www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 2 Feb. 2017, Page No. 20215-20220
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i2.09

Securing E-healthcare records on Cloud Using Relevant data classification and Encryption

Rizwana Shaikh [1], *Jagrutee Banda*[2], *Pragna Bandi*[3]
[1]Department of Computer Engg.,
SIESGST, Nerul , Navi Mumbai, India
rizwana.shaikh@siesgst.ac.in
[2]Department of Computer Engg.,
SIESGST, Nerul, Navi Mumbai, India
manjagprag@gmail.com
[3]Department of Computer Engg.,
SIESGST, Nerul, Navi Mumbai, India
manjagprag@gmail.com

Abstract: ***Information security is always the area of concern for cloud users. The confidentiality of the Electronic Health Records (EHRs) is major issue when commercial cloud servers are used by hospital staff to store the patients' medical records because it can be viewed by everyone. There are various issues and challenges toward achieving detailed data access control based on cryptography. To achieve fine grained and scalable data access control for medical records stored in cloud servers, we propose Attribute Based Encryption (ABE) techniques such as key policy attribute based encryption, role based encryption, etc. to encrypt each patient's medical record file. For this we describe an approach which enables storage which is secure and patient's health data with controlled sharing. We explore key-policy attribute based encryption to gain patient access control policy such that everyone can download the data, but only authorized user can view the medical records. A high degree of patient privacy is maintained using multiple cryptographic algorithms applied on the various types of data.***

Keywords: Information security, confidentiality of EHRs, cloud, ABE, authorized users, cryptographic algorithms, data classification.

I. INTRODUCTION

Digital Technology has drastically changed our daily lives and the way of communication. Medicine is an information-oriented entity. Maintaining paper-based records of patients in the healthcare organizations can become strenuous with time. To attain smooth flow of information within a healthcare infrastructure, Electronic Health Records are used. Electronic health record (EHR) systems can completely digitize the health care system that utilizes clinical information to help providers deliver higher quality of care to their patients.

The EHRs can automate and streamline the doctor's workflow and can generate a complete record of patients thus enhancing the quality of care. With EHRs, it is possible to access information anywhere anytime.

Associated with EHRs is the major concern of Security and Privacy of the records. Exposing sensitive information to unauthorized entities can lead to stigma and embarrassment to that particular patient. Also, tampering with health record information can completely change its meaning; it is an offense and can cause humiliation to the patient's dignity.

When these records are outsourced on a public platform, then the job to secure these records increases even more. So for such privacy to be maintained there is urgent need to take the required measures to protect the health records by allowing only authorized users to view these records.

So here we are proposing data classification encryption technique that is used to protect the records confidential data.

II. LITERATURE REVIEW

Security of EHRs has been the topic of research since the past few years. Many authors have discussed issues and proposed their solutions to incorporate security of EHRs as well as cloud-based EHRs.

Researchers have examined the pros and cons of EHRs by considering clinical outcomes. Many clinical outcomes relate to quality of care and patient safety. Quality of care is doing the right thing at the right time in the right way to the right person and having the best possible results and patient safety is avoiding injuries to patients from the care that is intended to help them. Security and privacy of records is our major concern. There are more and more healthcare organizations adopting for EHRs (Electronic Health Records), there storage becomes a concern and cloud provides inexpensive as well as flexible solution and wide-area mobile access is increasingly needed in the modern world which makes the cloud storage compelling for deploying EHRs. Although it has its own benefits, but cloud-based EHR systems must address data security, patient privacy and overall performance before they are deployed in the real world.

