Asian Journal of Applied Science and Technology (AJAST)
(Peer Reviewed Quarterly International Journal) Volume 2, Issue 4, Pages 124-131, Oct-Dec 2018

Ensuring the Privacy of Patient Health Records (PHR) Sharing Scheme in Public Cloud by the Hybrid Encryption Cryptography

Safeena C[1] and VR. Nagarajan[2]

[1]*Research Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore - 641 105.*
[2]*Assistant Professor, PG & Research Department of Computer Science, Sree Narayana Guru College, Coimbatore - 641 105.*

Article Received: 25 May 2018 *Article Accepted: 27 September 2018* *Article Published: 08 October 2018*

ABSTRACT

Secured cryptographic algorithms are developed for the enterprise or for the purpose of individuals since they don't have complete trust on others for sharing the confidential information. Most of the individuals or organizations need to gather, examine and propagate the information hastily and accurately Many types of entities need to collect, analyze, and disseminate data rapidly and precisely, without revealing the confidential information to illegal parties. Hence the emergence of cloud computing helps the users to store and upload the huge amount data in remote public cloud servers. The cloud computing serves as the medium for administering their data but this is not entirely trusted by the individual users. On the other hand, if the confidential information outsourced to the public cloud the privacy preserving data security turns out to be the immediate problem in public clouds. The proposed work presents the hybrid encryption algorithms for sharing the private information efficiently in the public clouds. The method comprise of hybrid encryption which is the combination of Advanced Encryption Standard (AES) and RSA algorithm for preserving the privacy of sensitive information onto the cloud. The projected method affords bendable effectiveness of data during the disputes occurred in data sharing. The approach is reasonable and effective. The work is developed for sharing Patient Health Records (PHR) of the patients in public clouds. The privated health information is made to be more secured by cryptographic encryption algorithms.

Keywords: PHR, AES, RSA, Public clouds, Data sharing.

1. INTRODUCTION

A Patient health record (PHR) is an authorized health records or the documents that is shared between various amenities and organizations. The functioning of PHRs is more expanding and dominant because most the patient records are made digital and the maximum number of customers articulate a yearning to view the health records with the help of mobile access [17]. The PHR is the form of an electronic application that includes the patient's health chart. The patients can maintain and store their medical information in a secured environment. They are mostly patient oriented information available only to certified users.

PHR generally includes:

- History about the patient's disease, treatment and the plan, immunization schedule, allergies and the laboratory test reports.
- Detailed information regarding health care visits with the professionals
- Hospitalization records
- Surgery information

The main attribute of PHR is that the health records can be generated and administered by certified users in the electronic way and the information can be shared between multiple care enterprises. Since the patients health records are increasing the digital formats can be stored in the public clouds and it can be shared among the multiple organizations and it is shown in figure 1.

