IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Performance Analysis of Data Encryption Algorithms for Secure EHR Transmission

Shraddha M. Dudhani[1*], Santosh S. Lomte[2]

[1]Dr. D. Y. Institute of Management Research Pimpri, Pune, India
[2]Radhai Mahavidhyalaya, Aurangabad, India

DOI: https://doi.org/10.26438/ijcse/v7i2.363366 | Available online at: www.ijcseonline.org

Accepted: 16/Feb/2019, Published: 28/Feb/2019

Abstract- Hypothetical Data security is the most troublesome issue on the planet and the diverse security risks in the computerized security must be avoided and to give more prominent protection to the customers additionally, to engage high dependability and openness of the data. For the equivalent the assurance of the proper data encryption estimation depends consistently on its key length, data size and its execution criteria. In this paper, we separated the distinctive data encryption figuring for instance, DES, AES, blowfish, MD5 estimations on the reason of the diverse parameters and made a comparison of these counts for secure trade of EHR.

Keyword*: EHR, Performance Analysis, Algorithm*

I. INTRODUCTION

The cryptography plays vital role the cryptography calculation strategy will make the information in the system secure by ad lobbing security to them. It enables just the proposed individual to see the information that is sent. The cryptography is typically said to be the craft of concealing the message by encryption i.e., the change of the message into an unintelligible configuration (encoded text) called the figure content and the transformation of the message from the figure message back to the unique arrangement is known as the decoding. The information before it is unscrambled is known as the plain information and the information comes after it is unscramble is known as the figure content.

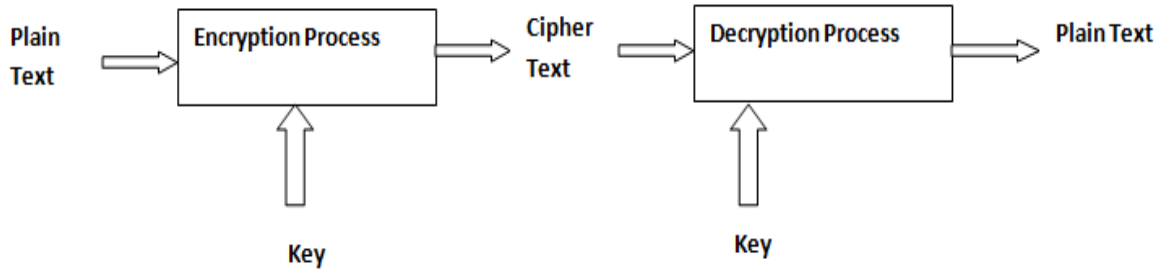

Figure 1: AES encryption algorithm process

Ordinarily the cryptographic calculations gounder the two wide arrangements
• Symmetric encryption calculations
• Asymmetric encryption calculations
The Symmetric calculations utilize a solitary key to perform both the encryption and the unscrambling procedure. This mystery key can be known just to the sender and the recipient, while the Asymmetric encryption calculation or people in general key frameworks utilized two keys to be specific the private key and the open key.. i.e., private key can be known just to the beneficiary furthermore, the general population key can be referred to everybody as it is kept open. The Asymmetric encryption is reasonable in the event of the securityhighlights; however the symmetric encryption is appropriate in the viewpoint of computational techniques. The principle targets of cryptography are to give the clients Privacy, Integrity, Non-disavowal, Authentication, and Access Control. Following are organized of paper which will be advance well ordered.
In section I contain introduction section II contain literature review Section III is about related work section IV contain metrology in section V includes result and discussion In section VI contains result and discussion.

II. LITERATURE REVIEW

1. Health Records Protection in Cloud Environment by Doan B. Hoang, Lingfeng Chen in 2014 IEEE 13th International Symposium on Network Computing and Applications 978-1-4799 5393-6/14. This paper discusses the concept of active electronic health records (or active data cubes) and technologies that ensure the integrity and the welfare of EHRs this paper focus on the protection of EHRs in Cloud environment with the support of the proposed framework.
2. Protection of Electronic Health Records (EHRs) in Cloud by Abdul Atif, Ibrahim Khalil, Vu Mai School of Computer Science and Information Technology RMIT university 35th Annual International Conference of the IEEE EMBS Osaka, Japan, 3 - 7 July, 2013
   This paper discussed about the protection of electronic health record in cloud designing an access control model for encrypted EHRs in the cloud relies mainly on various aspects, including the encryption scheme, the key management mechanism of encrypted EHRs and the natural flow of communication between the different participants.
3. Secret Sharing for Health Data in Multiprovider Clouds by Tatiana Ermakova, Benjamin Fabian by 2013 IEEE International Conference on Business Informatics 978-0-7695-5072 This paper proposed a novel architecture for sharing electronic health records in a multi-cloud environment, i.e., where data is not only stored at a single CP, but at several independent providers in parallel.
4. Secure Sharing of Electronic Health Records in Clouds Ruoyu Wul, Gail-Joon Ahnl, Hongxi**n**Hu2 8th International Conference on Collaborative Computing: Networking, Applications and Work sharing, Collaboration 2012 Pittsburgh, PA, United States, October 14-17, 2012. In this paper, we focus on access control issues in electronic medical record systems in clouds. They proposed a systematic access control mechanism to support selective sharing
5. Secure Key for Authentication and Secret Sharing in Cloud Computing by Dr. Santosh Lomte, Shraddha Dudhani International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 6, June 2015 ISSN: 2277 128X. In this paper the security provided to the cloud with the help of Kerberos it is authentication protocol it works on four parties.

