COMPARATIVE STUDY OF DATA SECURITY IN CRYPTOGRAPHY ALGORITHMS USING CLOUD ENVIRONMENT

Leelavathi .M, Josephine. P
Assistant professor, Department of Computer Science,
Padmavani Arts and Science College for Women, Salem.India

Abstract:

Cloud Computing is a web based application. There are many Challenges faced by the data owner in outsourcing the data because the data can be changed or damaged when it is stored in third party Cloud. Several Cloud service provider gives the some short of secure services to client data but they are paid services and do not give the guarantee of data security from unauthorized access. Cryptography plays an important task in accomplishing information security in cloud Environment in data encryption is the key role in current and future technologies. In recent years in order to avoid this problem some Cryptographic algorithm on different data to provide most secure and efficient algorithm. These algorithms perform encryption and decryption operation on data at client machine before storing data into the cloud. The Cryptographic keys like public, private are to be used to give secure system.The purpose of this research is to analyze and compare theperformance of selected algorithms namely: AES, ECC, DH, and RSA.These four cryptography algorithms are compared based on the parameters namely, Memory Usage, Encryption Length, and Encryption Time.

Keywords: Cloud computing, Cryptography, Security algorithms, Performance Analysis.

1. INTRODUCTION:

Cloud Computing is made up by aggregating two terms in the field of technology. First term is Cloud and the second term is computing. Cloud is a pool of heterogeneous resources. It is a mesh of huge infrastructure and has no relevance with its name “Cloud”.Cloud Computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. Cloud Computing is the key driving force in many small, medium and large sized companies and as many cloud users seeks the services of Cloud Computing, the major concern is the security of their data in the Cloud.

Securing data is always of vital importance, because of the critical nature of Cloud Computing and the large amounts of complex data it carries, the need is even more important. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of Cloud Computing services. To be effective, cloud data security depends on more than simply applying appropriate data

security procedures and countermeasures. Computer based security measures mostly capitalizes on user authorization and authentication.

1.1 CRYPTOGRAPHY

Cryptography can help emergent acceptance of Cloud Computing by more security concerned companies. The first level of security where cryptography can help Cloud Computing is secure storage. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms. Now a day's cryptography is considered as a combination of three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric- key algorithms, and Hashing.

In Cloud Computing, the main problems are related to data security, backups, network traffic, file system, and security of host, and cryptography can resolve these issues to some extents. Consider an example, in the cloud consumer can protect its confidential data, then he has to encrypt his information before storing in the cloud storage, and it is advised not to save an encryption key on the same server where you have stored your encrypted data. Cryptography [2] is based on fundamental terms which areconfidentiality, integrity and availability.

1.2 SECURITY OF CLOUD COMPUTING

Since Cloud Computing is utility available on internet, so various issues like user privacy, data theft and leakage and unauthenticated accesses are raised, Cryptography is the science of securely transmitting and retrieving information using an insecure channel it involves two processes:

1.2.1 Encryption

Encryption is a process in which sender converts data in form of an unintelligible string or cipher text for transmission, so that an eavesdropper could not know about the sent data.

1.2.2 Decryption

Decryption is just the reverse of encryption. The receiver transforms sender's cipher text into a meaningful text known as plaintext. It has two kinds of key which are thepublic key and the private key. There are also two kinds ofencryption; these are symmetric encryption which utilizes asimilar key in encryption and decryption. The other one isasymmetric encryption which utilizes diverse key, public keyfor encryption and private key for decryption.

The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user and infecting the entire cloud .This leads to affects many customers who are sharing the infected cloud. There are five types of issues raise while discussing security of a cloud:

- Data Issues
- Privacy issues
- Infected Application

- Security issues
- Trust Issues

This paper analyzes and compares the performance of selected algorithms, namely: AES (Rijndael), ECC,RSA and DH. The rest of the paper is organized as follows: section two discusses the selected security algorithms. Section four explains the methodology used in the study. Section five presents the results and analysis of this research. Finally, the conclusion is drawn in sectionsix.

2.LITERATURE REVIEW

RachnaArora, AnshuParashar[2]:

In this paper describe about Cloud Computing security issues, mechanism, challenges that cloud service provider face during cloud engineering and presented the metaphoric study of various security algorithm.

Mohammed NazehAbdul Wahid,Abdulrahman Ali, BabakEsparham and Mohamed Marwan [11] :

In this paper, we will present the result of the implementation and analysis that applied on several cryptographic algorithms such as DES, 3DES, AES, RSA and blowfish. Also, we will show the comparisons between the previous cryptographic techniques in terms of performances,

ShaffyBansal, Dr. GagandeepJagdev[14]:

In this research paper along with discussing the basics of cloud computing and the threats involved in a cloud environment, the two main algorithms of cryptography, DES(Data Encryption Standard) and AES (Advanced Encryption Standard) has been elaborated with their individual practical implementation detailing the conversion of plain text to cipher text and vice versa.

