the doctor as well as the patient.

2. LITERATURE REVIEW

A Hybrid Secure and Scalable Electronic Health Record Sharing (HSS-EHRS) system, whereby two cryptographic methods are utilized for providing a flexible, secure and fine-grained access to EHR files in hybrid cloud. The proposed framework divides the system into two security domains and utilizes an ABE encryption scheme to encrypt the EHR files. The proposed system proved its efficiency based on encryption time and concurrent recipient data access and sharing. The enhanced MA-ABE encryption scheme is capable of handling on demand recipient data access and providing high levels of security.[1]

It has focus to developed an attribute based, field level, document encryption for managing the access and data security of cloud-based EHRs. In their approach they designed and developed a complex knowledge graph that details the roles and attributes of different stakeholders of the medical organization along with the various relationships between them. They also developed an open-source, easy to use user interface.[2]

The existing strategy in cloud security to assess the three primary parameters such as judgment, verification and secrecy. To make strides each aspect various strategies is got to join that are distinctive from conventional security framework on information exchange or record capacity framework. The summarized the existing strategy advance up to information and gives future scope of the strategy. The cloud capacity security framework requires the compelling strategy to overcome the issues such as information spillage, unreliable transmission and get to qualifications.[3]

It provides the health-related data is encrypted using Blowfish and keys are managed by the improved RSA technique when stored in cloud storage. Benefits of this

hybrid approach were quick encryption, a huge prime number pool for key production, and effective key management. The simulation results unequivocally demonstrate that the suggested hybrid technique's encryption and decryption times are faster than those of the other approaches taken into consideration.[4]

This study proposes a data security protection system based on infrastructure security of human, network, and cloud, as well as the related security technology and strategy, to address the issue of cloud computing security. This paper addresses the easily overlooked security issues with cloud service provider internal staff by proposing identity authentication and role-based access control strategies based on account and certificate, analyzing and researching cloud security standards and legal maintenance, and presenting a cloud security assessment system along with pertinent legal recommendations and measures to offer a robust defense.[5]

3. SYSTEM ARCHITECHURE

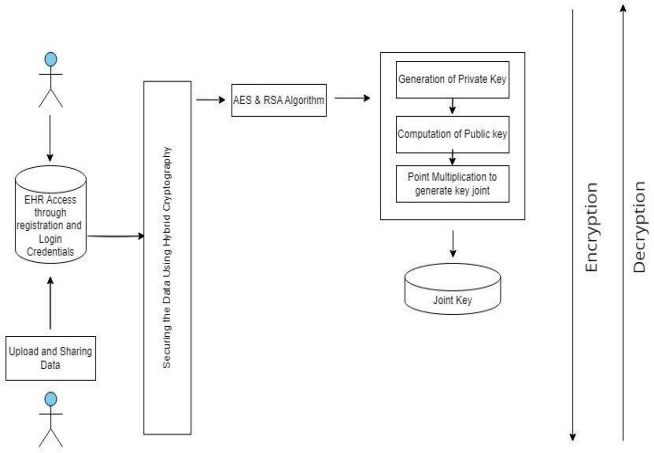

Fig 1. System Architecture of EHR system

Proposed research study is to develop a web app that would run on a server and keep track of patient health records. The health records and respective patient information is expected to be shared between the patient and his respective doctor. An added feature in the proposed web app is that the file of the patient can also be shared between multiple doctors if the patient wishes to do so. To accomplish the aim of this study; the author of the research has put forward the concepts of encryption techniques and cryptography so that secured transfer of information exchange can occur between the patient and the doctor. Since the webserver is deployed on cloud using MS Azure, patient data is at risk to exposure and data loss. For this purpose, a hybrid cryptographic technique (HCT) that combines the fundamentals of RSA and AES encryption are used. The deployment of the web server occurs on cloud using MS Azure and can thereby be accessed by the doctor as well as the patient.

4. RESULT AND ANALYSIS

Discover everything there is to know about electronic health records and the specific security threats they provide. Learn about the fundamentals of hybrid cryptography, such as the ways in which RSA and AES can work in tandem. When designing your system's architecture, take into account the safe storage, access, and transmission of EHR data. Determine the precise situations and use cases in which hybrid cryptography will be used. Select suitable encryption and decryption techniques for AES and RSA. Recognize both algorithms' key management procedures. Integrate the selected algorithms, making sure they are efficient and compatible with your EHR system. Provide techniques for combining RSA's asymmetric key encryption with AES's symmetric key encryption. To manage key generation, distribution, storage, and rotation securely, put in place a strong key management system. Carry out extensive testing to make sure the safety precautions work. Analyse your implementation's performance and make the required adjustments. Provide thorough justifications for the selected algorithms, important management procedures, and system architecture in your implementation documentation. Make sure that all of your work is unique and that any use of pre-existing methodology is appropriately cited.

```
.exe' 'c:\Users\Lenovo\.vscode\extensions\ms-pytho
py\launcher' '52631' '--' 'D:\Cyber Security M\EHR
AES algorithm is working correctly.
Accuracy: 100.00%
Encryption time: 0.003053 seconds
Decryption time: 0.000000 seconds
Transmission rate: 123.08%
PS D:\Cyber Security M\EHR Cloud\Acc>

.exe' 'c:\Users\Lenovo\.vscode\extensions\ms-pytho
py\launcher' '52647' '--' 'D:\Cyber Security M\EHR
RSA algorithm is working correctly.
Accuracy: 100.00%
Encryption time: 0.000000 seconds
Decryption time: 0.009667 seconds
Transmission rate: 1969.23%
PS D:\Cyber Security M\EHR Cloud\Acc>
```