III. RELATED WORK

A. AES (Advanced Encryption Standard)

In 1997 the NIST endeavors to build up a calculation to defeat every one of the lacks of both the DES and. AES (Propelled Encryption standard) is produced by Vincent Rijmen, Joan Daeman in 2001. The AES is the symmetric encryption calculation that has three square figures to be specific AES-128, AES-192 and AES-256. Each figure content of 128- bits are forms utilizing the keys of 128 bits, 192 bits and 256 bits separately. The 10 rounds are improved the situation 128-piece keys and 12 rounds for 192-piece key and 14 rounds for 256-piece keys are present. Every single round in the AES are indistinguishable but the last round. Every encryption round are handled to finish each round till n. Each round has four rounds for example Substitute byte, Shift lines, Mix Column and Add round key.

In AES encryption process, it utilizes distinctive round Keys called the state exhibit of keys.i.e.The keys are handled to perform numerical tasks alongside the array of keys. The information accessible in the AES squares are of specific estimate. This encryption procedure incorporates following procedure:

1. First determine the distinctive round keys from figure key.
2. Introduce the state cluster with square information or plaintext.
3. Begin with starting state cluster by including round key.
4. Play out the procedure of state control in nine rounds.
5. After tenth round of control, we will get the last yield as figure content.

B. MD5 (Message Digest 5):

The Message Digest5 (MD5) was created by Ronald Rivest in 1992 by taking the square sizes as 512 pieces and the summary size as 128 pieces. The hash work delivering the 128 bit hash esteem. The MD5 can be utilized as the best answer for force the savage power assault to act against the broad vulnerabilities and to give unnecessary security.

IV. METHODOLOGY

EHR which is created by doctor is in plain text which is converted into encrypted format then apply MD5 algorithm and convert data into hash values and stored it .in this the two level security we are applying so that data(EHR) is more secure for this purpose we are implemented all encryption algorithm in JAVA using crypto tool .

V. RESULT AND DISCUSSION

As in above section described methodology that how to implement encryption algorithm .in this section we calculate performance analysis and comparative analysis of all encryption algorithm To remove any outlier each EHR file of different size run 1000 time on crypto tool and calculate the average time (which is in millisecond) for each encryption algorithm . In graph (figure 2) it is clearly motioned that AES required less time than all algorithm.

Table 1: Time Required For Encryption Algorithm for Encryption

File Size	AES	DES	BLOWFISH
1MB	128.4	257.2	78.6
10MB	581.4	2339	480
30MB	1489.2	7877.2	1879.2
50MB	4231.2	9012.76	4601.21

Table2: Time Required For Encryption Algorithm for Encryption

File Size	AES	DES	BLOWFISH
1MB	81.6	272.6	100.2
10MB	570.8	1936.6	647.8
30MB	1539	7934.2	2712.2
50MB	4313.11	9096.54	8045.65

