International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Big Data Security Analytics in Clinical Data using Cryptographic Algorithms

Steena Gracious, Geethu Nandanan, Dagma K. R, Hari Narayana AG

Abstract**: *With increasing apprehension and concerns of cloud computing and information security, awareness about the use of security algorithms in data systems and processes is indispensable. The objective of this paper is to examine a set of cryptographic algorithms for cloud platforms to secure clinical data. The main benefits of cloud storage are scalability, resilience, cost efficiency, high reliability and easy access to your knowledge anyplace, anytime. Because of these benefits every organization is moving its data to the cloud. So there is a necessity to protect that data against unauthorized access, modification or denial of access etc. we analyzed the use of cryptography in securing clinical data sets using evaluation parameters such as computing memory, encryption time and decryption time.***

Index Terms**: *Cryptography in clinical data, AES, ECC, DES, RSA algorithms.***

I. INTRODUCTION

Cloud Computing can be defined as the ability to utilize and access a pool of computing infrastructure and services built, operated and maintained by a third party via the Internet. Big data enables the processing and management of huge amounts of data. Big data on healthcare has potentially significant to refine results of various patients, foretell outburst of fatal epidemic diseases, gain precious insights, prevent avertable diseases, mitigate healthcare cost and improvise the quality of living. Big data, however, how helpful and important for the development in the field of medical science and crucial for successful establishment of all healthcare consortia, can only be utilized if safety concerns have been resolved. Cryptography is a method which is meant to transform the information and it can be used to provide various requirements concerned to security such as confidentiality, authentication, and integrity of data, authorization and non-repudiation. Mainly it depends on two basic elements: an algorithm (a cryptographic method) and a key. These algorithms will provide cryptographic security to the information in the system, by the means of encryption and the reverse through decryption. These different algorithms might be Symmetric Key Algorithm, also known as secret key algorithm or Asymmetric key algorithm, one with public key. Cryptography is a technique that can be viewed as a way of hoarding and concealing highly confidential or secured data in a cryptic manner so it can be accessed or used only for those intended. It will ensure the successful and secured communication of data in the existence of a combatant and these algorithms will palliate security concerns by using cryptography approaches, authentication and distribution of keys in more secured manner. Consequently, cryptography is the discipline of creating data and messages by transforming the end user data into a format that is cryptic and non-readable and encrypting the data or conglomerating plaintext by collecting end user or plain text data as input and converting it into cipher text or to the encrypted form and then performing the process of decryption which is returning back to the native form. Cryptography is widely used with these abilities to provide the security parameters as follows:

- Data Integrity: it has value only if information is precise or faultless. It guarantees the data correctness and consistency throughout its lifetime, and during its implementation and usage of any information system which stores, processes, or retrieves or recover data this will be an important aspect
- Authentication: It is the process of deciding whether, in fact, something is what is declared or confirms the origin and integrity of the content.
- Non Repudiation: It is an attribute which ensures, a team or individual cannot refuse the authenticity of sending a message that was originated from them.
- Confidentiality: It can be linked to the lost privacy, or unapproved access to information and theft of identity.

II. METHODS USED IN PROPOSED SYSTEM

The primary goal of the work is to evaluate the efficiency performance of a set of algorithms in order to determine which is best suited for cloud platforms. A detailed research of the encryption algorithms like RSA, DES, ECC and AES is presented here.

A. *Data Set*

We used a collection of clinical data sets available at https://github.com/search?q=clinical+data ,which includes information about particular diseases .

Revised Manuscript Received on 30 July 2019.
* Correspondence Author

Steena Gracious*, Computer Science and IT, AmritaVishwaVidyapeetham/ Amrita School of Arts and Scineces Kochi, Ernakulam, India.

.**Geethu Nandanan**, , Computer Science and IT, AmritaVishwaVidyapeetham/ Amrita School of Arts and Scineces Kochi, Ernakulam, India.

Dagma K R, , Computer Science and IT, AmritaVishwaVidyapeetham/ Amrita School of Arts and Scineces Kochi, Ernakulam, India.

Hari Narayanan A G, Computer Science and IT, AmritaVishwaVidyapeetham/ Amrita School of Arts and Scineces Kochi, Ernakulam, India.

B. *Encryption Algorithms*

We have chosen four algorithms for evaluation based on the comprehensive study and analysis in terms of performance measures. We briefly explained each of the selected algorithms as follows.

