IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Comparative study of various Security Algorithms applicable in Multi-Cloud Environment

Ms.Theres Bemila[1], Karan Kundar[2], Lokesh Jain[3], Shashikant Sharma[4], Nayan Makasare[5]

Assistant Professor, Dept. of Information Technology, Shah & Anchor Kutchhi Engg., College, Mumbai, (MH) India[1]

B.E.Student, Dept. of Information Technology, Shah & Anchor Kutchhi Engg., College, Mumbai, (MH) India [2,3,4,5]

Abstract: In Cloud computing, data security is the major issue. Cloud computing environment security issues are handled by the system administrator or Cloud administrator. All the services related to data storage, data Availability is managed by third party who owns the infrastructure .Researches on Security in single Cloud is paid more attention than in Multi-Cloud. Organizations are migrating towards multi-Cloud due to its ability to overcome issues like data Availability, integrity and authenticity in this paper; we describe an architecture for security of data in multi-Cloud environment. The security of the data can be done by using different secret sharing algorithm. A systematic analysis of the various security algorithms is done, to improve security on multi-Cloud. This architecture will address data security in multi-Cloud environment and enhance security to some extent.

Keywords: Multi-Cloud, AES, DES, 3DES, RSA, CSP.

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]. Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [2][3]. The Cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [4]. Cloud is the metaphor of Internet. As the data storage is the main facility provided by Cloud, there are security threats and issues regarding to the data storage in Cloud. Hence enabling security in Cloud computing is major issue.

In single Cloud security risks are many and it is prone to different attacks. Hence new concept of multicloud can be used to solve security problems. Multicloud is also called as interclouds i.e. Cloud of Clouds. Data can be stored in multiple numbers of Clouds. Security regarding with data storage in multicloud is more popular than in single Cloud due to its less risks of attacks. This paper includes proposed multicloud system security architecture wherein multicloud storage system is used to store client's data. For enabling security in the multicloud architecture two ways are incorporated namely splitting and data encoding technique. Client data can be encrypted using data encoding technique and the data will be split into three different Cloud server and thus stored into the multicloud.

The study presented in this paper is organized with a view to discuss and identify the approach to cloud computing as well as the security issues and concerns that must be taken into account in the deployment towards a cloud based computing infrastructure. The remainder of this paper is organized as follows. Section II describes the proposed multi-cloud security architecture. In addition, it illustrates modules with working. Section III discusses the different types of algorithm that can be used in the cloud computing infrastructure. Section IV analyses and comprises of the different types of algorithms in new generation of cloud computing, that is, multi-clouds and recent solutions to address the security of cloud computing, as well as examining their limitations. Section V concludes the paper based on the discussion on the technological concepts and approaches to data security in multicloud environment.

II. SECURITY MECHANISM ARCHITECTURE

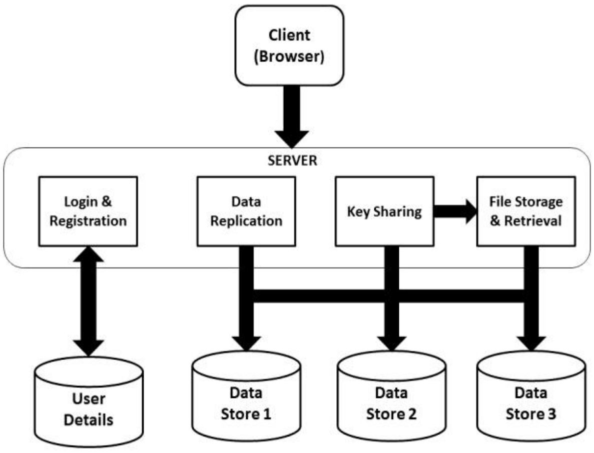

Figure 1. Security Mechanism Architecture

DOI 10.17148/IJARCCE.2016.53111

The Security Mechanism consists of following :-

- Client browser:- It's a interface from which client can access the Cloud services.

- Server:- It is responsible for processes including data replication, key storage, file retrieval, file storage. The security mechanism will be implemented at server side. User details will be managed and controlled by Cloud administrator.

- User-Detail:- It is a Database that consist of details of Registered Users.

- Data-Stores:- These are the individual Clouds in which the data get splits into multiple parts so it is not readable(i.e. in encrypted form). Once the data is encrypted by the Server, the data is divided into multiple parts according to the number of clouds and stores them in these individual Data Stores.

