International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Survey on Data Security using Encryption Algorithms in Cloud Environment

Santhi Baskaran, Isaiarasi A
Information Technology, Pondicherry Engineering College, Pillaichavadi, Puducherry, Tamil Nadu, India

ABSTRACT

Cloud Computing is very flexible in nature that helps to quickly access the resources efficiently from the third party service provider to expand the business with low capitalization cost. A cloud storage system stores large number of data in its storage server. Since the data is stored for a long term over the internet it does not provide the data confidentiality and make the hackers to steal the data provided in the storage system and even when data forwarded to cloud environment, it lacks data integrity and makes the cloud user unsatisfied. In this paper, study about the different encryption technique to protect the cloud storage environment. This paper concisely covers some of the existing cryptographic approaches that can be used to improve the security in cloud environment.

Keywords : Cloud Computing, Cloud security, Encryption algorithms, Security challenges, security.

I. INTRODUCTION

Cloud computing is the latest approach in the present generation to minimize the cost by providing a sharing environment for the cloud user, the cloud users can remotely store and retrieve their data into the cloud. By envisioning outsourcing of data, users can be released from the burden of data storage and maintenance. Preserving integrity of data is an issue that the physical possession of the possibly outsourced data is not known by the user makes the Cloud Computing very challenging and potentially tasking, particularly for users with certain constrained computing resources and capabilities. Cloud computing, enables users to keep their information in the cloud so as to utilise scalable on demand services.

Cloud Computing is a type of computing infrastructure that consists of a collection of inter-connected computing nodes, servers, and other hardware as well as software services and applications that are dynamically provisioned among competing users. Services are delivered over the Internet or private networks, or their combination. The cloud services are accessed over these networks based on their availability, performance, capability, and Quality of Service (QoS) requirements. The focus is to provide reliable, secure, fault-tolerant, maintainable and scalable services, platforms and infrastructures to the end-users. These systems have goals of providing virtually unlimited computing and storage and hiding the complexity of large-scale distributed computing from users. Thus cloud computing is a new way of distributing services.
Depending on the type of service provided, there are three types of cloud services also termed as delivery models; Infrastructure as a service, (IaaS), Platform as a service (PaaS) and Software as a service (SaaS).IaaS deals with providing computing facility, storage or any other hardware resource. Amazon is one of the cloud providers offering IaaS, where these services are EC2 and S3.

PaaS provides platforms in terms of operating system and other system software that can be used to build custom applications by the users. User can configure and develop their application on the specific platform. Microsoft Azure is an example of PaaS. SaaS deals with using any application or service via cloud. Google Apps is one of the examples that provide collaboration on various applications, like event management, project management etc. via internet. In this paper, describe various cryptographic techniques can be used to protect the data used in the cloud and prevent information from being betrayal and to ensure that the privacy has been maintained. The cryptographic methods were used to confirm security for the data stored in the cloud.