Ronald S. Cordova, Rolou Lyn R. MaataAlrence S. Haliba, Rula Al-Azawi, Member[12]:

The purpose of this research is to analyze and compare the performance of selected algorithms namely: AES (Rijndael),Blowfish and RSA. The results show that Blowfish manifested a higher time efficiency ratio when subjected to various data loads and memory size as compared to AES and RSA.

Omar G.Abood, ShawkatK.Guirguis[13]:

In this paper, we discuss several important algorithms used for the encryption and decryption of data in all fields, to make a comparative study for most important algorithms in security effectiveness, key size, complexity and time, etc. This research focused on different types of cryptography algorithms that are existing, like AES, DES, TDES, DSA, RSA, ECC, EEEandCR4.etc

3.PROPOSED SYSTEM

In the Proposed System mainly concentrates on user cloud security of Cloud Computing using Cryptography encryption algorithm using particular existing plan.To secure the Cloud means secure the “databases hosted by the Cloud provider”. Security goals of data include three points namely: Confidentiality, Integrity, and Availability (CIA).

Confidentiality of data in the cloud is accomplished by encryption and Decryption process. Cloud security implementation using various cryptographic algorithms. This paper describes the comparison among these algorithms.

- Elliptical Curve Cryptography (ECC)
- Advanced Encryption Standard (AES)
- Diffie Hellman Key Exchange (DH)
- Rivest, Shamir and Adleman (RSA)

These four encryption cryptography algorithms are compared based on the parameters namely, Memory Usage, Encryption Length, and Encryption Time. It can implement software to select the suitable and highest security encryptionalgorithm.The quantitative research in this paper is to do an experiment using graph of the range of algorithms used in data access security in cloud service provider.

4.SECURITY ALGORITHMS

4.1 AES

Advanced Encryption Standard(AES Rijndael) is asymmetric encryption technique and it was created by Joan Daemon and Vincent Rijmen [6]. It is a strong and secureencryption algorithm.AES uses the encrypted symmetric keyor secret key to encrypt and decrypt a message; therefore itis necessary to utilize the same secret key for both the senderand receiver.

4.2RSA

This is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). RSA is basically an asymmetric encryption /decryption algorithm. It is asymmetric in the sense, that here public key distributed to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not shared to everyone.

4.3ECC

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

4.4. Diffie-Hellman Key Exchange Algorithm

Diffie-Hellman Key Exchange In 1976, Whitfield Diffie and Martin Hellman introduced a key exchange protocol with the use of the discrete logarit

hm problem. In this protocol sender and receiver will set up a secret key to their symmetric key system, using an insecure channel.

5. SYSTEM METHODOLOGY

The four most common security algorithms used in cloudcomputing [5] were selected and compared in this paper. Then, simulation was done in order for us to record theperformance of each algorithm. Two computers have beenutilized, both having Intel Dual core 2.5GHZ with 1GB and 80GBRAM, respectively. NetBeans IDE 8.02 was used to run Javaprograms for the algorithms, all the programs are same instructors. AES, ECC, DH and RSA cryptographicalgorithms were implemented using Java programminglanguage on the same programming environment.

6.RESULT AND DISCUSSION

In this paper, the results are analyzed based on the implementation that performed.

i. Figure 1 shows that the DH algorithm records the fastest encryption time, and ECC algorithm records the slowest encryption time. Based on the encryption time we will select the DH technique for further evaluation.

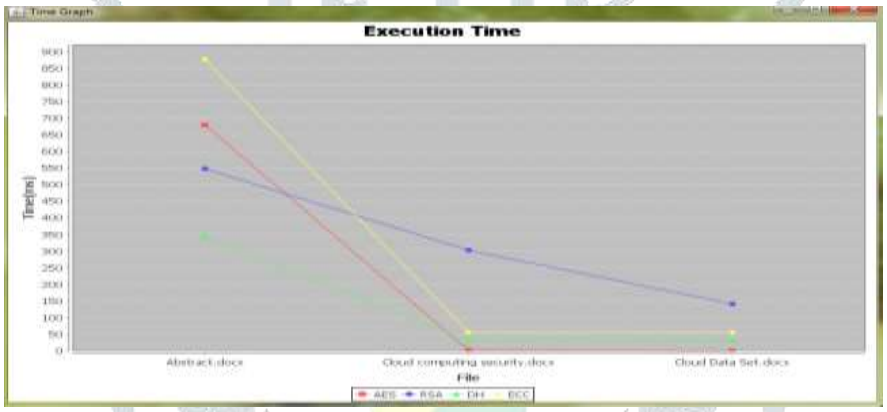

Figure1.EncryptionTime

ii. Up next in the figure 2 presents that memory used for unit operations for all cryptographic techniques that we studied. Blowfish consumed less memory storage than other types,
while RSA uses the highest memory.