The author in the paper [1] throws light on how modern healthcare environments where healthcare providers are more agreeable to migrate their electronic medical record systems to clouds. This enables to achieve lower operational cost and excellent interoperability with other healthcare providers rather to opt for building and maintaining dedicated data centers. Adoption of cloud computing in healthcare systems, however, may also raise many security challenges associated with identity management, authentication, access control, trust management, and so on. In this paper, focus is on access control issues faced in electronic medical record systems in clouds. The author of the paper [2] focuses on moving patients' medical information to the Cloud that implies several risks related to the security and privacy of sensitive health records. The risks of hosting Electronic Health Records (EHRs) on the cloud servers of third-party Cloud service providers are reviewed. Some suggestions for healthcare providers regarding the protection of confidentiality of patient information and process facilitation are made. Analysis of arising security and privacy issues in access and management of EHRs is discussed in the paper [3]. They also describe an EHR security reference model for managing security issues in healthcare clouds. Author in [4] proposes the use of Cipher-text-Policy Attribute-Based Encryption (CPABE) to encrypt EHRs which are based on healthcare providers' attributes or credentials, to decrypt EHRs; they must possess the set of attributes needed for proper access. According to the paper on[5] the existing security solutions for such EHR systems mainly focus on the authentication to realize that a user's private data cannot be illegally accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions**.** In the existing systems, authentication is addressed but there is no focus on privacy issues.

Also, traditional storage systems do not have significant savings. It is possible that security of confidential information can be compromised when users challenge cloud server to request other users for data sharing, hence, this issue will be addressed using encryption on EHRs. In the previous systems, data classification was not performed on medical information. Hence, we propose "SECURE" to secure medical healthcare records before outsourcing these records to public that will in turn help in maintaining data security, availability and integrity.

III. PROPOSED SYSTEM

The objective of proposing a system for maintaining EHRs is to secure them before deploying them for sharing among healthcare providers.

The proposed system is based on the following:

- A web-based system with secure login and registration.
- Cloud storage for flexible retrieval and is a feasible alternative
- Data Classification and Encryption.

➢ **Web-Based System With Secure Login And Registration:**

A web-based system can be accessed anywhere, anytime with the help of good internet connectivity. The system will be designed in such a way that only authorized users to access the relevant information. Patients and doctors have to first register. After registration, they will be a given a Unique Key that will be used by them to avail the information.

➢ **Cloud Storage For Flexible Retrieval And Is A Feasible Alternative:**

Cloud storage provides rapid deployment. It has greater accessibility and reliability, also data backup and disaster recovery is possible. The overall storage costs are low because there is no need of purchasing, managing and maintaining expensive hardware that makes Cloud storage economically feasible.

➢ **Data Classification and Encryption:**

Classification will be done on the basis of sensitivity levels of confidential medical information.

Data that falls under higher sensitivity will be given more security focus as compared to its less sensitive counterpart.

Data will be classified as authentication information, personal details and medical tests and reports. Medical tests and reports need highest security from exposure to unauthorized access than authentication information and personal details.

This will be done using various cryptographic techniques like Rivest-Shamir-Adleman (RSA) Algorithm, Advanced Encryption (AES) Algorithm to provide security to the data according to their associated sensitivity level.

- AES, RSA for providing confidentiality.
- Hashing techniques such as SHA-1, MD5 for integrity, e.g. passwords.
- For authenticity we propose digital signatures.
- Security for databases.
- Possible elimination of different attacks like SQL Injection, Cross Side-Scripting, etc.

We propose SECURE a central unified platform for doctors and patients of all the hospitals where the system is able to store electronic healthcare records in encrypted form on cloud using various cryptographic techniques and using relevant data classification on those records. Data classification enables the record's data to be classified into various levels of varying sensitivity. The need to segregate data based on such levels of sensitivity was due to the need to maintain confidentiality of those records since the doctor patient privileges are of utmost concern. A patient would not want any outsider to view his/her records. And as such records are leased on cloud where cloud is accessible by everyone, security becomes a major concern. The most plausible way to provide security to these records is via encryption.