Table 1: Literature Survey

Technique	Author	Algorithms	Performance	Advantages	Disadvantages
Data Access	Mazar Ali et al., 2015[13]	Fragment placement, Fragement replication	Have a more no of replica copies	Full data is not revealed on attack of single node.	Time and Resource consumption is more.
	Kaitai et al., 2015 [12]	Searchable Attribute based proxy reencryption system	The system enables a data owner to efficiently share his data to a specified group of users matching a sharing policy	Secure ciphertext	Lazy revocation process.
	Peng et al., 2016	Conditional Identity based Broadcast PRE (CIBPRE)	CIBPRE allows a sender to encrypt a message by identifying the receivers identity	Efficient with respect to communication	escrow
	Mazhar Ali et al., 2015[13]	DaSCE and Shamirs scheme	DaSCE was evaluated based on the time consumption during file upload and download.	DaSCE provides high security standards and does not compromise the keys under outsourced data	DaSCE methodology can be extended to secure group shared data and secure data forwarding
Data Availability	Zhang et al., 2015[14]	CHARM	Integrates two key functions 1. selecting suitable clouds 2. Transition process to redistribute data	Saves cost	Risky to choose the cloud
	Xu et al., 2015	DelayDedup	Delaydedupe is combined with replica management that determines new duplicated chunks	Reduces response time	Need more storage space
	Mingqiang et al., 2016	CDstore	A unified multicloud storage solution for users to outsource backup data	Guarantees reliability, security and cost efficient	cost
	Seungycon et al., 2016	MetaSync	Provides multiple cloud synchronization services as untrusted storage providers	Provides better availability, stronger confidentiality and integrity	Key management
Data Integrity	Zhongyuan et al., 2016	Cluster Content Caching structure in C-RANS	By using a stochastic geometry-based network model, the effective capacity can be achieved	Effective capacity and energy efficiency	Performance is improved by combining the designs of RRU allocation and RRH association
	Shubhashis et al., 2015[15]	Data Vaporizer	Advanced techniques of secret sharing of the keys to improve the security level and reliability	Storage cost is minimum	Design of highly configurable framework for data storage on top of cheap commodity cloud storage
	Huagun et al., 20	ID-PUIC	Realizes checking of data integrity of both private/public authorization	Checking of the integrity on clouds improve the performance	Computation overhead is more
	Yong et al., 2016	Public integrity auditing scheme	A cloud server can collude with a revoked user to deceive a third-party auditor (TPA) that a stored file keeps.		Aforementioned attacks

II. RELATED WORK

Xu, Lei and Wu, Xiaoxin and Zhang, Xinwen,Data access refers to a user's ability to access or retrieve data that is stored within a database or other repository. Xu et al., [25] developed Ceritificate Less Proxy Re-Encryption (CLPRE), a new proxy-based re-encryption scheme augmented with certificateless public key cryptography. CL-PRE is used for data storage and also to generate secret key and distributed to users for securely sharing the data. Along with CL-PRE, symmetric data encryption is used for encryption purpose by generating proxy re-encryption keys. The data is decrypted using by using users private key. uses MCL-PKE and Security Mediator (SEM) to get the key that is used to get back partial private key information.

III. SECURITY ALGORITHMS

Many organizations and people store their important data on cloud and data is also accessed by many persons, so it is very important to secure the data from intruders. To provide security to cloud many algorithms are designed. Some popular algorithms are:-

A. Data Encryption Standard (DES)

This stands for Data Encryption Standard and it was technologically advanced in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher. [5]

Algorithm:
function DES_Encrypt (M, K)
where M = (L, R)
M ← IP (M)
For round ←1 to 16 do
K←SK (K, round)
L←L XOR F(R,Ki)
swap(L, R)
end
swap (L, R)
M←IP-1(M)
return M
End.

A. Advance Encryption Algorithm (AES)

It is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. AES having a variable key length of 128, 192, or 256 bits and default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES Encryption is more fast and flexible. It can be applied on various platforms especially in small devices. Also, AES has been carefully tested for many security applications. [6][7]

B. Triple- DES (TDES)

This was introduced in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in unique DES but applied 3 times to increase the encryption level. But 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power depletion and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics. [6][8].

C. IDEA

International Data Encryption Algorithm was considered as best symmetric key algorithm. It accepts 64 bits plain text and key size is 128 bits. IDEA consists of 8.5 rounds. All rounds are similar except the one. In IDEA the 64 bits of data is divided into 4 blocks each having size 16 bits. Now basic operations modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied on sub blocks. There are eight and half rounds in IDEA each round consist of different sub keys. Total number of keys used for performing different rounds is 52. In round 1 the K1 to K6 sub keys are generated, the sub key K1 has the first 16 bits of the original key and K2 has the next 16 bits similarly for K3, K4, K5 and K6. Therefore for round 1 (16*6=96) 96 bits of original cipher key is used.