III. DIFFERENT ALGORITHM FOR DATA SECURITY MECHANISM:

- 3DES:- 3DES is exactly what it is named–it performs 3 iterations of DES encryption on each block. As it is an enhanced version of DES so is based on the concept of Feistel Structure. The 3DES uses a 64 bit plain text with 48 rounds and a Key Length of 168-bits permuted into 16 sub- keys each of 48- bit length. It also contains 8 S-boxes and same algorithm is used in reversed for decryption[6].

- RSA:- The RSA (Rivest-Shamir-Adleman) algorithm is the most important public-key cryptosystem. It is best known and widely used public key scheme. It uses large integers like 1,024 bits in size. It has only one round of encryption. It is asymmetric block cipher. RSA is an algorithm used by modern computers to encrypt and decrypt messages. RSA is an asymmetric cryptographic algorithm. This is also called public key cryptography, because one of them can be shared with everyone and another key must be kept private.

- AES:- In 1997, the National Institute of Standards and Technology (NIST) announced an initiative to choose a successor to DES; in 2001, it selected the Advanced Encryption Standard as a replacement to DES and 3DES. AES (Advanced Encryption standard) is developed by Vincent Rijmen, Joan Daeman in 2001. The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively [7].

- BlowFish:- Blowfish was developed by bruce schneier in 1993. It is basically a symmetric block cipher having variable length key from 32 bits to 448 bits. It operates on block size 64 Blowfish is a variable key length algorithm and it is having 64-bit block cipher. The algorithm consist of two sub parts, one is key expansion part and second data encryption part. Data encryption is done by completing 16 rounds fiestel network. bits. It is a 16-round Feistel cipher [7].

- DES:- DES is symmetric key algorithm based on the backbone concept of Feistel Structure. The DES is a block cipher that uses a 64 bit plain text with 16 rounds and a Key Length of 56-bit, originally the key is of 64 bits (same as the block size), but in every byte 1 bit in has been selected as a 'parity' bit, and is not used for encryption mechanism [8].

- Diffie-Hellman:- It is the first public key encryption algorithm, using discrete logarithms in a finite field. Allows two users to exchange a secret key over an insecure medium without any prior secrets.Diffie-Hellman (DH) is a widely used key exchange algorithm. In many cryptographically protocols, two parties wish to begin communicating. The key exchange by Diffie-Hellman protocol, by allowing the construction of a common secret key over an insecure communication channel. [9].

IV. COMPARISON OF VARIOUS DATA SECURITY ALGORITHMS

This analysis presents a performance evaluation of selected symmetric and asymmetric encryption algorithms such as DES, 3DES, AES, Blowfish, RSA and Diffie Hellmen. The following factors are used as the performance criteria, such as the Throughput, Keys used, Tunability, Computational speed, Key length, Encryption ratio and the security of data against attacks.

- Throughput - It refers to how much data can be transferred from one location to another in a given amount of time. It is used to measure the performance of hard drives and RAM, as well as Internet and network connections.

- Keys used - It refers to the use of same or different in encryption and decryption process. In short , it refers to the level of security, of that particular algorithm.

- Tunability - It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters limits the usability of the scheme to a restricted set of applications.

- Computational Speed - In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.

- Key Length Value - In the encryption methodologies the key management is the important aspect that shows how the data is encrypted. The image loss the encryption ratio is based on this key length. The symmetric algorithm uses a variable key length which is of the longer. Hence, the key management is a considerable aspect in encryption processing.

- Encryption Ratio - The encryption ratio is the measure of the amount of data that is to be encrypted. Encryption ratio should be minimized to reduce the complexity on computation.

DOI 10.17148/IJARCCE.2016.53111

- Security of data against attacks - Security Issues Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack. For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security. In our analysis we measure cryptographic security in three levels: low, medium and high.

Table 1.Comparison of Encryption Algorithm.