There are various cryptographic techniques available and each varies with respect to cryptanalysis. It is optimal to encrypt higher sensitive details with higher level of encryption where hiding such information is a major focus. Lower sensitive details of an electronic such as report time and date which become important at some specific times can be encrypted with the lower level of encryption. The system also maintains privileges permission according to the authority level of the user. To explain it simply a patient is not allowed to update or create records but a doctor can. Therefore SECURE as a unified system is accessible by different types of people ranging from a receptionist at a hospital or to a doctor or an administrator but with different privileges to access the resources of the system to ensure the authoritative limitations are maintained and thus security is availed by the system. An electronic healthcare record has various types of information in it. Classifying the information is a step forward in making the record more secure and achieving confidentiality of records from interceptors and attackers.

Main purpose of classification:

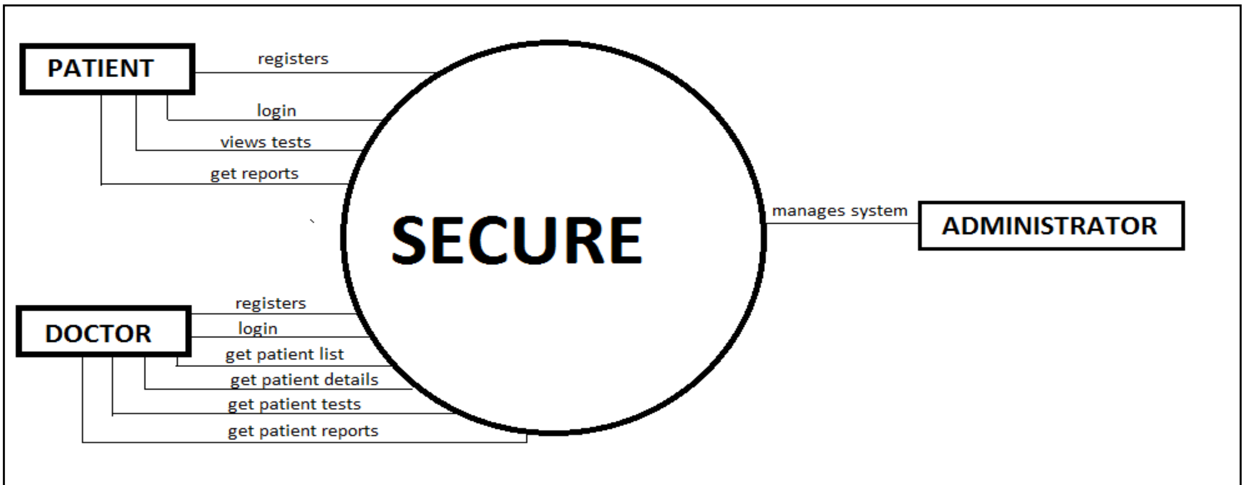
- Maintains simplified data view.
- Classification allows proper discretion of records where each record can be thought of divided into entities of similar level of sensitivity.
- Disclosure of particular type of entity is based on keys required to unlock the cipher used for encryption for that particular part.
- Classification allows the system to take secret key as input from user, apply some algorithm on that key and generate different system generated keys which are further used for encipherment of different entities of same sensitive level.
- It allows increased time for cryptanalysis which increases the security factor of electronic healthcare records.
- Easy retrieval of data from database, since the system is known about the classified data.

IV. IMPLEMENTATION

The proposed system implements data classification based on the sensitivity levels of data i.e. for higher sensitive data higher level of encryption will be enforced and lower sensitive data will use lower level of encryption. The system allows the doctor to upload the document and then doctor is asked his secret key where the system uses this key along with the doctor and patient information to create a system generated key to encrypt the document.

Data Flow Diagram:

The EHRs to be stored on cloud, a cloud framework needs to be implemented for the proposed system. The framework should provide Platform as a Service (PaaS) so that the whole system is deployed in the cloud itself. Cloud provides with multiple benefits that best suit the system to be implemented like easy sharing, reduces capital costs and provides flexibility. The cloud framework must provide network resources, computing capabilities and a dashboard that helps the users to navigate through the system. The whole system is deployed on the cloud platform where the EHRs can be shared with ease and decrypt it likewise.



