Securing Personal Health Records using Advanced Multi-Factor Authentication in Cloud Computing

Meena.S, V.Gayathri

Abstract: ***Cloud computing is a novel prototype to provide services via the internet. Most of the fields like banking, industries, educational institutions, and healthcare are storing their applications, data and accessing it through cloud because of its versatility and affordable price. Even though cloud has a many special feature, data security and privacy are the most important issues in a cloud background. Especially in healthcare sector, according to recent report numerous amount of healthcare data breached by unknown websites and hackers, and much healthcare information breaches are occurring around the world for different purposes and still it is vulnerable on account of storing and accessing data through third party cloud servers. Due to many attacks on personal health records data security and privacy in cloud environment, it is a primary task to concentrate on solving this issue because such health information are really sensitive, and playing vital role in decision-making of patients health which wrong decision may spoil patient's health, life along with health institution's reputation. To ensure security and privacy, data encryption and authentication are the key technologies which are a technique to secure data and create proof identities to obtain access of data in the system. Conventional password authentication does not provide sufficient security for information to the new means of attacks. So, this paper introduces a framework for data encryption using standard RSA and Hash function and advanced multi factor authentication technique to cloud data access which authenticates the user based on different factors such as contextual, signcryption and iris bio-metric features. This prototype to cloud computing is implemented using open source technology. The proposed advanced system minimizes intermediate data access due to the complexity of key access and strong authentication. The performance of the system has been evaluated using experimental results such as encryption and decryption time, authentication accuracy, execution time.***

Keywords: ***Cloud Computing, Cloud Security, Privacy, Encryption, Decryption, Multifactor Authentication,***

I. INTRODUCTION

In the developing technology, healthcare system [1] and humanities services are playing a significant role in a medical field because it requires the health information to manage the person's health status sequence. The medical field acquiring much health information [2] which are continuously accessible by the patient, relatives, health sectors, and physician, lab technician and so on. Due to various requests and acceptances of the health record [3] it has to be stored in the third-party server called cloud. The cloud provides the access permission to people, and they can access the records from everywhere in the world. The humanities and health system include several million of patient records, personal information and disease details which has acquired by the hospital.

The personal records [4] consist of disease information, patient health condition, severity status, symptoms, stages of disease, billing details, radio graphic information, clinical information, sugar level, diagnosis procedure, medical treatment details, blood information and genetic problems are ought to saved in the cloud. These particulars can be accessed by anyone when they are having rights to access it. In addition to this personal health record information [5] much information such as disease particulars, imaging reports, disease diagnosis results, laboratory details, family ancestry details, drug information, reaction of drug, surgery information, dosing level, prescription and other written documentations shall be stored in the cloud because, it can be used in the further physical analysis process. The cloud environment [6] needs to be dynamic and support the security of personal health records, scalability, reliability, privacy and agility because health data is more sensitive and important. As per the health insurance portability and accountability rule, health care data security [7] is one of the most significant elements. The accountability rule includes the various risk assessment process and conducts different risk assessment program to cover the healthcare data security. This developed program controls the data vulnerabilities [8] and trying to give the data integrity, confidentiality, availability and safeguard the personal health records. Even though the health insurance portability and accountability rule making sure about various securities [9] related awareness and still data security and privacy are the major challenges in cloud environment. Found on the healthcare association survey [10], 65% of the United States organization faces phishing attack in 2019 while sharing their health records in cloud. Globally 55% of organization and health sectors are suffering by the phishing and cyber security problem in 2020. In addition to the third-party survey called Proofpoint dew point reported that 35000 people record have got attacked by intermediate attackers. The survey has conducted by different people among various countries like France, Australia, Japan, Germany, and Spain in which 600 IT Professionals are lost their personal health report. In addition to this, 9 million people have reported that personal records that has accessed through the suspicious mail via the 50 million simulated phishing emails in the year of 2019. As per the US based cyber security firm FireEye reported on 2019 that 68 lakhs personal health records have been stolen from Oct 2018 to Mar 2019 which contains patient information, personally identifiable information (PII), doctor information, PII and credentials. As a result of the critical issues of the data security [11], cloud environment retains the personal record by offering security as a service.

Revised Manuscript Received on March 28, 2020.

Meena.S, Research Scholar, Department of Computer Science, Periyar University, Salem, Tamil Nadu.

Dr.V.Gayathri, Assistant Professor, Department of Pee Gee College of Arts and Science, Dharmapuri, Tamil Nadu.