Algorithms Parameters	DES	3DES	AES	Blowfish	RSA	Diffie-Hellman
Encryption technique	Asymmetric key	Asymmetric key	Asymmetric key	Asymmetric key	Symmetric key	Symmetric key
Keys used	Same key used for encryption and decryption.	Same key used for encryption and decryption.	Same key used for encryption and decryption.	Same key used for encryption and decryption.	Different key used for encryption and decryption.	Key exchange.
Throughput	Lower than AES.	Lower than DES.	Lower than blowfish.	Very High	High	Low
Encryption ratio	High	Moderate	High	High	High	High
Key Lengths	56 bits.	112 to 168 bits.	128,192 or 256 bits.	32 bits to 448 bits.	>1024 bits	Key exchange management.
Rounds	16	48	10,12,14	16	1	56
Tunability	No	No	No	Yes	Yes	Yes
Security against	Brute force attack	Brute force, choosen-plain text, known plain text.	Chosen plain, known plain text.	Dictionary attacks	Timing attacks.	EavesDropping.
Flexibility support	No	Yes	Yes	Yes	Yes	No
Modification	No,DES does not support any modification	The key size is increased from 56 to 168 bits	128,192 or 256,Its structure was flexible to multiples of 64	Key length in blowfish should be multiples of 32	Key length in RSA algorithm can be 256 ,512,1024,2048, 4096 bits	No modification in key length.
Created by	IBM	IBM	Vincent Rijmen , Joan daeman	Bruce Schiener	Ron Rivest,Shamir & leonard Adleman	Whitfield diffie, Martin Hellman
Year	1970	1978	1978	1993	1978	2002
Structure of the Algorithm	Feistal structure	Feistal structure	Feistal structure	Feistal structure	Feistal structure	Tree based
Cloud Compatibility	Yes (Generally not used)	Yes	Yes	Yes	Yes	Yes
Algorithm used in Cloud	Not used in Cloud (it is prone to many attacks and easy to break)	Not used in Cloud (it is prone to many attacks and easy to break)	Google Drive, OneDrive, Dropbox	Mozy Backup, Foopchat, GigaTribe	Amazon web Services, RSAWeb	CurveCP
Application	Smart Card	Microsoft OneNote,Outlook 2007	Password Manager	IDS Server,Sql Server 2000	Online Credit Card Security System,RSA Signature Verification	In many Protocols like SSL,SSH,IPSec

DOI 10.17148/IJARCCE.2016.53111

This paper presents a performance evaluation of selected symmetric and asymmetric encryption algorithms such as DES, 3DES, AES, Blowfish, RSA and Diffie Hellmen. We can evaluate a table that the encryption ratio is high in using the both encryption techniques. Each algorithm has its own benefit according to different parameters. The key length is high in asymmetric encryption algorithm so to break the code is complex in RSA. In the aspect of throughput, Throughput is increased so power consumption is decreased. In the symmetric key encryption techniques the blowfish algorithm is specified as the better solution. In the Asymmetric encryption technique the RSA algorithm is more secure since it uses the factoring of high prime number for key generation. Hence, the RSA algorithm is found as the better solution in this method.

V. CONCLUSION

Cloud computing is a revolution in information technology, still there are various issues related to security in cloud computing. Cloud computing, user store the sensitive data storage so that they can be accessed later. There is need to store the data securely and the data is to be made available to authenticated authorized users only. CSP(Coud service provider) might reclaim storage for monetary reasons by discarding data that has not been or is rarely accessed, or even hide data loss incidents so as to maintain a reputation. In short, storing data to the cloud is economically attractive for long-term large-scale data storage, it does not immediately offer any guarantee on data integrity and availability. From above study, RSA algorithm can be applied for data security in multi cloud environment. Our current aim is to secure text documents which may include confidential data like credit card details, bank customer’s record etc. This paper is schema of proposed framework, and hence addresses the security issues in multi cloud environment.

REFERENCES

[1] Peter Mell, and Tim Grance, “The NIST Definition of Cloud Computing,” http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin,Heidelberg,pp347–358 http://www.jisajournal.com/content/4/1/5

[3] Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN’10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 93–97 http://www.jisajournal.com/content/4/1/5

[4] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available:https://Cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[5] Parsi Kalpana, Mrs. Sudha Singaraju: Data Security in Cloud Computing using RSA Algorithm, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841,Vol.1,Issue-4,September(2012). http://www.ijrcct.org/index.php/ojs/article/download/53/40

[6] COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS. Singh et al., International Journal of Advanced Engineering Technology E-ISSN 0976-3945

[7] A Review and Comparative Analysis of Various Encryption Algorithms. International Journal of Security and Its Applications Vol. 9, No. 4 (2015),pp. 289-306. http://dx.doi.org/10.14257/ijsia.2015.9.4.27.

[8] Symmetric Algorithm Survey: A Comparative Analysis. International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.

[9] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.

DOI 10.17148/IJARCCE.2016.53111