SECURE DATA FLOW DIAGRAM

DOI: 10.18535/ijecs/v6i2.09

V. ANALYSIS

Encryption algorithm:

Various algorithms were studied in the process to encrypt the EHRs that are to be stored on cloud. As every encryption algorithm has different encryption and decryption time. The encryption and decryption formula for RSA is given as C= (P^e mod n) and P= (C^d mod n) respectively which follows the polynomial time complexity whereas for attacker it is $^e\sqrt{C}$ mod n which follows modular exponential complexity.

With usual implementations, doubling the RSA key length means that *encryption* will be four times slower, and *decryption* will be eight times slower. RSA encryption is much faster than RSA decryption. The theory says that for a *n*-bit key, computational effort for encryption is proportional to n^2, while effort for decryption is proportional to n^3**.**

Table specifying RSA encryption-decryption time [12]:

Operation	Milli vseconds/ Operation	Megacycles/ Operation
RSA 1024Encryption	0.08	0.14
RSA 1024Decryption	1.46	2.68

RSA Encryption and Decryption Results on different file sizeinputs[9]:

Record no.	Encryption Time (seconds)	Decryption Time (seconds)	Input File Size (KB)
Record no. 1	5.637362	5.637362	15
Record no. 2	11.27472	11.27472	30
Record no. 3	16.91209	16.91209	45
Record no. 4	22.54945	22.54945	60
Record no. 5	28.18681	28.18681	75

RSA Encryption Throughput: 2.660819 KB/Sec

RSA Decryption Throughput: 2.660819 KB/Sec

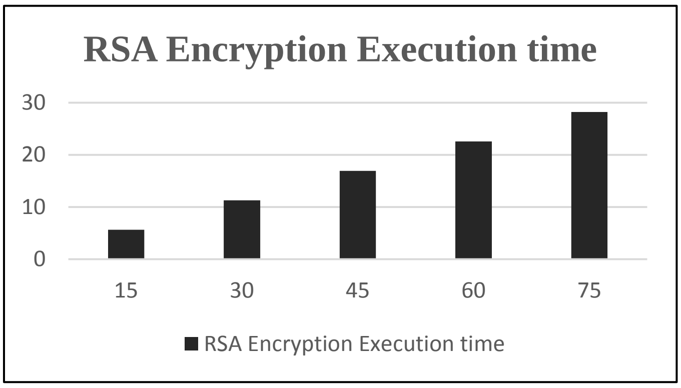


Figure: RSA Encryption Execution Time

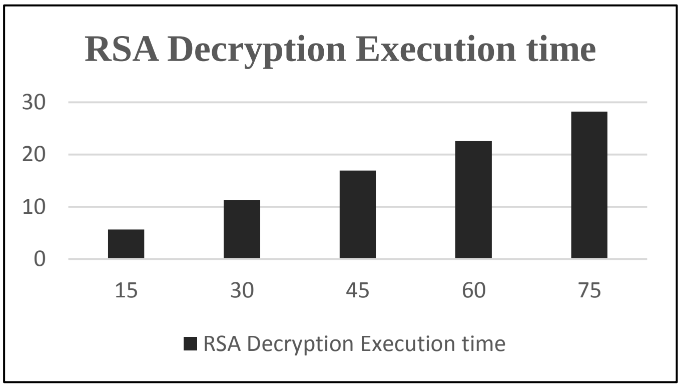


Figure: RSA Decryption Execution Time

Similarly if play-fair attack is used, which is symmetric encryption technique where a brute force attack and frequency analysis is difficult since the size of the key domain is 25! Encipherment using play-fair hides the single-letter frequency of the characters which is helpful when the number of characters to be encrypted is less [8].

AES (Advanced Encryption Standard) algorithm, also known as Rijndael,is a non-Fiestel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12 or 14 rounds. The key size which can be 128, 192, or 256 bits, depends on the number of rounds. Depending on the key size there are three different versions of AES: AES-128, AES-192 and AES-256[7].