Even if the cloud offers security as a service, the information may be damaged by the insider subordination, accidental disclosure, insider curiosity, outside intrusion, uncontrolled secondary usage, integrity factors and data stealing and it seriously affects the data security and privacy [12]. For reducing the security issues, various encryption techniques [13] such as cipher text policy-based approach, expressive key-based approach, Hybrid Attribute-based Encryption with Proxy Re-encryption scheme, Identity based Encryption (IBE), Re-Encryption techniques, attribute-based encryption (ABE), expressive key-based approach, Proxy Re-encryption approach, hierarchical attribute-based encryption, hierarchical identity based encryption (HIE), key-based approach and fuzzy identity based encryption (FIE) and some others have been proposed up to now. Although the above methods [14] provide adequate protection to data, sometimes it takes too much time of managing data confidentiality, integrity, authentication and privacy as a result of intermediate attacks. Moreover, it is difficult to ensure safety of data and privacy at all times. More at times third parties have the ability to guess the secret keys even if it is public or private keys which reduces the authentication [15] between users and suppliers. To eliminate the above mentioned security problems many of a constrictive and optimization techniques have been proposed to manage the security, confidentiality, authentication [16] and privacy of the personal health records still it gives a challenge on complete security and time difficulty. The hybridized methods also extends key management issues which maximizes the overall complexity while transferring sensitive health data in cloud environment. To solve the aforementioned security problems, this framework uses data encryption using standard RSA algorithm and hash functions along with advanced multi factor authentication. Initially, Patients' data is first got by the hospital and then stored in the cloud after encryption using both the RSA algorithm and the hash function then the introduced multi-factor authentication follows three key steps such as contextual, signcryption and iris bio-metric. When it comes to accessing information, user's first need to perform contextual authentication, followed by signcryption verification, and then ensure that they are the authenticated person through iris bio-metric authentication. These multi-factor authentication processes create the complexity of accessing a shared key in a cloud environment. Finally, the performance of the system has been evaluated using test results and discussions based on the open source framework.In the remainder part of this manuscript, part 2 analyzes the views of secure sharing in cloud of other authors. Part 3 discusses an advanced multi-factor authentication based healthcare data storage, access and its methodology. Part 4 describes the merits of the proposed framework.

II. RELATED WORKS

This section discusses a comprehensive research study on the process of protecting medical health data in the cloud environment. (Abouelmehdi, K., et al., 2018) [17] Analyzing the security and privacy of health data in big data. Big Data is one of the best platforms offering the ability to store, share and deliver valuable data free. Given the importance of healthcare data, security privacy should be managed by minimizing trust issues. To deal with the security issues discussed above, the author analyzes various encryption techniques, including the process of anonymous identification. In addition, the strengths and limitations of the respective methods are clearly discussed.(China Appala Naidu R et al., 2019) [18] Introduces an attribute-based encryption process to maintain health data protection and privacy. During the data transfer process, personal health records must be stored in encrypted form to maintain data security. Therefore, in this work, the SHA 512 algorithm is used to encrypt the data before storing it in the cloud database. People can access patient information by performing the encryption process. In this process, access policies are used to perform a secret key delivery process that maintains data security. According to personal information, the implemented system automatically generates the medicine for a patient. Finally the performance of the system is evaluated using the IBM Blue Mix Load Balancer, in which the system responds effectively to patient health records. (Guojun Wang et al., 2011) [19] Maintains authentication, data confidentiality, and trust between the user and the provider through the use of a hierarchical attribute encryption process. This method uses the cyber text policy encryption process to encrypt health data and be stored in the cloud. After performing the encryption process, access controls are provided using the lazy re-encryption and proxy re-encryption process that controls unauthorized access. This effective re-encryption process recognizes access control and successfully terminates access rights. Finally the performance of the system is evaluated using test analysis. (Prajakta Solapurkar et al., 2012.) [20] Examines various data encryption techniques such as proxy re-encryption techniques, proxy re-encryption techniques, identity encryption, hybrid attribute encryption along with proxy re-encryption and attribute encryption techniques for ensuring the data sharing process. These security techniques have been used to resolve security, confidentiality, privacy, on-demand accessibility, flexibility and trust issues. By resolving these systems, shared personal health records can provide information data authentication and authorization, which effectively eliminates transient access. Finally, the effectiveness of the system has been evaluated using test results. Huda Elmogazy et al.,2013 [21] Introduces a fully homomorphic encryption algorithm to maintain data security, authentication, availability and authorization, while storing personal health records in a cloud environment. The introduced algorithm uses the key partitioning procedure, which determines the key to shared data according to the key representative. These generated key values enable access to patient data in a cloud environment. It is difficult to find shared key values with an intermediate user attempt to access data and that completely reduces unauthorized functions on the personal health record. Based on the above study, it is clear that personal health records require protection and privacy to eliminate the transitional attack. From the point of view of the above research concept, in this work, effective and optimal authentication techniques are used to create security for the data. A detailed description of the introduced method is discussed in the following section.