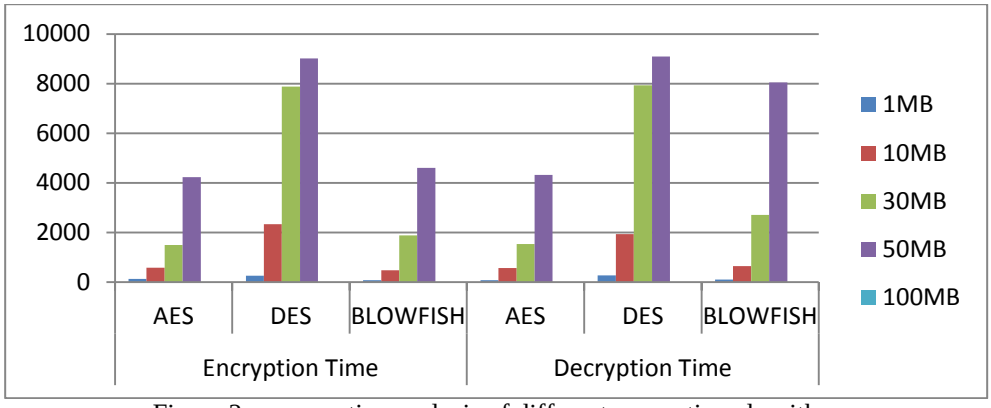

Figure 2: comparative analysis of different encryption algorithm

Figure 2 speaks to the different information encryption calculations and its related execution criteria to demonstrate that the different calculation isn't effective insufficient to sent the secret encryption messages. The AES calculation is considered among the best secure and proficient calculation in the previously mentioned all calculations yet the AES is restricted to the specific key size and can't stretched out over the dimension what's more, it is important to acknowledge the encryption calculation that is ended up being exceptionally secure and furthermore it has higher key size is worthy. In this way, we need to trust that the AES is goes about as an effective calculation in the information encryption standard and it is actualized in the following period of the venture.

VI. CONCLUSION AND FUTURE DISCUSSIONS

Form the above discussions it is proved that the AES algorithm is considered to be the most promising solution to every one of the information vulnerabilities present in the framework and goes about as a very trading off information encryption standard for the information present in the system. By adding the higher square size to the Framework we can probably build the security and the uprightness of the framework.

In future we can use AES for encryption of EHR but for more security further generated key will be again encrypted and convert in to hash value so that will overcome to key transmission problem on public media.

REFERENCES

[1]. Dac-Nhuong Le, Bijeta Seth "A Hybrid Approach of Secret Sharing with Fragmentation and Encryption in Cloud Environment for Securing Outsourced Medical Database: A Revolutionary Approach", Journal of Cyber Security and Mobility, Vol. 7 4, pp.379–408, October 2018.

[2]. Pradeep Deshmukh "Design of cloud security in the EHR for Indian healthcare services Journal of King Saud University Computer and Information Sciences" Production and hosting by Elsevier B.V. This is an open access article 2017.

[3]. RizwanaShaikh ,Jagrutee Banda , Pragna Bandi "Securing E-healthcare records on Cloud Using Relevant data classification and Encryption", International Journal Of Engineering And Computer Science, Volume 6 Issue 'ISSN: 2319-7242, 2017.

[4]. Pooja Sagathia, Saylee Salgaonkar, Akshata Sawant, Hammad Shaikh "Secure Data Sharing in Cloud", International Journal of Scientific & Engineering Research', Volume 8, Issue 2, February 2017

[5]. Gupta, P, Koushal, V, Narayan, C., and Anand,'A. "Building Genetic Database at Medical Institutes", Implement Patient Cost Audit and Improve Biomedical Research. Annals of neurosciences, 24(1), pp.3–4, 2017.

[6]. Jain, A., and Soni, B. K., "Secure Modern Healthcare System Based on Internet of Things and Secret Sharing of IoT Healthcare Data", International Journal of Advanced Networking and Applications, Vol 8(6), pp 3283, 2017.

[7]. Amandeeep Kaur, Er. Anupama Kaur, **"**Asymmetric Key Cryptography Based Technique to Detect and Isolate a zombie Attack in Cloud Architecture", International Journal of Advanced Research in Computer Science and Software Engineering' Volume 6, Issue 3, March 2016. ISSN: 2277 128X

[8]. Van, V. N., Long, N. Q., Nguyen, G. N., and Le, D. N "A performance analysis of open stack open-source solution for IAAS cloud computing", Proceedings of the Second International Conference on Computer and Communication Technologies, pp. 141–150 2016.

[9]. D. AsirAntontony Gnana Singh , R.Priyadharshini, "Performance Analysis of Data Encryption Algorithms for Secure Data Transmission", International Journal for Science and Advance Research in Technology, Volume 2 Issue 12–ISSN [ONLINE]: 2395-1052, December 2016.

[10]. Sareen, S., Sood, S. K., and Gupta, S. K. "Towards the design of a secure data outsourcing using fragmentation and secret sharing scheme", Information Security Journal: A Global Perspective, Vol 25(1–3), pp.39–53, 2016.

[11]. Niraj Bachhav, Swapnil Biradar, Mayank Mishra, Priti Purbey, Monali P. Deshmukh, "A Construction for Secret Sharing Scheme with General Access Structure", International Journal of Innovative Research in Science, Engineering and Technology', Vol. 5, Issue 5, May 2016

[12]. Vijaya Pinjarkar, Neeraj Raja, Krunal Jha, AnkeetDalvi, "Single Cloud Security Enhancement using key Sharing Algorithm", Recent and Innovation Trends in Computing and Communication, 2016.

[13]. Pundkar, S. N. and Shekokar, N, "Cloud computing security in multi-clouds using Shamir's secret sharing scheme", International Conference on Electrical, Electronics, and Optimization Techniques'(ICEEOT), pp. 392–395, 2016

[14]. Hossain, M. A., Hossain, M. B., Uddin, M. S., and Imtiaz, S. M, "Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research, Computer Science and Software Engineering, 2016.