Various algorithms are analyzed with their break time that can be used to achieve various levels of security.

DOI: 10.18535/ijecs/v6i2.09

AES Encryption and Decryption Results on different file size inputs [10]:

Sample Record no.	Encryption Time(seconds)	Decryption Time (seconds)	Input File Size (KB)
1	1.6	1	153
2	1.7	1.4	196
3	1.8	1.6	312
4	2.0	1.8	868

AES Encryption Throughput: 215.5321 KB/sec

AES Decryption Throughput: 263.6207 KB/sec

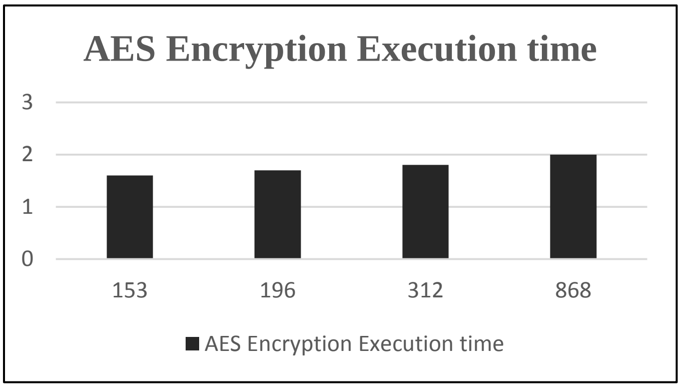


Figure: AES Encryption Execution Time.

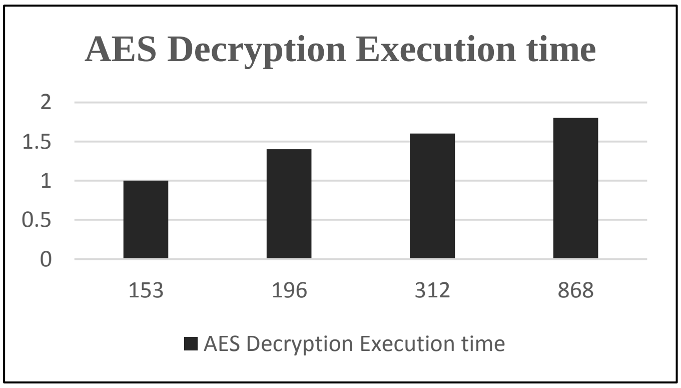


Figure: AES Decryption Execution Time.

Integrity algorithm:

When integrity algorithms are used such as SHA-1 for creating hashed digest where SHA-1 has larger states i.e. 160 bits and 80 rounds. SHA-1 rounds have an extra bit rotation which makes it much stronger against collision attacks. SHA-1 has extra bit rotation hence there is more confusion than the previous version. It is one-way transformation. SHA-1 hashing function is used for integrity of the data that is to be sent. Any change in the data with very high probability change the hash value and thus the receiver would know that the data has been changed.

Table 3.3.1.b: Characteristics of Secure Hash Algorithms (SHAs)[8]:

