ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Enhancing File Security using Cryptography Algorithms in Cloud Computing: A Survey

Punam V. Maitri [1], Aruna Verma[2]

ME Student, Dept. of Computer Engineering, DPCOE, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering, DPCOE, Pune, India[2]

ABSTRACT: Now a day cloud computing is used tremendous amount in different field. Large amount of data is generated in daily life. To store this huge amount of data we use cloud computing services. Cloud computing is provides different types of services to the user. While storing the data on cloud there are n number of issues. The main issues of cloud computing are data security, integrity ,authentication and confidentiality .To provide the solution to these security issues different algorithm and techniques has introduced by different researchers but every algorithm and technique having their own merits and demerits. In this paper we have done the survey of different symmetric and asymmetric algorithms. Symmetric algorithms are AES ,DES ,TDES ,IDEA, and RC6 .RSA and ECC algorithm are asymmetric algorithms.

KEYWORDS: Public key ,Secret key, encryption, Decryption, Integrity ,Availability ,Confidentiality ,Blowfish

I. Introduction

Cloud computing storage is used based on user's requirement. User can access that data from cloud any time as well as any place. Now a day's large amount of data is stored on cloud but we don't know about our data is stored on cloud securely or not. To provide the security to data on cloud one of the solution is cryptography algorithms .Cryptography is process in which we can store data securely on cloud and transmit it in unreadable form so only authorized person can access sensitive data. Cryptography is classified into types .That is symmetric algorithm and asymmetric algorithms. Symmetric algorithms are AES, DES, IDEA, TDES, Blowfish and RC6. RSA and ECC are asymmetric algorithms. Symmetric algorithm uses same key for data encryption and decryption that is secret key and asymmetric algorithm uses two keys. Public key is used for data encryption and private key is used for data decryption.

Three level security is achieved with the help of cryptography algorithm. First level security is achieved using digital signature .AES algorithm is used for second level security .Data confidentiality is achieved using AES algorithm and provide the security to AES algorithm key using Diffie Hellman key Exchange algorithm. Data integrity is maintained while downloading the data from cloud using hash algorithm. This three level security mechanism overcome the cloud security issues.[1]

Different combination of cryptography algorithms are used in paper [2]. The new type security model overcome different issues of cloud security i.e. Data security, verification and authentication.RSA algorithm gives high level security to data as well as provides data confidentiality .Secure communication is done using asymmetric algorithm .Encrypted data is stored on cloud so unauthorized person cannot access data from cloud. User authentication is done using MD5 algorithm so only authorized person cal upload the data on cloud. In this proposed system no one can access secure data of user because different cryptography algorithms are run at different places in the cloud models.

Data security is major issue in cloud computing .To overcome this problem different researcher has introduce different cryptography algorithms and technique .Data security is overcome by using TDES algorithm. Diffie Hellman key exchange algorithm is used securely exchange keys through unsure communication channel. For the user authentication purpose signature is used .Signature is in image format. Secure file upload and download is done with the help of cryptography algorithm. This proposed framework provide security to video ,audio ,text and image file .Actual data is stored al local server .Cipher text and metadata of files are stored on cloud server .Disadvantage of this new security architecture is TDES algorithm consumes more time for data encryption and decryption as compare to RSA and DES algorithm.[3]

DOI: 10.15680/IJIRCCE.2015. 0310107

Security is provided for data according to the requirements of client. Cloud computing provides different types of services and deployment model. Every cloud computing model provides the different level of security. In this proposed system security is provided according to the model which is selected by user. In cloud deployment models different combination of algorithms are used to achieve data confidently, integrity and authentication. Data is stored in different deployment model of cloud computing according to the security requirement of the user. [4]

Lightweight cryptography algorithm has introduced by Sana Belguith .Symmetric algorithm gives better performance in terms of speed as compare to asymmetric algorithm and Asymmetric algorithm gives maximum security as compare to symmetric algorithm.AES algorithm is used for data confidentiality .RSA algorithm solves the key distribution problem .This new hybrid cryptography algorithm gives better performance in terms of security as well as increase the speed of data encryption and decryption.[5]

Now a day's large amount of data is stored on cloud. But it's difficult task to provide security to data for life time. To provide solution to this problem RC6 algorithm is introduced .This algorithm is used for provide security to data. This symmetric block cipher algorithm has achieved data confidentiality. Advantage of this proposed system is provide secure data backup facility.[6]

Merkle hash tree technique is used for public auditing .In this technique relative index is used to make it dynamic. For data encryption AES algorithm is used .This algorithms consumes less time for data encryption. Security and data confidentiality issues are avoided using merkel hash tree technique.[7]

In the hybrid algorithm data integrity is done by using MD5 hashing algorithm. Blowfish algorithm is provides data confidentiality facility. Authentication is done using RSA algorithm. In this way hybrid technique achieved different security parameters data confidentiality, authentication and data integrity. The main aim of this hybrid technique is provide high efficiency.[8]