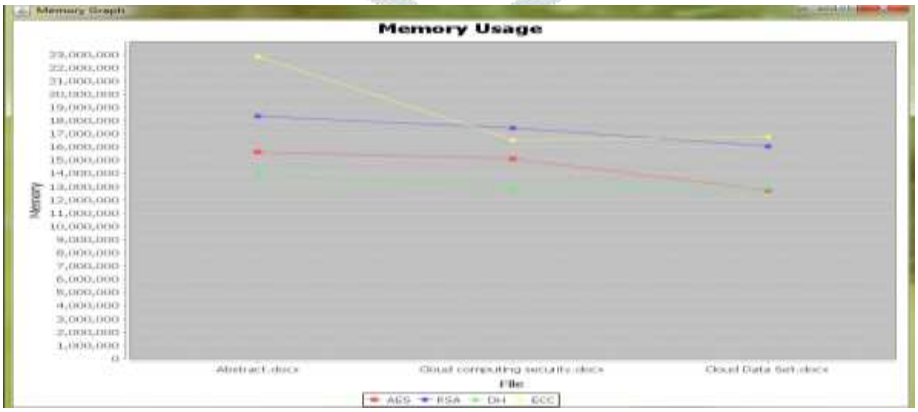

Figure 2.Memory usage

iii. Table 1 presents AES demands the highest number of bits to be encoded optimally, whereas DES demands the lowest number of bits to be encoded optimally.

Table 1.Optimal encoding length

Algorithm	Encryption length
AES	27
RSA	32
ECC	35
DH	15

7. CONCLUSION

This paper is secure service provisioning in cloud using DH. This DH provides normal encryption and extra access control function. DH is more efficient, flexible and suitable than other cryptographic techniques like ECC, RSA, AES, and may be a lightweight security solution for web services. Cloud services are also delivered as web services. Thus, our proposed system intends to implement Diffie Hellman based public security in provisioning cloud services to the users. This approach, confidentiality of service information can be achieved even if control is lost over the service reply during transmission. Simulation for different algorithms will be done on the CloudSim. The results will be obtained on basis Encryption Time, Encryption Length, Memory Usage and Scalability, Execution time performance parameter. All the algorithms are applied on both the cloud network and single system.

8.BIBLIOGRAPHY

1. Joshi, J.B.D., Gail-JoonAhn. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security Privacy Magazine, Volume 8, IEEE Computer Society, 2010, p.24-31.
2. RachnaArora, AnshuParashar "Secure User Data in Cloud Computing Using Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA), Issue 4, Jul-Aug 2013, pp.1922-1926.
3. FarzadSabahi. Cloud Computing Security Threats and Responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.
4. AshishAgarwal, AparnaAgarwal. The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences [VOL I, SPECIAL ISSUE ON CNS, JULY 2011] [ISSN: 2231-4946].
5. Ashutosh Kumar Dubey, Animesh Kumar Dubey, MayankNamdev, Shiv Shakti Shrivastava. Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. Software Engineering (CONSEG), CSI Sixth International Conference, Sept. 2012.
6. M.Venkatesh, M.R.Sumalatha, Mr.C.SelvaKumar. Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing. Recent Trends In Information Technology (ICRTIT), 2012 International Conference, April 2012.
7. PrashantRewagad, YogitaPawar in. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

8. Hai Yan, Zhijie Jerry Shi. Software Implementations of Elliptic Curve Cryptography. Information Technology: New Generations, Third International Conference, April 2006.
9. W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 1976.
10. Ravi Gharshi, Suresha. Enhancing Security in Cloud Storage using ECC Algorithm.International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 7, July 2013.
11. Mohammed Nazeh Abdul Wahid*,Abdulrahman Ali, BabakEsparham and Mohamed Marwan.A Comparison of Cryptographic Algorithms:DES, 3DES, AES, RSA and Blowfish for Guessing Attack prevention.ISSN Online: 2474-9257.july 2018.
12. Ronald S. Cordova, Rolou Lyn R. MaataAlrence S. Haliba, Rula Al-Azawi, Member, IEEE.Comparative Analysis on the Performance of Selected Security Algorithms in Cloud Computing.(ICECTA)2017.
13. Omar G.Abood, Shawkat K. Guirguis [11]:A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018 ISSN 2250-3153

14.ShaffyBansal, Dr. GagandeepJagdev, Comparative Analysis and ImplementationofCryptographic Algorithms in Cloud Computing.International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)Volume 5, Issue 1, 2018, PP 17-25