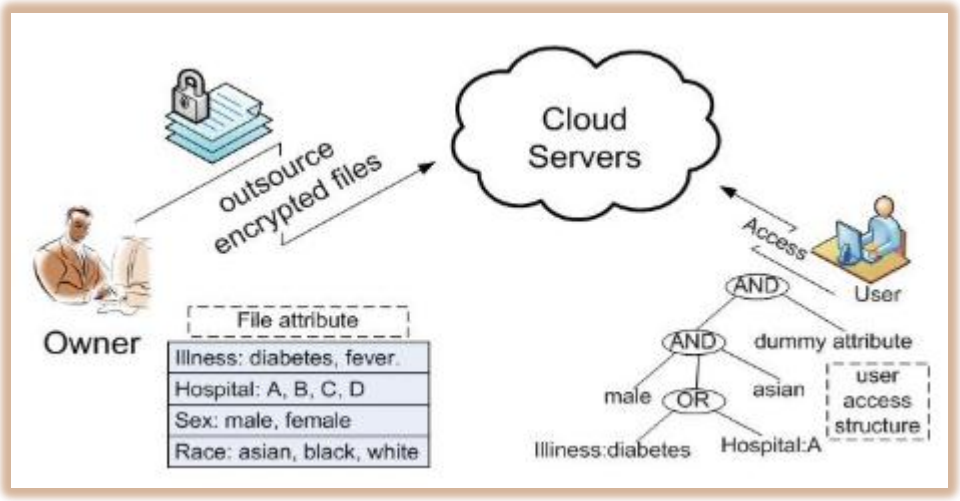

Figure No: 1 Cloud Computing Scenario for PHR

The enormous development in the field of cloud computing made the users to transfer the information to the public cloud servers. The cloud computing mitigates the data management consumption, information processing and the cost coverage of the system and personnel maintenance [4]. Even though the cloud computing is filled with more advantages it is affected with more barriers which makes the organization more hesitant to transfer the information to the cloud server. The owner and the controller of the public cloud are public cloud servers (PCS) but this turn to be untrusted because the information may be stolen by it or it may obtain the stored user information. Hence there is a necessity of security mechanism for enhancing privacy preserving in public clouds.

The data sharing is very important in cloud computing applications particularly for the organization. The information has to assure the at most security in various applications: a) privacy preserving data b) illegal access should not be able to obtain the outsourced information and the remote data can be shared among the others. Data sharing method has to be designed for the attainment of data confidentiality and information privacy. Here, the PHR involves more protection because of the privacy of the patients. The patient's electronic health records are stored and it can be accessed only by certified entities. The illegal access does not obtain the medical or health data by ensuring the data confidentiality [16]. Hence the data integrity and data confidentiality can be afforded by the hybrid encryption mechanism called AES encryption and RSA encryption.

The research work deals with offering a solution in ensuring the secure data storage in the cloud. Before transferring the information to the cloud, the information must be encrypted. The symmetric enciphering method called AES and the asymmetric enciphering method called RSA is utilized for obtaining the benefits like security, heftiness and speed. The information is enciphered by the AES algorithm and it is stored in the public cloud. Then the AES key is enciphered by the RSA algorithm and it is intern stored in the server. The data integrity and confidentiality assured by affording data access by having authentication. This type of hybrid encryption is performed for securely storing the data and improves the conflicts to various attacks.

2. RELATED WORK