III. ADVANCED MULTI FACTOR AUTHENTICATION-BASED PHR THAT PROTECTS DATA SECURITY AND PRIVACY.

This section analyzes the advanced multi factor authentication process to protect the privacy and security of personal health records [22]. It is difficult to store the patient's personal records on a third-party server without providing any proper protection. The medical information generated is stored in a cloud accessible by a health consultant, doctors, users, family members, medical researchers and others. During this process, if the intermediate user or unauthorized user accesses information that creates difficulties when making medical decisions. This work proposes an advanced multi-factor authentication mechanism to solve the above issues [23] to ensure data security, privacy, and confidentiality. Based on the above discussion, a general examination of the safe personal health record storage and access process is depicted in Figure 1

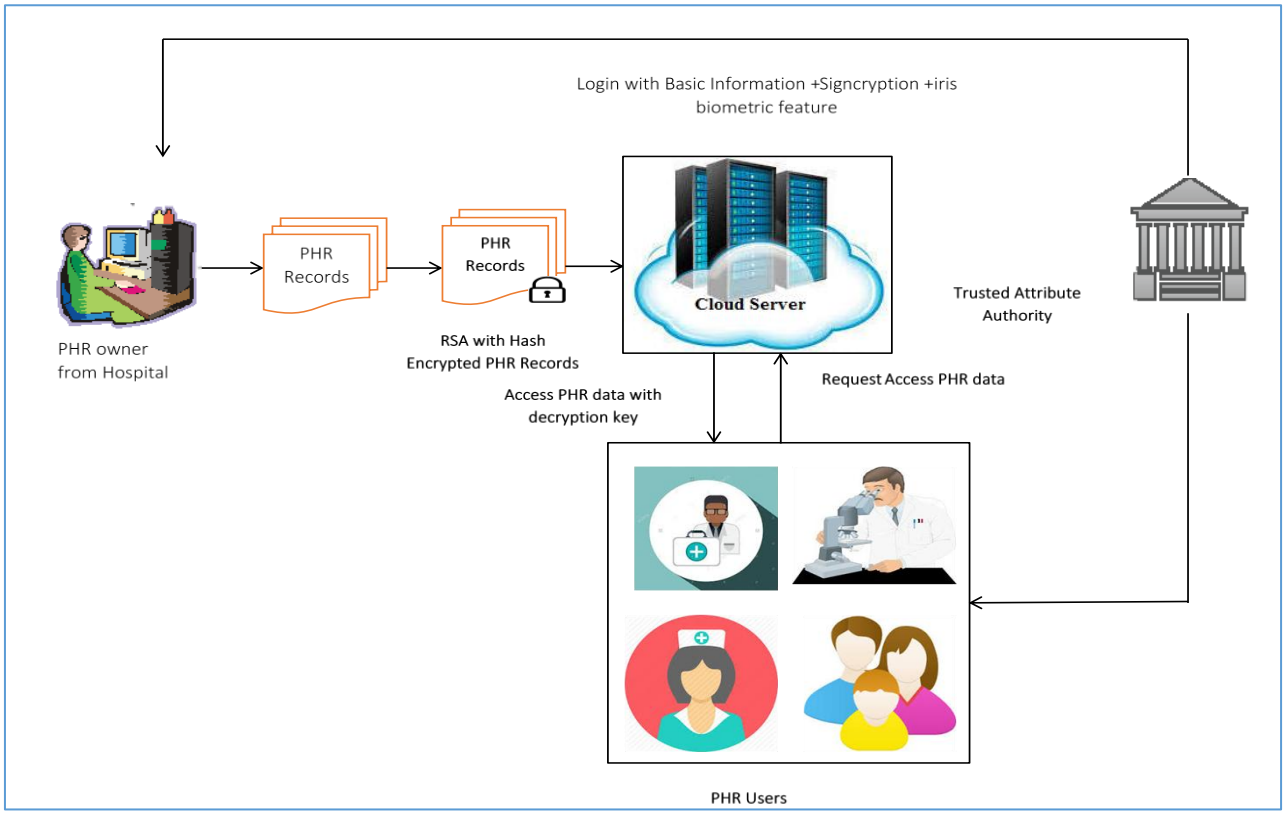


Figure 1: Advanced Multifactor authentication based secure personal health record maintenance process

Figure 1 illustrates the advanced multi-factor authentication process for managing data security and privacy while storing personal health records in a cloud environment. The security process has been achieved in the hospital and user environment. During this process, the layer of authentication process worked to ensure data security. According to above fig 1, the PHR owner from the hospital side stores the data in a cloud environment by performing a proper encryption process, which is done by using standard RSA with the hash encryption process.

Personal Health Record Encryption process.

The first step in this process is the encryption of the personal health record collected by the hospital. PHR information includes physical history, genetic problem, identity sheet, progress notes, problem list, imaging report, recommendations, immunization records, laboratory reports, physician orders, consultation history, authorization form, discharge history, operation report and pathology reports and all. This collected information is usually secured on a third-party server to make emergency decisions. During this process, the stored data is encrypted using the Rivest Shamir Adleman (RSA) and hash encryption algorithm [24]. This algorithm provides better security for data. This algorithm uses the public key for encryption and uses the private key for decryption. The public key is selected from two large prime numbers published with an auxiliary value. Then, to avoid unnecessary data access, the private key (decryption process) must be stored and secured. The key sharing process performs the cryptography procedure in an asymmetric method, which increases the computational speed. Because of this fast computation and high speed, in this work, personal health records are encrypted with the help of the RSA algorithm. This algorithm ensures security by performing different steps [25], such as key generation, key distribution, encryption, and decryption. During the key generation step, large positive integer's p and q are chosen randomly.