RSA

Ron Rivest, Adi Shamir, and Leonard Adleman developed RSA, a public key system in 1978. RSA is a public key algorithm and it is divided into key generation, encryption, decryption used in computers to encrypt and decrypt data. In key generation first take two large prime numbers p_1 and q_1 then find n_1=p_1*q_1.find m_1 =Φ(n)=(p_1 -1)*(q_1-1).Then select a small number e_1 ;GCDΦ(n_1),e_1)=1;1<e_1< Φ(n_1).find d: de mod Φ(n_1)=1 then give e_1 and n_1 as public key and d_1 and m_1 as secret key. In encryption process, c= $(m_1)^{e}$ mod n_1 .in decryption process, m_1 =c^d mod n_1

Elliptic Curve Cryptography (ECC)

ECC algorithm uses very small keys, signatures and cipher texts. They also support fast key generation.ECC has fast encryption and decryption of data. It uses three schemes such as Diffie Hellman scheme, Elliptic Curve Integrated Encryption and the digital signature algorithm. The public key cryptography is the basis of Diffie Hellman scheme and Elliptic Curve Integrated Encryption is based on encryption and key generation, it was done in a single step. For computation process it uses less memory.

Advanced Encryption Standard (AES)

AES is mainly applied in encryption of sensitive data and which is using a 128-bit block size for both encryption as well as decryption of data. It is a block cipher that uses 128, 192, or 256-bits key size. although algorithms like Rijndael and AES are often mutually used, there exists many dissimilarities between these two in terms of both block and key sizes used.

Data Encryption Standard (DES)

DES is one of the globally accepted cryptographic systems that is currently available today. A 56-bit key is required to encrypt data with block size 64 bit. There occurs a processing of 64-bit inputs into 64-bit cipher-text and 16 iterations are performed by algorithm.

III. RELATED WORK

Earlier research in this area is focused on addressing the security issues of data on various platforms using both symmetric and asymmetric algorithms. They also analyzed a group of cryptographic algorithms with respect to different parameters like time, memory used, key exchanges and flexibility. Jorge E. Camargo, Diego F. Sierra and Yeison Torres proposed a work on Study of Cryptographic Algorithms to Protect Electronic Medical Records in Mobile Platforms [1]. The paper analyses a number of cryptographic algorithms for the protection of medical records in mobile applications. The results of the study indicate that health and patient records are secured sufficiently with good performance and computer resources in context of mobile platforms. Cryptographic security is essentially defined as to how secure the algorithm is against various attacks. The performance and efficiency of these cryptographic algorithms depend on their structure, length of the key, block size, number of rounds and required time. Conclusively all these factors influence the safety of a particular algorithm [2]. There are a number of papers available to discuss the performance evaluation of certain symmetric and asymmetric algorithms. From the computation test results presented, it was concluded that a specific algorithm performs better than other algorithms in different aspects. [3].At first glance, the definition of data may be prosaic; interestingly it was difficult in formulating a definitive and useful definition. Data on healthcare are considered sensitive and highly confidential globally. Classification of less sensitive data may therefore appear to be relatively unimportant for research in this field. There are some papers examine the argument that this is not necessarily the case [9]. The whole world is going wireless and growing fast with electronic resolutions. It is time to remotely control devices such as Smart Cards, PDAs and mobile phones with new and faster cryptosystems. This paper outlines the key concepts of public key crypto algorithms RSA, ECC and Goldwasser- Micali for a comparative research and performance analysis of various encryption in these cryptosystems [5]. Big data offers numerous opportunities to conduct health research, discovery of knowledge. They have been discussed several examples of related successful works throughout the globe. Issues regarding Privacy and securities are also presented in every single phase of the Big Data Life Cycle, across with their merits and demerits of current privacy and security policies with respect to the Big Health Data Industry [8]. The security issues in Big Data Platforms can be classified into various levels, namely authentication, data level, network level and general problems. Different methods such as data encryption, network encryption, logging, node maintenance and encryption technique algorithms were discussed [10]. With increased awareness and concern about cloud computing and information security, the need for understanding in the use of security algorithms in data systems is increasing. [4]. In the paper ‘Security Algorithms for Cloud Computing’ Akashdeep Bhardwaja, GVB Subrahmanyamb, Vinay Avathic, Hanumat provide a comprehensive inspection about Symmetric and Asymmetric algorithms focusing on a set of Symmetric Algorithms in the account of significance for security in cloud platforms for cloud- based applications and for the various services in cloud. Basically big data has brought drastic changes in the way organizations functions, governs, and utilize the data in any industries [7]. The Wireless Body Area Network is segment of the Wireless Sensor Network, it can transmit medical data in a run- time environment and works with medical devices.

for Healthcare devices. Due to these constraints, the implementation of high levels of safety is an intimidating task. The proposed work implements Elliptic Curve Cryptography (ECC) for key secure distribution and data transfer [6].