While uploading huge amount of information in public clouds the new model for information management has to be developed. The information sharing is the obligatory service method from the cloud computing. For performing data sharing in cloud, Chu et al. [1] projected new method of public-key cryptosystems. The newly model can create cipher texts which are of constant-size by understanding the allocation of providing rights for decryption of cipher texts. Tong et al. [2] investigated the problem of privacy of mobile healthcare systems by the usage of private cloud. Pervez et al. [3] projected the self healing attribute-based privacy method that is conscious about the information sharing in cloud. To comprehend the management of dynamic membership with random states, Fan et al. [4] developed an attribute-based encryption method. Boneh et al. [5] developed and built a public key encryption scheme with the combination of searching the keyword. Cao et al. [6] projected a general method for searching the multi-keyword rank over encrypted data of the cloud, and then they offer two methods of drastically enhanced multi-keyword ranked investigate methods that can gratify various methods of rigorous privacy requirements. The interceded certificate less encryption method was developed by Seo et al. without pairing operations. They interceded certificate less encryption scheme is utilized to develop an effectual confidential information sharing method in public clouds [7]. Various works are found for the data authentication and information matching.

Hence the huge improvement of health records, the data is uploaded into the public clouds by more number of hospitals and hand over the public cloud afforders to handle their information. Storing of Medical/health records have data security has fascinated many of the researchers. Li et al. [8] developed a new patient-centric structure and a mechanism for information access control to personal health records that is stored in the semi-trusted servers. Benaloh et al. [9] constructed an effectual method that permits the patients for sharing the limited access control rights among others, and to execute the record searching. Sun et al. projected a secured method of cryptographic mechanisms for electronic health record system for enabling the secured sharing of confidential information of the patient's data through collaboration and conserve the information privacy of the patient. Again the method is integrated with various mechanisms for controlling the fine-grained access and revoking the on-demand service, since it is an improvement to the general access control feature provided by the delegation and revocation method respectively [10]. The rest of the sections are organized as follows: section 3 describes the characteristics of cloud computing, section 4 describes enhancing security in cloud computing, section 5 describes incorporating hybrid encryption into public clouds, section 6 describes the results and discussion, section 7 describes the results and section 8 gives the references.