The selected prime numbers have different lengths, but the value of the similar size must be kept secret. With the help of the prime number, n must be computed to generate the public and private key.

$$n = p * q \quad (1)$$

The computed n value is represented in terms of the key length bits.

After that, the value of λ (n) is computed as follows.

$$\lambda(n) = lcm\ (\lambda(p), \lambda(q)) \quad (2)$$

The computed λ (n) is kept secret. From the computed λ (n) value, the integer value of e must be chosen as 1 <e <λ (n). Then determine the value of d as follows.

$$d = e^{-1}(mod\ \lambda(n)) \quad (3)$$

In eqn (3), d is represented as the modular multiplicative inverse of e.

After computing the value of n, d, $\lambda(n)$ the key is to be distributed, since the key distribution process only serves to perform the encryption and decryption process. Therefore, the public key (n, e) is sent to the public and the private key (d) key is kept confidential (never distributed). The encryption process is done using the public and private key. Transmitted health information is considered M, which is encrypted using the public key e and generates cipher text for information m. The encryption process is performed as follows,

$$c = m^e(mod\ n) \quad (4)$$

Although the chosen prime numbers are large, the modular process is easy to calculate and transmit cipher text to the cloud for data storage. Data storage is effectively accessed by completing the correct verification and authentication process. Once the authentication is complete, the data is accessed by performing the decryption process. Decryption is performed using eqn (5).

$$c^d = (m^e)^d = m(mod\ n) \quad (5)$$

From the decryption process, the message, M can be obtained from making the padding program more efficient. The aforementioned verification process using the advanced multi-factor authentication procedure discussed in the following.

User authentication To Access Personal Health Record

The next step is user authentication because this step eliminates intermediate access, unnecessary data conversion and security issues. To overcome the above problems, advanced multi factor authentication is used. If the user wishes to access medical health data, they must be authorized first and then only the user can access the data. During the data access process, the user register their personal and credentials information on the authorized server. Registered information is used to verify the user when the user tries to access the data. Initially, the process of context recognition [26] is used to authenticate the user. When the user accesses health information, the contextual authentication process collects different information such as date, time, geolocation and IP address details. The information collected is used to verify users by comparing provided information with an already registered information. If the user constantly changes their location, users will be verified by sending one-time password to the user. This process helps reduce fraudulent activity. After verifying the general information, the signcryption process [27] is used to enhance the further security and authentication process. This system is capable of providing data for both encryption and digital signature protection. Dual encryption process maximizes data security effectively and limits unnecessary access. The signcryption process consists of three steps, namely key generation, signcryption and unsigncryption. This signcryption process is perfectly providing security, privacy, efficiency, integrity, and confidentiality. As a result of these reasons in this task signcryption concept is used for authenticating the user before accessing data in a cloud environment.

Key Generation

The first step of the task is to create both public key and private key. X and Y are random numbers. The random number combination is selected as the private key.

Signcryption steps

The second step is the signcryption process, wherein each user has an ID that is identified using the ID. After that, the random integer r is chosen $r \in R(1, n-1)$. R is represented as the selected random number and the prime sequence number. Then secrete key for user must be generated$T \leftarrow [k]SK1$. This is done after the set of key values is generated from the key derivative process $(K1|K2) \leftarrow Key\ derivation(T, 1)$ (6)

From the first key derived, the cipher text is generated, which is specified in eqn (7).

$$c \leftarrow EK1(m) \quad (7)$$

Then the signature is generated with the help of other key and message authentication code referred to $signature \leftarrow MACk2(c)$. Finally signcrypted text is sent to the user, including public key (p), cipher text (c) and generated signature. As previously discussed, once the user tries to access the health records, they must authenticate for this purpose and the unsigncryption process must be performed. The unsigncryption process [28] uses receiver ID and cipher text messaging. So, initially, the message string is generated with the key derivative function. The string text is generated using eqn (8)

$$Text\ (T) \leftarrow [x]P \quad (8)$$

Decrypt the message using the first key$m \leftarrow Dk1(c)$, and the signature generated using the message authentication code and the second key, which is done as follows

$$signature\ 1 \leftarrow MAC\ k2(m) \quad (9)$$

The computed signature 1 is compared to the signature value and allowing the user to access the data if both signatures are equal. The user is checked again using biometric features to give an additional security to the system. For this procedure, iris biometric features are used because of the fine texture sensitive cornea and highly transparent also difficult to access by a third-party user. The iris biometric features [29] have several key points that can be used to match the user when accessing PHR data. Initially the collected iris images are converted to grayscale images. The noise in the images is eliminated by computing the median value. If, the pixel is distorted by any noise replaced using the median value. Different biometric minutia features are extracted to create a template for performing the correct matching process. During the minutiae extraction process the images are divided into 5 * 5 matrices, and each image is analyzed to calculate the average value of the pixels. In addition, the image boundary value is estimated to predict dark and light pixel values. These defined values are identified according to the fuzzy membership value, which helps to identify the ridges of the biometric image. The skeleton of the images was successfully identified. The extracted minutia details are stored in the database as a template when the user enters the computer, and the matching process is performed. The matching procedure is performed by using the Chebyshev distance measure, which is calculated using eqn (10).