E. Blowfish Algorithm

This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier.

Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various investigation and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption [8].

Algorithm: Divide x into two 32-bit halves: xL , xR
For i = 1to 16:
x L = xL XOR Pi
x R = F(xL) XOR xR
Swap xL and xR Next i
Swap xL and xR (Undo the last swap.)
x R = xR XOR P17 x L = xL XOR P18
Recombine xR and xL

F. Holomorphic Encryption

Homomorphic encryption uses asymmetric key algorithm in which two different keys are used for encryption and decryption i.e. public key and private key [10]. In mathematics homomorphic means conversion of one data set to another, without losing its relation between them. In homomorpic complex mathematics functions are applied to encrypt the data and similar but reverse operation is applied to decrypt the data.

G. RSA

The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption [9].

Algorithm
Key Generation:
KeyGen(p, q)
Input: Two large primes –p, q
Compute n = p. q $\varphi(n) = (p-1)(q-1)$
Choose e such $\gcd(e, \varphi(n)) = 1$
Determine d such that $e.d \equiv 1 \bmod \varphi(n)$
Key: Public key = (e, n) Secret key= (d, n)
Encryption: $c = m^e \bmod n$

H. Diffie- Hellman Key Exchange

It is a key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange applied within the field of cryptography. The Diffie–Hellman key exchange technique allows two parties that have no previous knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt ensuing communication using a symmetric key cipher.

Table 2 : Comparative Study of Various Symmetric Encryption Algorithms

Characteristics	**Blow fish**	**AES**	**RC5**	**IDES**	**3-DES**	**DES**
Developed	1993	2000	1994	1992	1998	1977
Key Length	32 to 448 (default 128	128, 192 or 256	2040 (Max	128	112,168	56
Block Size	64	128, 192 or 256	32, 64 or 128	64	64	64
Cipher Text	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	
Cryptanalysis Resistance	Strong against the standard differential and linear cryptanalysis	Very strong against differential, truncated differential, linear interpolation and square attack	Vulnerable against differential, truncated differential, linear interpolation and square attack.	Vulnerable to differential and linear cryptanalysis	Strong against differential, truncated differential, linear interpolation and square attack	Vulnerable to differential and linear cryptanalysis. Weak substitution table
Security	Considered as more Secure	Considered Secure	Considered Secure	Proven inadequate	Secure	Proven inadequate
Possible Keys	2^{448}	2^{128},2^{192},2^{256}	2^{128},2^{192},2^{256}	2^{128}	2^{56}	2^{56}
Speed	Very Fast	Fast	Slow	Slow	Slow	Very slow

IV. DATA SECURITY IN CLOUD COMPUTING

Major concern is security of data. Data relocation on high level has negative implications for data safety and data security as well as data availability. Thus the main apprehension with reference to safety of data residing in the Cloud is: at the rest how to safe security .Although, customers know the location of data and there in no data mobility, there are question relating to its security and secrecy of it. No confusion the Cloud Computing area has become bigger because of its wide network access and flexibility. But we can also rely in terms of a safe and secure atmosphere for the personal data and info of the user is being required.

A. Data Security Issues in Cloud Computing

1. Privacy and Confidentiality:
The client show data to the cloud there should be some security that access to that data will only be incomplete to the authorized access. Inappropriate access to client sensitive data by cloud staff is another risk that can create potential threat to cloud data. The client is being provided assurance and proper practices and safe policies and procedures should be in place to guarantee the cloud users of the data safety. The cloud seeker must be assured that data propagate on the cloud will be confidential.