3. CHARACTERISTICS OF CLOUD COMPUTING

The important feature emerged in the development of software in the recent days. This method utilized the feature of calculating the storage capacity of the servers and the computers. The software and hardware can be utilized by the individual users of the cloud that are administered by other users at remote locations [13]. The Security prevailing in cloud computing includes the features like network security, apparatus and control mechanisms organized to safe guard the data, various infrastructure and applications connected with cloud computing. The most

significant part of the cloud computing is the conception of interconnection with various materials that makes the situation hard and providing security to environments. Security problems in a cloud platform may cause economic loss and brings poor reputation when there is more number of public users and these are the reasons for the massive approval. The security feature permits the data confidentiality, availability, integrity and authenticity [11]. The betterment of the technologies and their regularity makes accessible a variety of algorithms and rules for acknowledgement to the problems.

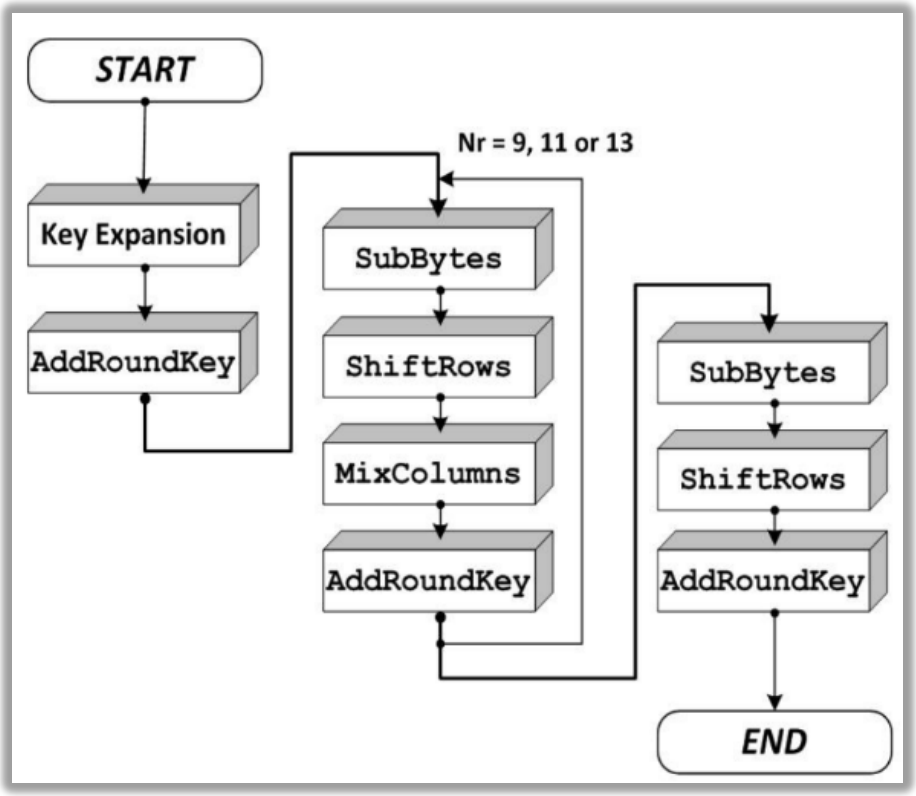

Figure No: 2 AES Encryption

4. ENHANCING SECURITY IN CLOUD COMPUTING

4.1 AES Algorithm

AES is a variation of Rijndael with the fixed block size of 128 bits and a key size of 128, 192, or 256 bits. The size of the key specified in the AES cipher is denotes the number of reverberation of the transformation rounds [14]. The key size used for an AES cipher specifies the number of repetition of transformations rounds and it is described in figure 2. The replications are given below:

- 10 rounds of transformation with the key size of 128-bit keys.
- 12 rounds of transformation with the key size of 192-bit keys.
- 14 rounds of transformation with the key size of 256-bit keys.