$$D_{chebyshev}(x, y) = max_i(|x_i - y_i|) \quad (10)$$

In Eqn (10), x is represented as a template feature, and y is a test iris feature. The estimated similarity value is compared to the threshold value of 0.3. If the value is the maximum value, it should be compared to the threshold value, and if the user is accepted they may have access to the data or their access will be terminated. Finally, the RSA decryption process is used to decrypt the personal health record and use it. The effectiveness of multi-factor authentication is evaluated using the test analysis discussed in the next section.

IV. RESULTS AND DISCUSSION

This section discusses the advanced multi factor authentication process for accessing personal health records in a cloud environment. During this process, health records are encrypted with the help of the standard RSA algorithm which is stored on a third-party server. When users attempt to access health data, they are authenticated via multi factor to provide greater security to the data. Contextual authentication, signcryption and biometric based verification process ensures that authentication establishes trust between the user and the service provider. In addition, the multi factor algorithm ensures data security, privacy, and confidentiality also creates difficulties when predicting a shared key value. The performance of the system is evaluated using encryption time (converting plain text to cipher text), decryption time (converting cipher text to original text), and authentication (confirming user identities performed through the encryption and encryption process). Authorization (granting access to the user) and security (eliminating unnecessary intermediate access and changes data). The VA Personal Health Record Sample Database [30] is used to evaluate the effectiveness of the system during the implementation process. The implementation is done with the python language version 3.6.5. According to the discussion, the obtained encryption and decryption time is depicted in table 1 (a) and (b) [31].

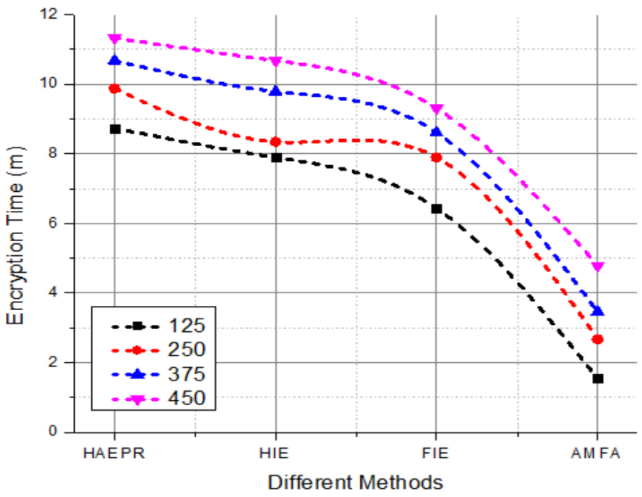
Table 1: (a) Encryption time

Method/ Data	HAEPR	HIE	FIE	AMFA
125	8.73	7.89	6.43	1.54
250	9.872	8.34	7.89	2.67
375	10.67	9.78	8.6	3.45
450	11.32	10.67	9.3	4.78

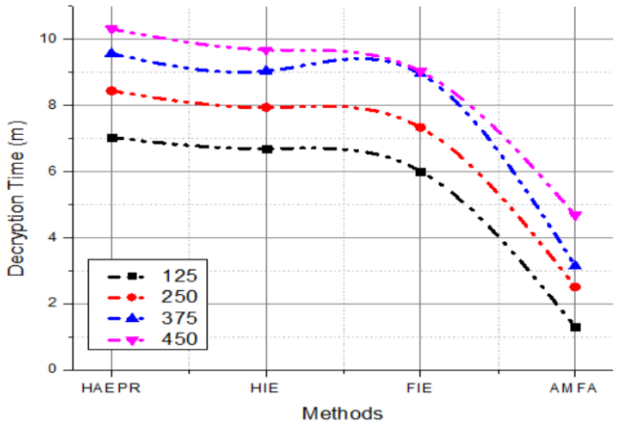
Table 1: (b) Decryption time

Method/ Data(b)	HAEPR	HIE	FIE	AMFA
125	7.02	6.68	6	1.3
250	8.43	7.93	7.32	2.5
375	9.56	9.03	8.94	3.14
450	10.3	9.67	9.02	4.67

In the above table 1 (a) and (b), AMFA encryption and decryption time is compared with different existing methods. In that, AMFA has done very well in a very short time. In this, the execution time is measured in minutes and the amount of data in bits. The figure 2 (a) & (b) below illustrates them clearly.