Fig 2. System Architecture of EHR system

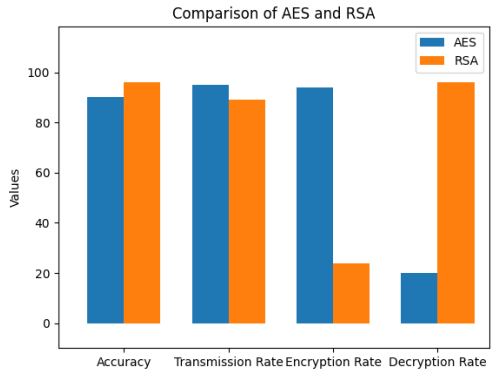

Fig 3. Testing of Encryption & Decryption using HCT

The above result shows the accuracy of encryption and decryption using hybrid cryptography technology based on two algorithms.

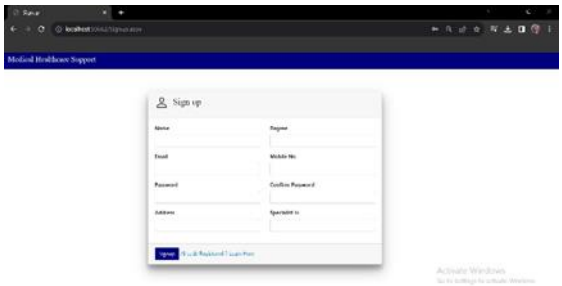

Fig 4. Signup Page for Doctors

Above fig 4. Shows the Signup page for the certified Doctors to get registered to manage the patient details.

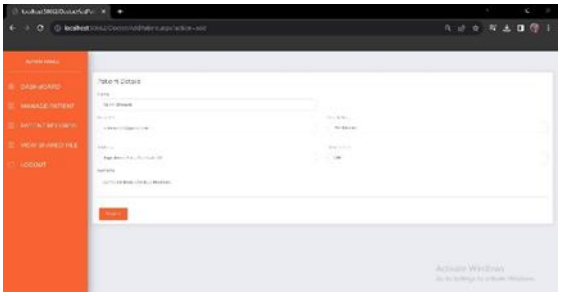

Fig 5. Doctor Dashboard panel to manage patient detail

From here Doctors can manage their Patient heath report and can give medication remark according to the patient health condition.

5. CONCLUSIONS

The main steps we used in the project is to focused on establishing the foundational components for data security and user access control in the EHR system. The hybrid cryptography approach, along with the signup and login pages for doctors, will form the basis for a robust and secure EHR system. As the project progresses, further features and security enhancements will be implemented to ensure comprehensive data protection and a seamless user experience and Doctor can see the patient detail and go through the patient report and suggest medicine to the patient according to their report. Regular monitoring and updates are essential for maintaining the effectiveness of the security measures over time.

ACKNOWLEDGEMENT

We would like to take this opportunity to express our gratitude towards all the people who have in various ways, helped in the successful completion of our project. We must convey our gratitude to our project guide Prof. Sneha Sankhe for giving us the constant source of inspiration and help in preparing the project, personally correcting our work and providing encouragement throughout the project. We also thank all my faculty members for steering me through the tough as well as easy phases of the project in a result-oriented manner with concern attention.

REFERENCES

[1]. R. Manoj, A. Alsadoon, P. W. C. Prasad, N. Costadopoulos and S. Ali, "Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud," 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (Mobile Cloud), San Francisco, CA, USA, 2017, pp. 185-190, doi: 10.1109/MobileCloud.2017.38.

[2]. M. Joshi, K. P. Joshi and T. Finin, "Delegated Authorization Framework for EHR Services Using Attribute-Based Encryption," in IEEE Transactions on Services Computing, vol. 14, no. 6, pp. 1612-1623, 1 Nov.-Dec. 2021

[3]. Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2021, pp. i-cxviii

[4]. P. Chinnasamy and P. Deepa Lakshmi, "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 1717-1720, doi: 10.1109/ICICCT.2018.8473107.

[5]. W. Xiaoyu and G. Zhengming, "Research and Development of Data Security Multidimensional Protection System in Cloud Computing Environment," 2020 International Conference on Advance in Ambient Computing and Intelligence (ICAACI), Ottawa, ON, Canada, 2020, pp. 67-70, doi: 10.1109/ICAACI50733.2020.00019.

[6]. C. K. a. D. R. V. P. M. Aryan, "Enhanced Diffie Hellman algorithm for reliable key exchange," IOP Conference Series: Materials Science and Engineering, vol. 263(017) 042015, pp. 1-8, 2017

[7]. Kanna, G.P., Vasudevan, V.: A fully homomorphic–elliptic curve cryptography-based encryption algorithm for ensuring the privacy preservation of the cloud data. Clust. Comput. 22, 9561–9569 (2019)

[8]. Bhatt Agarwal, R.: A technological review on scheduling algorithm to improve performance of cloud computing environment. Int. J. Innov. Technol. Explor. Eng. (IJITEE) 8(6), 166–172 (2019)

[9]. Moudgil K, Maheshwari R, Parekh HB, Devadkar K. Cloud-based secure smartcard healthcare monitoring and tracking system. In: 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT). Coimbatore: IEEE;(2017).10.1109/ICECCT.2017.8117869