The benefits of the AES algorithm are not prone to any type of attack but it is susceptible to brute force attack. Conversely, the type of Brute Force attack is not a simple job even for a super computer because the size of the encryption key employed by AES algorithm which is in the order 128, 192 or 256 bits. This is the integration of

more number of permutations and combinations. The characteristics like High speed and low RAM prerequisites of the AES selection process. Thus AES executes well on a extensive variety of hardware i.e. from 8-bit smart cards to high-performance computers. The traditional algorithms are slower when compared to AES and hence AES is adopted. In the recent days, AES S-box is proposed to be more effectual.

4.2 RSA Algorithm

The most widespread Public Key encryption algorithm is RSA that is named after the inventors Rivest, Shamir, and Adelman of MIT. RSA is essentially an asymmetric encryption/decryption algorithm. Here the public key is dispersed to all the users during which one can encipher the information and for performing the decryption process the private key is used by making it secret and not sharable with other users [15]. The method is completely based on the exponentiation in a limited field over integers modulo a prime numbers and the method is described in figure 3. The process of the RSA algorithm is described in figure 4.

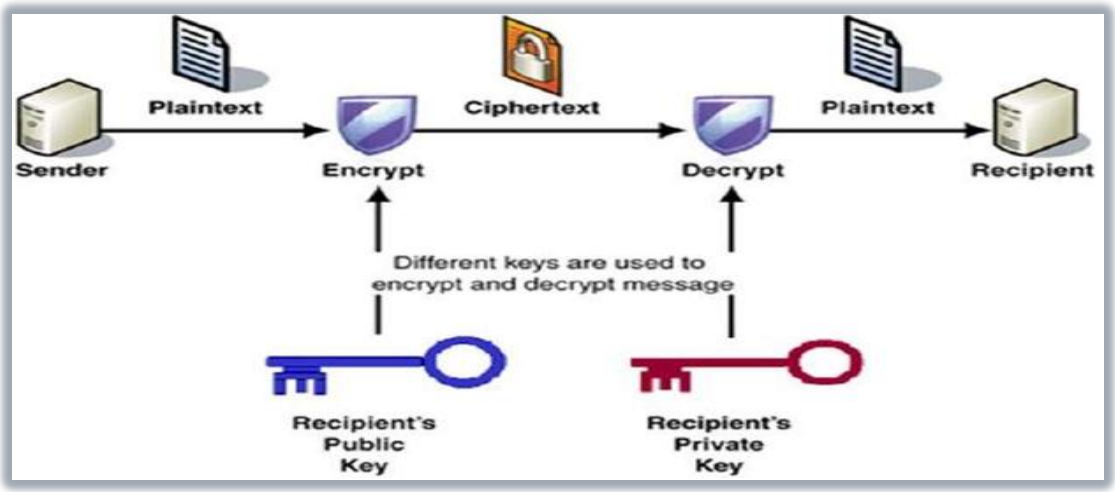

Figure No: 3 RSA Algorithm

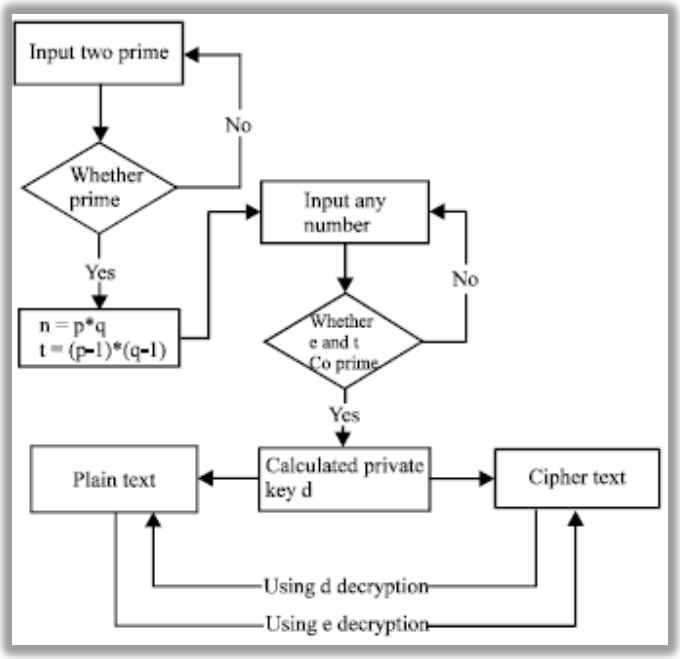

Figure No: 4 Process of the RSA

Online ISSN: 2456-883X

5. INCORPORATING HYBRID ENCRYPTION INTO PUBLIC CLOUD

The cloud storage must be provided with the accurate, secure and competent algorithm for securing the information that is stored in cloud. This type of hybrid algorithm recommends the file encryption to be uploaded on the cloud. The data integrity and confidentiality uploaded by the user is certified twice as by not only enciphering it but also affording the data access on flourishing authentication. The file can be enciphered using AES algorithm. To improve the security; AES key will be enciphered using RSA algorithm and will be stored in intern server. The certified user can also download any of the uploaded enciphered files and read it on the system and the process id described in figure 5.