(a)



(b)

Figure 2: (a) encryption time and (b) decryption time

Figure 2 illustrates that Advanced Multi Factor Authentication (AMFA) ensures minimum encryption and decryption time when storing and accessing health data. The introduced AMFA algorithm effectively encrypts different size files. The proposed method encrypts in a very short time compared to the old methods namely, Hybrid Attribute-based Encryption with Proxy Re-encryption (HAEPR) [32], Hierarchical Identity-based Encryption (HIE) [33], Fuzzy Identity-based Encryption (FIE) [34]. As a result of the minimum encryption and decryption time, the system uses the minimum execution time while providing security for data. Therefore, the table value and graphical analysis of the overall system implementation time is depicted in table 2 and Figure 3.

Table 2: Execution time

Method/ Data	HAEPR	HIE	FIE	AMFA
125	7.04	6.64	6.1	1.5
250	8.45	7.94	7.35	2.6
375	9.54	9.02	8.95	3.13
450	10.2	9.68	9.03	4.65

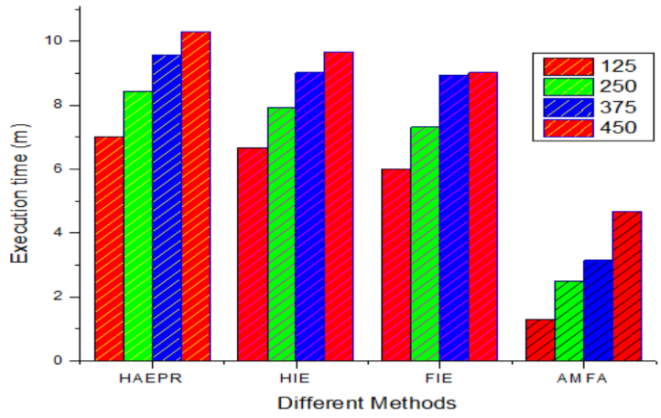


Figure 3: Execution Time

Figure 3 illustrates the execution time of the Advanced Multi-Factor Authentication (AMFA) system. From the analysis, it was clearly depicted that the AMFA algorithm ensures the minimum execution time for encrypting data and accessing data from the cloud. The execution time obtained is very short compared to other methods. In addition to this performance of the system is evaluated using authentication accuracy [35]. Due to the three stages of the verification process setup, only authorized users are allowed on the system. According to the discussion, the obtained accuracy value is demonstrated in table 3 and Figure 4.

Table 3: Authentication accuracy

Method/Data	HAEPR	HIE	FIE	AMFA
125	84.9	88.2	90.23	97.28
250	87.37	89.22	91.23	98.23
375	88.2	90.2	93.4	98.65
450	89.22	90.22	93.4	98.7

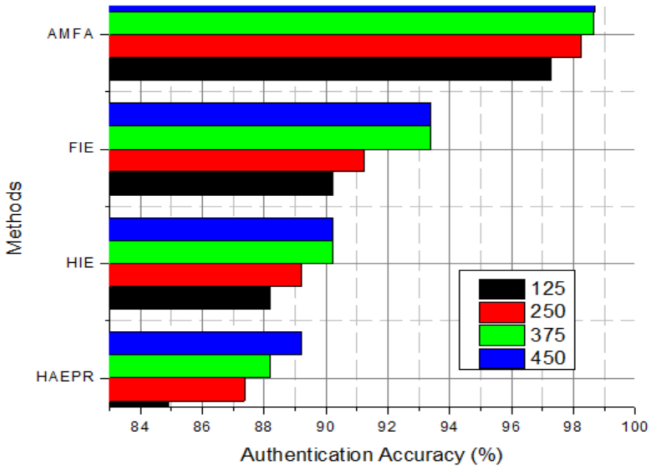


Figure 4: Authentication Accuracy

It is clear from table 3 and Figure 4 that the introduced AMFA system provides maximum accuracy (98.21%) for health records compared to other methods such as HAEPR (87.42%), HIE (89.46%) and FIE (92.06%). Therefore, the advanced multi factor authentication system maintains data security, privacy, and confidentiality with less operational time and accuracy compared to other methods. Also, data is successfully saved from unauthorized access.

V. CONCLUSION

Data protection and privacy are a very challenging issue as the data storage and access of the health department is done through a third party server. Furthermore, various research is being carried out worldwide to ensure data security and privacy. Based on that, this research has been experimented to provide additional security for data protection and privacy.