The grid based technique is used to provide more than one level data integrity while downloading the file form cloud server. This technique overcome the authentication and integrity issues of cloud computing. Two level security is provide by using grid based technique. Username and password credentials are used for first level security. Second level security is given using grid based technique. In the grid based technique 3 *3 matrix is generated then insert random values into the grid using random value generation technique. These random values are converted into hash then store at cloud server. [9]

Blowfish is symmetric block cipher algorithm. This algorithm is used for provide security to data. Different cloud computing issues are solved using this algorithm. Sensitive data of user stored on cloud in unreadable format. [10]

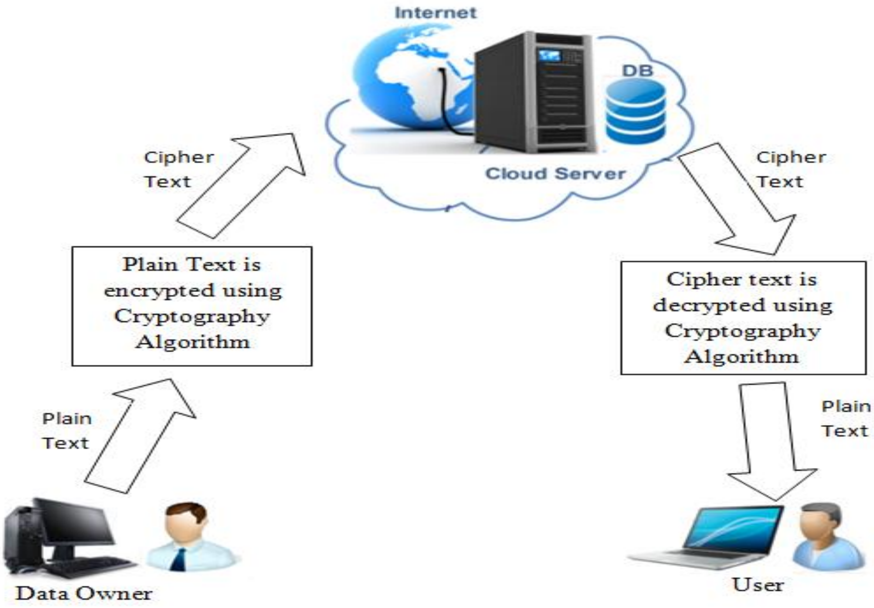
Internet
DB
Cloud Server
Cipher Text
Cipher Text
Plain Text is encrypted using Cryptography Algorithm
Cipher text is decrypted using Cryptography Algorithm
Plain Text
Plain Text
Data Owner
User

Fig 1. Cloud Storage Architecture.

Cloud storage architecture is shown in figure 1. Data owner and data user are shown in figure 1. If data owner wants to share the data on cloud. First data owner covert original plain text into cipher text using different cryptography algorithms. Cipher is uploaded on cloud. So only authorized user can access the sensitive data .If user want to download data from cloud for that user have to specify authentication details. If authentication details are match with database then that user is authorized user.

II. RELATED WORK

The new security model has proposed by Ranjit Kaur.This new security model provides security according to the cryptography technique and algorithm. Cryptography algorithms are used in different model of cloud computing based on requirements of different parameters like confidentiality, privacy, security and authentication .For authentication purpose unique token generation technique is used in private cloud. The speed of data encryption and decryption is increased in public cloud. Two level security is provided in hybrid cloud. In this proposed model two steps are followed .First one is data storage and second is data retrieval. In this security model user can select different section of cloud to store the data.AES symmetric algorithm is used in private cloud for data encryption and decryption. In public cloud blowfish algorithm is used for data security.SHA -1 algorithm is used in private cloud and public cloud for data integrity. Hybrid cloud provides two level security.AES, Blowfish and IDEA algorithms are used in first level security .Second level security is achieved using blowfish and IDEA algorithm. Using proposed security model author has achieved high security, availability, privacy, authentication, integrity, confidentiality and non-repudiation [4]
Author has introduced Lightweight cryptography algorithm in this paper. In this proposed system symmetric and asymmetric algorithms are used. In asymmetric algorithm two keys are used private key and public key. Key distribution problem is solved by using RSA algorithm. Symmetric algorithm is used for providing security to data and asymmetric algorithm is used for provide security to AES key. Data confidentiality is achieved using AES algorithm. Asymmetric algorithm gives high level security. AES algorithm require minimum time for data encryption and decryption .RSA algorithm require maximum time for data encryption and decryption but RSA algorithm is more secure than AES algorithm[5]
Secure data backup mechanism is implemented by Pravin Kulurkar. The main goals are data provide secure data backup and achieve high level security to the data while stored into cloud. If any file is corrupted or deleted by mistake form cloud server. Easily that file can recovered by using this proposed system.RC6 algorithm is symmetric block cipher algorithm .This algorithm supports three types of keys 128 bit,192 bit and 256 bit. Advantages of this proposed system are requiring minimum memory space and minimum time for data encryption and decryption. User requires keys to download the data from cloud. So only authorized person can download the data form cloud.[6]

III. PERFORMANCE REVIEW

Performance evaluation is done for different symmetric and asymmetric algorithms. These cryptography algorithms achieved different security parameters. In this paper we have done analysis of different algorithms and technique .Every algorithm and techniques are achieved different quality of service parameters.