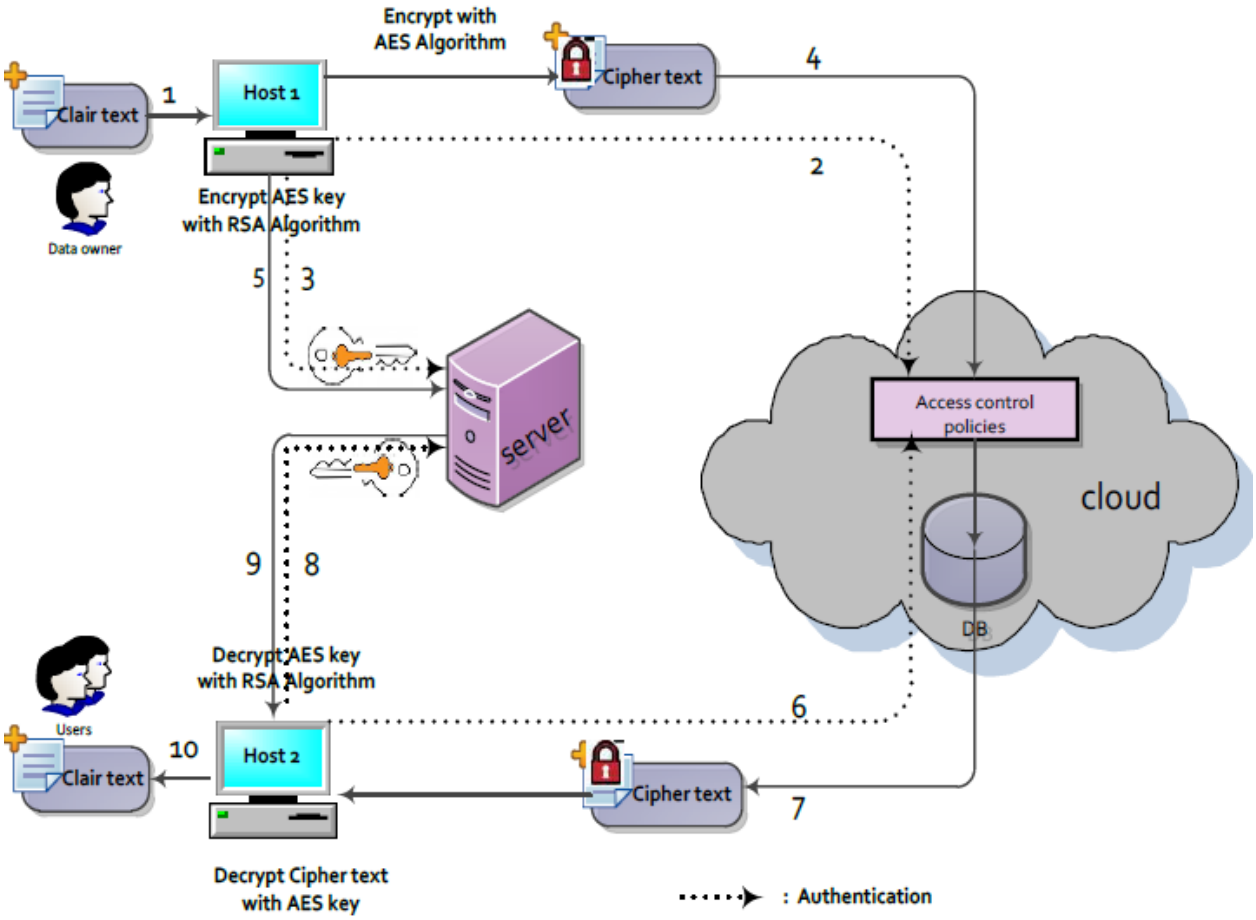

Figure No: 5 Proposed Model

6. RESULTS AND DISCUSSION

The result shows that while uploading PHR files, the security is more improved by the hybrid encryption algorithm. The accuracy of the algorithm is also calculated by taking the encryption and decryption time of the loaded file. The information is encrypted and sent to the cloud from the original machine to the receiving side and the decryption key mechanism is not present in the cloud. AES algorithm is termed as fast and more secured. The attackers are not able to break the content. This hybrid mechanism reaches the highest level of security. The comparison of the encryption and decryption time is shown in figure 6 and table 1.

 Online ISSN: 2456-883X

S.No	File Size	Encryption Time (seconds)	Decryption Time (seconds)
1	128	0.4	0.5
2	256	0.3	0.7
3	512	0.8	1.7
4	1024	1.8	3.4
5	2048	3.3	6.8