Especially in this work, the study examines advanced multi-factor authentication-based personal health records that maintain security in a cloud environment. Initially, PHR data is collected from VA Personal Health Record Sample Dataset. The collected dataset is stored in the cloud in encrypted format, using the RSA encryption method and hash function. Users are registered on the Cloud Server to provide authentication. Once the patient and authorized members wish to access the health data, they will be initially approved by the contextual authentication process. After verifying their location details, the signcryption verification process is performed using two secret keys. Finally, the iris bio-metric features are extracted and matched with the template features. These three layers of the verification process authenticate the user and eliminate intermediate access. The performance of the system is evaluated using test results using python language, in which the system ensures 98.21% authentication accuracy with minimum time. So, the proposed security system provides better security than the previous ones. In the future, novel algorithms can be defined to deploy in security systems. Hybrid algorithms and methods can be used for enhancing security also optimized techniques can be used to improve and protect the security of health data.

REFERENCE

1. Ben Rejab F., Nouira K., Trabelsi A. (2014) Health Monitoring Systems Using Machine Learning Techniques. In: Chen L., Kapoor S., Bhatia R. (eds) Intelligent Systems for Science and Information. Studies in Computational Intelligence, vol 542. Springer, Cham
2. Smys, S., Kumar, A.D.: Secured WBANs for pervasive m-healthcare social networks. In: 10th International Conference IEEE on Intelligent Systems and Control (ISCO), January 2016, pp. 1–4. (2016)
3. Li M., Yu S., Ren K., Lou W. (2010) Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings. In: Jajodia S., Zhou J. (eds) Security and Privacy in Communication Networks. SecureComm 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 50. Springer, Berlin, Heidelberg
4. Ibraimi, L., Asim, M., Petkovic, M.: Secure management of personal health records by applying attribute-based encryption. Technical Report, University of Twente (2009)
5. Korde P, Panwar V, Kalse S (2013) Securing personal health records in cloud using attribute based encryption. IEEE Trans Parallel Distrib Syst 2(Issue 4) ISSN: 2249–8958
6. Zheng Y, Ren K, Li M, Yu S, Lou W (2013) Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans Parallel Distrib Syst 24(No. 1)
7. Barouti S., Aljumah F., Alhadidi D., Debbabi M. (2014) Secure and Privacy-Preserving Querying of Personal Health Records in the Cloud. In: Atluri V., Pernul G. (eds) Data and Applications Security and Privacy XXVIII. DBSec 2014. Lecture Notes in Computer Science, vol 8566. Springer, Berlin, Heidelberg
8. Chen, Y., Ding, S., Xu, Z. et al. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J Med Syst 43, 5 (2019). https://doi.org/10.1007/s10916-018-1121-4
9. Wang, Z., Provably secure key-aggregate cryptosystems with auxiliary inputs for data sharing on the cloud. Futur. Gener. Comput. Syst., 2017.
10. Da Veiga, Adéle; Martins, Nico (2015). "Improving the information security culture through monitoring and implementation actions illustrated through a case study". Computers & Security. 49: 162–176. doi:10.1016/j.cose.2014.12.006. hdl:10500/21765.
11. Sangeetha, D., Vaidehi, V. A secure cloud based Personal Health Record framework for a multi owner environment. Ann. Telecommun. 72, 95–104 (2017). https://doi.org/10.1007/s12243-016-0529-4
12. Liu Z, Cao Z, Huang Q, Yuen TH, Wong DS (2011) Fully secure multi-authority ciphertext-policy attribute based encryption without random oracles. In: Computer Security-ESORICS, pp 278–297
13. Dixit P., Gupta A.K., Trivedi M.C., Yadav V.K. (2018) Traditional and Hybrid Encryption Techniques: A Survey. In: Perez G., Mishra K., Tiwari S., Trivedi M. (eds) Networking Communication and Data Knowledge Engineering. Lecture Notes on Data Engineering and Communications Technologies, vol 4. Springer, Singapore
14. Rajdeep Bhanot, Rahul Hans, "A Review and Comparative Analysis of Various Encryption Algorithms". In International Journal of Security and Its Applications, Volume 9, No. 4 (2015), pp. 289–306.
15. Tipton, S.J., Forkey, S. & Choi, Y.B. Toward Proper Authentication Methods in Electronic Medical Record Access Compliant to HIPAA and C.I.A. Triangle. J Med Syst 40, 100 (2016). https://doi.org/10.1007/s10916-016-0465-x
16. Chen C.W., Osman M.A., Zaaba Z.F., Talib A.Z. (2017) Managing Secure Personal Mobile Health Information. In: Akagi M., Nguyen TT., Vu DT., Phung TN., Huynh VN. (eds) Advances in Information and Communication Technology. ICTA 2016. Advances in Intelligent Systems and Computing, vol 538. Springer, Cham
17. Abouelmehdi, K., Beni-Hessane, A. & Khaloufi, H., "Big healthcare data: preserving security and privacy", J Big Data (2018) 5: 1. https://doi.org/10.1186/s40537-017-0110-7
18. China Appala Naidu R., Srujan A., Meghana K., Srinivas Rao K., Madhuravani B. (2019) Secure Privacy Preserving of Personal Health Records Using Attribute-Based Encryption in Cloud Computing. In: Bapi R., Rao K., Prasad M. (eds) First International Conference on Artificial Intelligence and Cognitive Computing. Advances in Intelligent Systems and Computing, vol 815. Springer, Singapore
19. Guojun Wang, Qin Liu, Jie Wu, MinyiGuo, 2011, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Journal Computers and Security, Volume 30 Issue 5, ACM.
20. PrajaktaSolapurkar, GirishPotdar, 2012, "A Survey on Secure Data Sharing and Collaboration Approaches in Cloud Computing", International Journal of Science and Research
21. Huda Elmogazy ; Omaima Bamasak, "Towards healthcare data security in cloud computing", International conference on Internet Technology and Secured Transactions in IEEE, 2013.
22. Patel, V., and Siminerio, E., Consumer Access and use of Online Health Records: It Takes Two to Tango. Health IT Buzz, 2014. Retrieved from http://www.healthit.gov/buzz-blog/consumer/consumer-access-online-health-records/.
23. Mir, S. S., HIPAA Privacy rule: Maintaining the confidentiality of medical records, Part 2. J. Health Care Compliance 13(3):35–78, 2011.
24. Cao B., Xu T., Wu P. (2018) RSA Encryption Algorithm Design and Verification Based on Verilog HDL. In: Gu X., Liu G., Li B. (eds) Machine Learning and Intelligent Communications. MLICOM 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 226. Springer, Cham
25. Tenca, A.F., Ruggiero, W.V.: CRT RSA decryption: modular exponentiation based solely on Montgomery multiplication. In: Asilomar Conference on Signals, Systems and Computers, pp. 431–436 (2015)
26. Buhan I., Lenzini G., Radomirović S. (2010) Contextual Biometric-Based Authentication for Ubiquitous Services. In: Yu Z., Liscano R., Chen G., Zhang D., Zhou X. (eds) Ubiquitous Intelligence and Computing. UIC 2010. Lecture Notes in Computer Science, vol 6406. Springer, Berlin, Heidelberg
27. Lu M., Wu Y., Xu Y., Yang Y., Wang J. (2018) SACP: A Signcryption-Based Authentication Scheme with Conditional Privacy Preservation for VANET. In: Chellappan S., Cheng W., Li W. (eds) Wireless Algorithms, Systems, and Applications. WASA 2018. Lecture Notes in Computer Science, vol 10874. Springer, Cham
28. Han Y., Fang D., Yue Z., Zhang J. (2014) SCHAP: The Aggregate SignCryption Based Hybrid Authentication Protocol for VANET. In: Hsu R.CH., Wang S. (eds) Internet of Vehicles – Technologies and Services. IOV 2014. Lecture Notes in Computer Science, vol 8662. Springer, Cham
29. Zhu, Y., Tan, T.: Yusag: Biometric Personal Identification based on Iris Patterns. In: 15th Internal Configuration Pattern Recognition, vol. 2(3), pp. 801–804 (2004)
30. https://catalog.data.gov/dataset/va-personal-health-record-sample-data
31. AmbadasVairagar, Rahul Kanthale, SandeepPawar, Markad, 2016, "A Survey on Sharing of PHR using ABE in Semi-trusted Servers", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 2.