2. Data Integrity:
The security of data, cloud service providers should apply mechanisms to ensure data truthfulness and be able to tell what happened to a definite data set and at what point. The client should be aware by the data

3. Data Location and Relocation:
Consumers do not always know location of their data. However, when an venture has some sensitive data that's reserved over a storage device in the Cloud, they will often keep asking the career than it. They

will also aspiration to specify a chosen location (e.g. data being trapped in India). This, then, needs a predetermined agreement, between your Cloud provider and also the consumer that data should live in a certain location or reside on a given known server. Also, cloud providers should take accountability to guarantee the security of systems (including data) and gives robust certification to protect customer's information.

5. Data Availability:
Customer info is normally saved in chunk on different servers often residing in different locations or even in different Clouds. In such cases, data availability becomes a major legitimate issue because use of un-interruptible and seamless provision becomes relatively difficult.

6. Storage, Backup and Recovery:
If you choose to maneuver crucial computer data for the cloud the cloud provider make certain adequate data resilience storage systems by the side of a minimum they need to be able to present RAID (Redundant Array of Independent Disks) storage systems while most cloud providers will store the details in many copies some independent servers..

B. Security Advantages in Cloud Environment

Many large systems are operated by current cloud service. They have complicated processes and specialization for maintaining their systems, which tiny enterprises may not have access to. As a result many direct and indirect security benefits
for cloud users. Here we show some of the key protection advantages of a cloud computing atmosphere.

1. Data Centralization:
In a cloud atmosphere, the service provider takes care of storage issues and small business will not spend a extra money on storage devices. Also, cloud based storage provides a technique to physical centralize the data more rapidly and potentially cheaper and useful for small businesses, which cannot spend money on security professionals to monitor the data.

2. Incident Response:
IaaS providers can offered a dedicated forensic server which they can use at the moment basis. Every time a security contravention occurs, the server could be brought online. In some investigation cases, backup with the environment can be simply made and hang onto the cloud without having affecting the traditional span of business.

3. Forensic Image Verification Time:

Some cloud storage implementations picture a cryptographic check sum or hash. For example, Amazon S3 generates MD5 (Message-Digest algorithm 5) hash without human intervention when you store an object. Therefore in theory, the need to produce time consuming MD5 checksums with external tools is eliminated.

4. Logging:

In a usual computing standard generally, logging is repeatedly an afterthought. In common, insufficient disk space is allocated that makes logging either non-existent or minimal. However, in a cloud, storage need for typical logs is automatically solved.

C. Security Disadvantages in Cloud Environment

In spite of security benefits, cloud computing paradigm also shows some key security challenges. Here we look at some key security challenges.

1. Data Location:

Cloud users are not aware of the exact position of the data center and also they do not have any power over the physical access mechanisms to that data. Most famous cloud service providers have datacenters around the globe. Some service providers also take benefit of their universal data centers. Though, in some cases applications and data may be stored in countries, which can bench concerns.

2. Investigation:

Investigating an illegitimate movement may not be possible in cloud environments. These surveys are hard by Cloud services because data for multiple clients may be co-located and may also be increase across multiple data centers. Users have little information about the network topology of the underlying environment. Service provider may also enforce limits on the network security of the service users.

3. Data Segregation:

Data in the cloud is usually in a shared environment together with data from other clients. Encryption cannot be assumed as the single solution for data separation problems. In some situations, customers would not like to encrypt data because there can be a case when encryption accident can demolish the data.

4. Long-term Viability:

When changing business situation as mergers and attainment service providers must ensure the data safety. Customers must ensure data accessibility in these situations. Service provider also makes sure data security in harmful business conditions like prolonged outage etc.

5. Compromised Servers:

In a cloud computing situation, users do not have a special of using physical acquisition toolkit. In that situation, where a server
is compromised; they need to close their servers down till they get a earlier backup of the data. This will more cause availability concerns.

6. Regulatory Compliance:

External audits and security certification are subjected by traditional service provide. If a cloud service provider does not hold to these security audits, then it leads to a perceptible decrease in customer trust.