Table No: 1 Execution Time for Encryption and Decryption

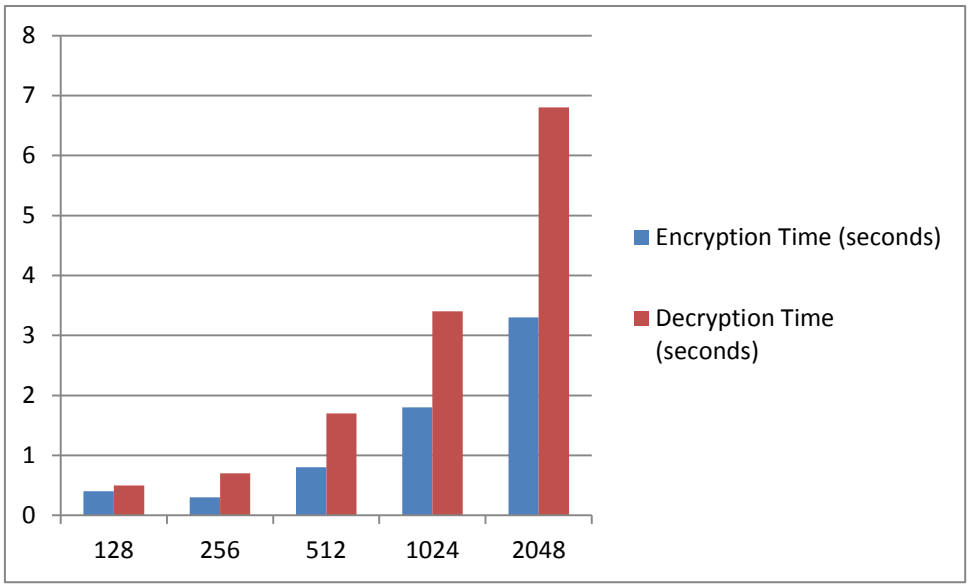

Figure No: 6 Execution Time for Encryption and Decryption

7. CONCLUSION

The cloud storage may have more advantages it is facing the security challenges. In this paper, we proposed a data sharing scheme which can achieve the anonymity and data confidentiality in public clouds. When the security criteria are eliminated the opportunity is going to be Cloud storage solutions for many business organizations. In this paper, a solution is suggested that permits the data storage in an open cloud. The information security is offered by executing this proposed algorithm. Only the legal users can have the data accessibility. When the intruder (unauthorized user) attempts to get the information inadvertently or deliberately, the user can not decipher it and requires two types of keys impending from two diverse locations.

REFERENCES

[1] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng,``Key-aggregate cryptosystem for scalable data sharing in cloud storage,,"IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 468477, Feb. 2014.

[2] Y. Tong, J. Sun, S. S. M. Chow, and P. Li, ``Cloud-assisted mobile-access of health data with privacy and auditability," IEEE J. Biomed. Health Inform., vol. 18, no. 2, pp. 419429, Mar. 2014.

[3] Z. Pervez, A. M. Khattak, S. Lee, and Y.-K. Lee, ``SAPDS: Self-healing attribute-based privacy aware data sharing in cloud," J. Supercomput., vol. 62, no. 1, pp. 431460, Oct. 2012.

[4] C. Fan, V. S.-M. Huang, and H.-M. Ruan, ``Arbitrary-state attribute-based encryption with dynamic membership," IEEE Trans. Comput., vol. 63, no. 8, pp. 19511961, Apr. 2014.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, ``Public key encryption with keyword search," in Advances in CryptologyEUROCRYPT. Interlaken, Switzerland: Springer-Verlag, May 2004, pp. 506522.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ``Privacy-preserving multikeyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222233, Jan. 2014.

[7] S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, ``An efficient certificateless encryption for secure data sharing in public clouds," IEEE Trans. Knowl. Eng., vol. 26, no. 9, pp. 21072119, Sep. 2014.

[8] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ``Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131143, Jan. 2013.

[9] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, ``Patient controlled encryption: Ensuring privacy of electronic medical records," in Proc. ACM Workshop Cloud Comput. Secur., Chicago, IL, USA, Nov. 2009, pp. 103114.

[10] J. Sun and Y. Fang, ``Cross-domain data sharing in distributed electronic health record systems," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 6, pp. 754764, Jun. 2010.

[11] KOLODNER, Elliot K., TAL, Sivan, KYRIAZIS, Dimosthenis, et al. A cloud environment for data-intensive storage services. In : Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on. IEEE, 2011. p. 357-366.

[12] P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, « Cloud Computing Security Issues in Infrastructure as a Service », Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no 1, 2012.

[13] M. D. K. Kumar, G. V. Rao, and G. S. Rao, « Cloud Computing: An Analysis of Its Challenges & Cloud Computing: An Analysis of Its Challenges & Security Issues ».

[14] ZHANG, Xiaoqiang, WU, Ning, YAN, Gaizhen, et al. Hardware Implementation of Compact AES S-box. IAENG International Journal of Computer Science, 2015, vol. 42, no 2.

[15] L. Arockiam, S. Monikandan « Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm » International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[16] Benaloh, J., Chase, M., Horvitz, E., Lauter, K.: Patient controlled encryption: ensuring privacy of electronic medical records. In: CCSW 2009: Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 103–114 (2009).

[17] Mandl, K.D., Szolovits, P., Kohane, I.S.: Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ 322(7281), 283 (2001).