RP. No.	Algorithms and Techniques	Advantages	Disadvantages
1.	Digital signature ,AES and Diffie Hellman Key Exchange Algorithm	1. Integrity 2. Confidentiality 3 Authentication	1.less Efficiency
2.	RSA ,Digital signature and MD5	1.Data security 2 Data integrity 3Authentication	1.Consumes maximum time
3.	Diffie Hellman key Exchange and TDES	1.Confidentiallity 2.Authentication	1. Week key 2. Time consuming

4.	Blowfish, AES ,IDEA and SHA1	1. Better Security 2.Confidentiality 3.Non-repudiation 4.Availabilty 5Privacy 6.Integrity	1.Less secure as compare to asymmetric algorithms 2.Key distribution problem
5.	AES and RSA	1. High speed 2.High system performance 3.Secuirty	1. RSA is more time consuming
6.	RC6	1. Less Memory space 2.Fast Encryption 3.Data recovery	1. Less Secure
7	Dynamic Merkle Hash tree and AES	1.Better security 2.Data confidentiality	1.Less secure as compare to RSA algorithm
8	RSA ,MD5 and Blowfish	1.Authentication 2.Intgrity 3.Data confidentiality	1.In Blowfish algorithm static key is used every time
9	SHA-1 and Grid based technique	1.Multilevel integrity 2.Confidentility 3.User Authentication	1.less efficiency
10	Blowfish	1.High availability 2.Data integrity 3.Confidenltiy 4.Data authentication	1.Less secure

Table 1. Performance Analysis Table for Cryptography Algorithms.

Table (1) shows the three columns. First column shows the reference number of papers. Second column display advantages achieved using different algorithm and techniques. End most column shows disadvantages of different algorithms and techniques. Based on this survey we conclude AES, Blowfish,RC6 algorithms are gives good result in terms of speed as compare to asymmetric algorithm. But RSA algorithm gives high performance in terms of security .

IV.CONCLUSION AND FUTURE WORK

Symmetric algorithms are gives better performance in terms of speed as compare to asymmetric algorithm. Asymmetric algorithms provide better security as compare symmetric algorithm.AES algorithm gives better security as compare to RC6 and Blowfish algorithm. But RSA algorithm gives more security than AES algorithm.RC6 and Blowfish algorithms gives better performance in terms of speed as compare to AES algorithm but AES algorithm require minimum amount of time for encryption and decryption as compare to RSA .In future we will introduce new cryptography algorithm to avoid the security risk in cloud computing and improve the quality of service parameters.

REFERENCES

1. D. Patel and M.B.Chaudhari,' DATA SECURITY IN CLOUD COMPUTING USING DIGITAL SIGNATURE', International Journal For Technological Research In Engineering Volume 1, Issue 10,PP.1177-1180, June-2014 .
2. B. Nayak, Sudhansu Ranjan Lenka,'Enhancing Data Security in Cloud Computing using RSA Encryption and MD5 Algorithm ',,IJCST ,Volume 2 Issue 3, pp.60.-64,June-2014
3. Deepika Verma, K. Mahajan,' To Enhance Data Security in Cloud Computing using Combination of Encryption Algorithms', International Journal of Advances in Science and Technology (IJAST), Vol 2, Issue 4 ,pp.41-44,December 2014
4. R. Pal Singh,' Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques', SSRG International Journal of Mobile Computing & Application , volume 2, Issue 3 ,pp.38-44,June 2015
5. Rabah Attia, Sana Belguith,' Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm', ICAS, 2015
6. P. Kulurkar ,Ruchira. H. Titare1, ' Data Security and Privacy in Cloud using RC6 Algorithm for Remote Data Back-up Server', IJESAT ,Volume-5, Issue-2, pp,149-153, Mar-Apr 2015
7. P. M. Pardeshi , Deepali R. Borade,' Enhancing Data Dynamics and Storage Security for Cloud Computing using Merkle Hash Tree and AES Algorithms , International Journal of Computer Applications ,Volume 98 – No.21,pp.1-7 July 2014

8. Hanumantha Rao.Galli,, P.Padmanabham,' Data Security in Cloud using Hybrid Encryption and Decryption', International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10,pp.494-497, October 2013

9. Sukhpreet Kaur,' Multi-Level Data Integrity Service', International Journal of Computer Applications , Volume 103 – No.14, pp.1-6,October 2014

10. S. B. Subhash, S,Thakur,' Data Confidentiality in Cloud Computing with Blowfish Algorithm, IJETST ,Volume-1, Issue-1,pp.1-6,March 2014 - Volume||01||Issue||01||Pages01-06|ume||01||Issue||01||Pages01-06||Marc