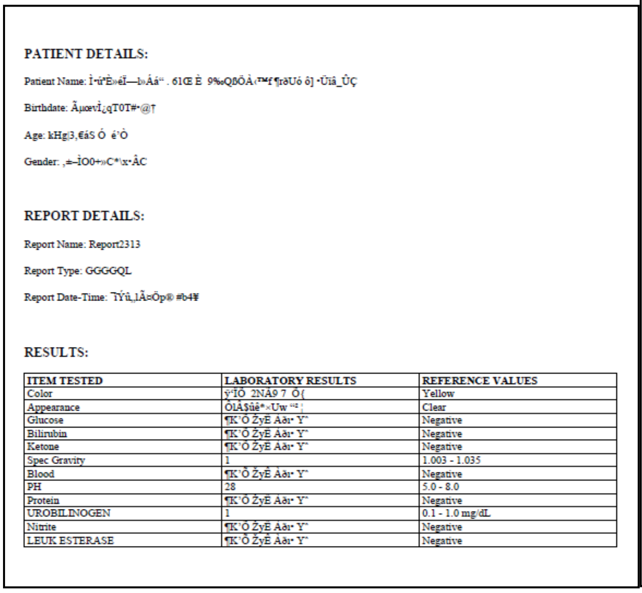
Characteristics	SHA-I	SHA-224	SHA-256	SHA-384	SHA-512
Maximum message size	2^{64} - 1	2^{64}– 1	2^{64} - 1	2^{64} - 1	2^{64} - 1
Block size	512	512	512	1024	1024
Message digest size	160	224	256	384	512
Number of rounds	80	64	64	80	80
Word size	32	32	32	64	64

The MD5, a cryptographic hash function i.e., a message digest algorithm which is widely used, produces a 128-bit (16-byte) hash value, typically is a 32 digit hexadecimal number 64 rounds expressed in text format[10].

Table specifying the hashing time for the following algorithms[12]:

ALGORITHM	MiB/ Second	Cycles Per Byte
SHA - 1	153	11.4
SHA-256	111	15.8
SHA-512	99	17.7
MD5	255	6.8

DOI: 10.18535/ijecs/v6i2.09



PATIENT DETAILS:

Patient Name: Ì•ú'È»éÏ—b»Áá" . 61Œ È 9‰QßÖÀ‹™f ¶rðUó ô] •Üîâ_ÛÇ

Birthdate: ÃµœvÌ¿qT0T#•@†

Age: kHg|3,€áS Ó é'Ò

Gender: ,±–ÌO0+»C*\x•ÂC

REPORT DETAILS:

Report Name: Report2313

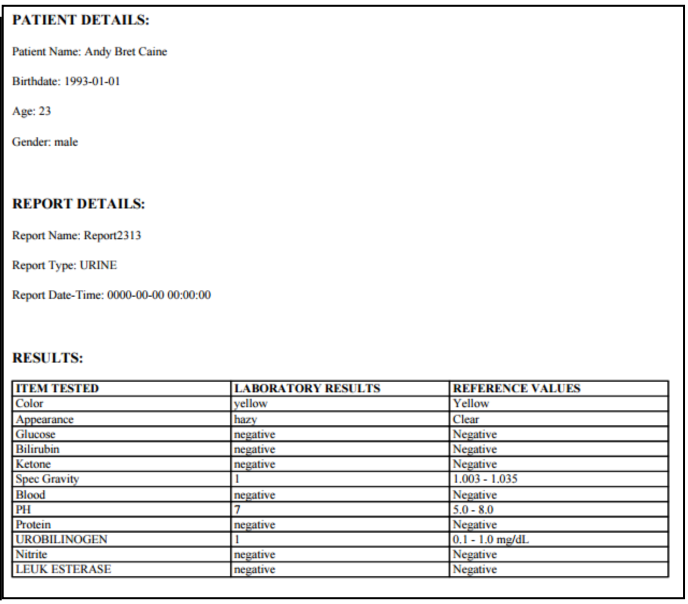
Report Type: GGGGQL

Report Date-Time: ¯ìÝû„lÃ¤Öp® #b4¥

RESULTS:

ITEM TESTED	LABORATORY RESULTS	REFERENCE VALUES
Color	ý'ÏÖ 2NÄ9 7 Ô{	Yellow
Appearance	ÒlÂ$ûê*×Uw "² ¦	Clear
Glucose	¶K'Ö ŻyĒ Àðı• Y˜	Negative
Bilirubin	¶K'Ö ŻyĒ Àðı• Y˜	Negative
Ketone	¶K'Ö ŻyĒ Àðı• Y˜	Negative
Spec Gravity	1	1.003 - 1.035
Blood	¶K'Ö ŻyĒ Àðı• Y˜	Negative
PH	28	5.0 - 8.0
Protein	¶K'Ö ŻyĒ Àðı• Y˜	Negative
UROBILINOGEN	1	0.1 - 1.0 mg/dL
Nitrite	¶K'Ö ŻyĒ Àðı• Y˜	Negative
LEUK ESTERASE	¶K'Ö ŻyĒ Àðı• Y˜	Negative