7. Recovery

Cloud service providers make sure the data security in familiar and man-made disasters. Generally, data is virtual across multiple sites. However, in the case of any such unnecessary event, provider must do a comprehensive and quick restoration

V. CONCLUSION

The data storage service is the main service provided by the cloud provider. The Cryptographic techniques have been used widely in cloud environment. Cryptography is an necessary tool that helps to assure our data exactitude. Cryptographic methods has been effectively lead by the development of cloud computing and also due to vast increment in the range of users of the cloud. The cloud storage researchers also focus more on the cryptographic techniques. The data is provided with security by the usage of these above discussed cryptographic techniques. The security properties like confidentiality, integrity, reliability can

be achieved. This paper describes various cryptographic techniques that can be used in cloud computing environment. Thus the data can be securely shared with the authorized users by accepting the cryptographic techniques.

VI. REFERENCES

[1]. T. Ramaporkalai, Security Algorithms in Cloud Computing, International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 2, Apr 2017 .

[2]. R.Kirubakaramoorthi*, D. Arivazhagan and D. Helen, Survey on Encryption Techniques used to Secure Cloud Storage , Indian Journal of Science and Technology, Vol 8(36),2015.

[3]. Kumar(2012), "World of Cloud Computing & Security," International Journal of Cloud Computing and Services Science (IJ-CLOSER)Vol.1, No.2, pp. 53~58.

[4]. Y.Tang, P.P.Lee, J.C.S.Lui, and R.Perlman (2012), "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, Vol.9, No.6, Nov. 2012, pp.903-916.

[5]. Shuhua Wu and Yuefei Zhu (2011), "Improved Two-Factor Authenticated Key Exchange Protocol," International Arab Journal of Information Technology, Vol. 8, pp.66-79.

[6]. Zarandioon, S., Yao, D. D., & Ganapathy V. (2011). "K2C: Cryptographic cloud storage with lazy revocation and anonymous access," International Conference on Security and Privacy in Communication Systems, vol.2 pp. 59-76, Springer Berlin Heidelberg.

[7]. Caching and M. Schunter," A clo9ud you can trust," IEEE Spectrum, Vol. 48, No. 12, 2011, pp.28-51.

[8]. S.Kamara and K. Lauter (2010), "Cryptographic cloud storage" Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp.136-149.

[9]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Ktaz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoics and M. Zaharia (2010), "A View of Cloud Computing, " Communications of the ACM, Vol.53, No.4, pp.50-58.

[10]. Yun, C. Shi, and Y. Kim (2009), "On protecting integrity and confiden-tiality of cryptographic file system for outscored storage," Proceed-ings of 2009 ACM workshop on cloud computing security CCSA'09, vol.2,pp. 67-76.

[11]. G. Ateniese, M. Steiner, and G. Tsudik (2000),"New multi-party authentication services and key agreement protocols," IEEE J. Sel. Areas Cmmun, vol. 18, no. 4, pp. 628–639.

[12]. W.Diffie, P.C.V.Oorschot, and M.J.Wiener (1992),"Authentication and authenticated key exchanges," Designs, Codes and Cryptography, IEEE Spectrum Vol. 2, No.2, pp.107-125.

[13]. Mazhar Ali, Saif Malik, and Samee Khan, "DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party", IEEE Transactions on Cloud Computing, 2015.

[14]. Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, and Yafei Dai, "CHARM: A CostEfficient Multi-Cloud Data Hosting Scheme with High Availability", IEEE Transactions on Cloud Computing, vol. 3, no. 3, pp. 372-386, July-September 2015

[15]. Jin Sun, Yupu Hu, and Leyou Zhang, "A Key-Policy Attribute-Based Broadcast Encryption", The International Arab Journal of Information Technology, vol. 10, no. 5, pp. 444-453, September 2013.

[16]. Amol S. Choure S. M. Bansode, "A Comprehensive Survey on Storage Techniques in Cloud Computing", International Journal of Computer Applications, vol. 122, no. 18, pp. 3-25, July 2015.