IV. PROPOSED WORK

We are intending to do a work that will evaluate a set of cryptographic algorithms to secure clinical data in cloud platforms.

The proposed schema implements Elliptic curve cryptography (ECC), RSA, AES, DES for securing clinical data. we analyzed these algorithms on clinical data sets with certain performance measures.

A. *Performance Measures*

Computing Memory

Main memory used to encrypt a set of clinical data sets with each encryption algorithm in kilobytes.

Encryption Time

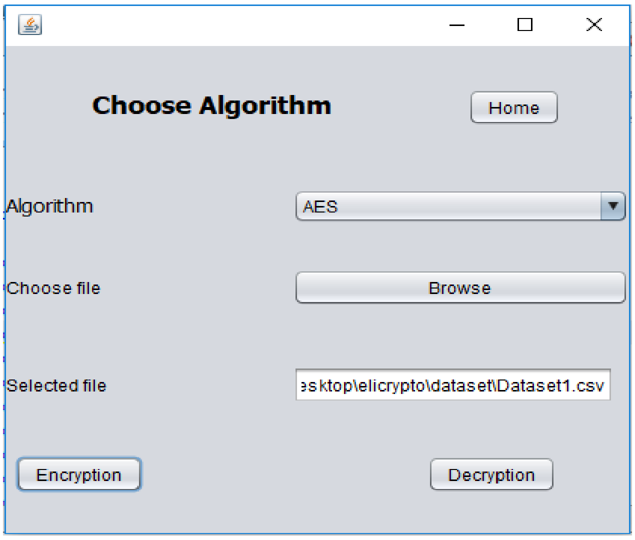
Time required encrypting a set of clinical data using each encryption algorithm in seconds

Decryption Time

Time required decrypting a set of clinical data using each encryption algorithm in seconds.

B. *Performance Evaluation*

The actions stated below were performed as input using each selected algorithm to encrypt the data (.csv file) to determine the time and memory needed for encrypting the file, and to decrypt it.



Choose Algorithm

Algorithm: AES

Choose file

Selected file: esktop\elicrypto\dataset\Dataset1.csv

Figure 1: encrypting a .csv file

The input parameters are

- File upload: C:\Users\HP\Desktop\dataset\Dataset1.csv
- Choosing algorithm:
- Mode: Encrypt or Decrypt

C. *Experimental Results*

Here we present the acquired results from the experiments conducted for each of the defined performance measures. The results from experimental work are illustrated below using file of various sizes as input and recording the computation time and memory used for those algorithms.

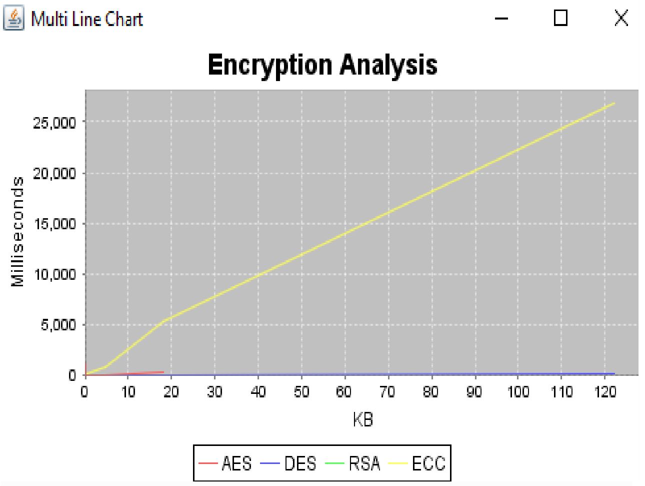


Figure 2: depicts the computation time and memory the algorithms used to encrypt the clinical data sets