Figure: Encrypted document sample



PATIENT DETAILS:

Patient Name: Andy Bret Caine

Birthdate: 1993-01-01

Age: 23

Gender: male

REPORT DETAILS:

Report Name: Report2313

Report Type: URINE

Report Date-Time: 0000-00-00 00:00:00

RESULTS:

ITEM TESTED	LABORATORY RESULTS	REFERENCE VALUES
Color	yellow	Yellow
Appearance	hazy	Clear
Glucose	negative	Negative
Bilirubin	negative	Negative
Ketone	negative	Negative
Spec Gravity	1	1.003 - 1.035
Blood	negative	Negative
PH	7	5.0 - 8.0
Protein	negative	Negative
UROBILINOGEN	1	0.1 - 1.0 mg/dL
Nitrite	negative	Negative
LEUK ESTERASE	negative	Negative

Figure: Decrypted document sample

VI. CONCLUSION

EHRs have revolutionized the modern healthcare system and improved the doctor-patient co-ordination. Vulnerability of health records in case of weak security measures. The above system aims at providing a high degree of patient privacy by providing security by classifying information on the basis of their sensitivity levels. The idea is to build a unified system that would accept reports of all the healthcare systems and accordingly provide security. The data in electronic healthcare records is classified based on the level of sensitivity of data contained in it. Attribute based encryption is used to achieve encryption. Various algorithms such as AES, RSA and Play-fair are studied for confidentiality and integrity of data. Integrity algorithms are analyzed based on their performance in terms of Cycles per byte and time. We have implemented the attribute based encryption on the patient's record using PHP and MySQL. Currently we are working on the Integrity algorithms and will deploy our algorithms on cloud.

REFERENCES

[1] Fernández-Alemán, José Luis et al. ,"Security and privacy in electronic health records: A systematic literature review" in Journal of Biomedical Informatics , Volume 46 , Issue 3 , 541 - 562

[2] R. Wu , G.-J. Ahn and H. Hu , "Secure sharing of electronic health records in clouds" , Proc. 8th IEEE Int. Conf. Collaborative Comput., Netw., Appl. Work-sharing , pp.711 -718 , October 2012

[3] JPC Rodrigues J, de la Torre I, Fernández G, López-Coronado M,, "Analysis of the security and privacy requirements of cloud-based electronic health records systems," Journal of medical Internet research, vol. 15, no. 8, 2013.

[4] R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," in Proc of CLOUD '10. IEEE, 2010, pp. 268-275.

[5] Alshehri, S.; Radziszowski, S.P.; Raj, R.K., "Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption," in Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on , pp.143-146, 1-5 April 2012

[6] H. Liu, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing" , IEEE Trans. Parallel and Distributed Systems , vol. 26 , no. 1 , pp.241 -251 , 2015

[7] William Stallings. Cryptography and Network Security Principles and Practices. Prentice Hall, November 16, 2005.

[8] Behrouz A. Forouzan, "Cryptography and network security", 2nd Edition, Tata McGraw-Hill Publications

[9] Sombir Singh, Sunil K Maakar and Dr. Sudesh Kumar, "A Performance Analysis of DES and RSA Cryptography", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 3, May – June 2013.

[10] Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013.

[11] Haeng Kon Kim, Sio-Iong Ao and Mahyar A., "Transactions on Engineering Technologies: Special Issue of the World Congress on Engineering and Computer Science 2013", Springer, 02-Jul-2014.

[12] Wei Dai, https://www.cryptopp.com/benchmarks.html, updated on 31-March-2009.