32. Changji Wang, XileiXu, Dongyuan Shi, Jian Fang, 2015, "Privacy-Preserving Cloud-Based Personal Health Record System Using Attributebased Encryption And Anonymous Multi-Receiver identity-Based Encryption" International Journal of Computing and Informatics.
33. Deep, G., Mohana, R., Nayyar, A., Sanjeevikumar, P., & Hossain, E. (2019). Authentication Protocol for Cloud Databases Using Blockchain Mechanism. Sensors, 19(20), 4444.
34. Deep, G., Mohana, R., Nayyar, A., Sanjeevikumar, P., & Hossain, E. (2019). Authentication Protocol for Cloud Databases Using Blockchain Mechanism. Sensors, 19(20), 4444.
35. Nishaal J. Parmar, Pramode K. Verma, A Comparative Evaluation of Algorithms in the Implementation of an Ultra-Secure Router-to-Router Key Exchange System, Security and communication networks.

AUTHORS PROFILE

Meena.S, I am a computer science researcher (part-time), Periyar University, Salem. I have six years of experience as a college assistant professor in department of computer science and one and a half years as a research assistant in Sirius techno solution at Coimbatore. I have published 6 articles in the domain of cloud computing at various international journals and conferences. I have research interests in the area of cloud computing, cloud security, data mining, image processing.

Dr.V.Gayathri completed her PhD in Computer Science at the Vinayaka Mission University, Salem. Currently working as an Assistant professor at the Pee gee College of Art and Science, Dharmapuri. She has experience in teaching and research for more than 13 years. She has guided many M.Phil. Scholars and currently guiding 4 Ph.D. scholars. She has published more than 15 international journals and articles in different domains of computer science. Her main area of interests are cloud computing, data mining and wireless networks.