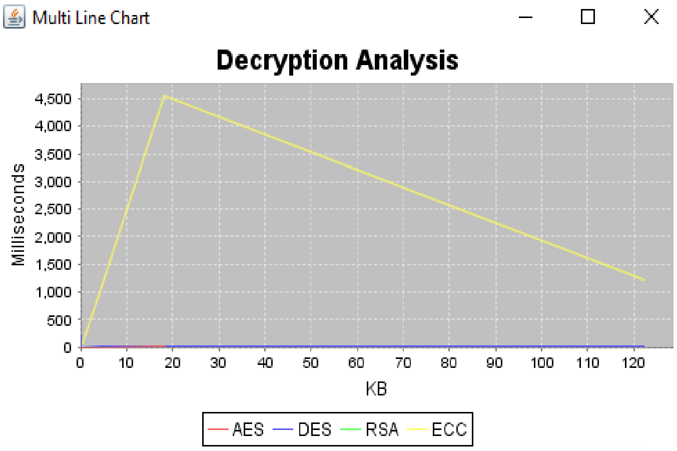


Figure 3: depicts the computation time and memory used for algorithms to decrypt the clinical data file

V. CONCLUSION

There are countless potential and unlimited opportunities for Big Data in the field of healthcare industry. There exist several drawbacks, including technical issues, security and trust issues, that delay its true potential. Big data security is considered as a huge complication for researchers in this field and it should be addressed. In this paper we presented an evaluation of the performance of different symmetrical and asymmetrical encryption algorithms such as AES, DES, ECC and RSA. This analysis is based on performance measures like computing memory and time used for encryption and decryption. From the conducted experiments, we came into a conclusion that DES was the most efficient in terms of encryption- decryption time than other algorithms.

A proposed direction could be to carry out the same experiments and implement them in the cloud platform for the future

REFERENCES

1. Jorge E. Camargo*, Diego F. Sierra and Yeison F. Torres: Study of Cryptographic Algorithms to Protect Electronic Medical Records in Mobile Platforms Indian Journal of Science and Technology, Vol 8(21), DOI: 10.17485/ijst/2015/v8i21/60739, September 2015

2. Zoran Hercigonja Druga gimnazija Varaždin, Croatia: Comparative Analysis of Cryptographic Algorithms International Journal of DIGITAL TECHNOLOGY & ECONOMY
3. Madhumita Panda: Performance Analysis of Encryption Algorithms for Security International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016
4. Akashdeep Bhardwaja*, GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastryd: Security Algorithms for Cloud Computing International Conference on Computational Modeling and Security (CMS 2016)
5. Gururaja.H. S1, M. Seetha2, Anjan K Koundinya3, Shashank.A.M4 and Prashanth.C. A5: Comparative Study and Performance Analysis of Encryption in RSA, ECC and GoldwasserMicali Cryptosystems ISSN 2319 - 4847, 2014
6. Shashi Kant Shankar, Anurag Singh Tomar, Gaurav Kumar Tak*: Secure Medical Data Transmission by using ECC with Mutual Authentication in WSNs
7. Karim Abouelmehdi*, Abderrahim Beni-Hessane and Hayat Khaloufi : Big healthcare data: preserving security and privacy, Abouelmehdi et al. J Big Data (2018)
8. .Karim ABOUELMEHDIa 1, Abderrahim BENI-HSSANEa, Hayat KHALOUFIa, Mostafa SAADIb : Big data security and privacy in healthcare: A Review
9. Dimas Natanaela,Faisala,Dewi Suryanib : Text Encryption in Android ChatApplications using Elliptical Curve Cryptography(ECC), 3rd International Conference on Computer Science and Computational Intelligence 2018.
10. K. Kalaiselvi ,Anand Kumar, Ph.D : Implementation Issues and Analysis of Cryptographic Algorithms based on different Security Parameters , International Conference on Current Trends in Advanced Computing (ICCTAC-2015)

AUTHORS PROFILE

Steena Gracious MCA Scholr at Amrita Vishwa Vidyapeetham University, Amrita School of Arts & Sciences, Kochi, Kerala, India.

Geethu Nandanan MCA Scholr at Amrita Vishwa Vidyapeetham University ,Amrita School Of Arts & Sciences,Kochi,Kerala,India.,

Dagma K R MCA Scholr at Amrita Vishwa Vidyapeetham University ,Amrita School Of Arts & Sciences,Kochi,Kerala,India..

Hari Narayanan A G Assistant Professor at Amrita VishwaVidyapeetham University, Amrita School of Arts & Sciences, Kochi, Kerala, India.