Data Security in Cloud Computing

Dimpy Jindal and Barkha Bahl***

ABSTRACT

Cloud computing is one among the fastest emerging technologies in to computing. There are many advantages yet as well as few security issues in cloud computing. It is a study of knowledge in the cloud and aspects associated with it concerning security. The paper will go in to details of data protection methods and approaches used throughout the planet to ensure maximum data protection by reducing risks and threats.

The two important hardware and software parameters for cloud architecture are Data security and privacy protection techniques. The focus is to review existing security techniques and their challenges with respect to both software and hardware aspects for shielding data within the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment. Cloud allow its users to remotely access and store data.

Keywords: *Cloud Computing; Data Security; Cloud Services; Confidentiality; Integrity; Availability; Authentication and Access controls.*

1.0 Introduction

Cloud computing is an emerging technology which recently has drawn significant attention from both industry and academia. It provides services over the web, by using cloud computing user can utilize the online services of various software rather than purchasing or installing them on their own computers. According to the National Institute of Standard and Technology (NIST) definition, cloud computing can be defined as a paradigm for enabling useful, on-demand network access to a shared pool of configurable computing resources.[1] Cloud Computing isn't considered as application oriented but service oriented. Sharing of data is one reason of losing data security and protection. In order to avoid potential risk to the data, it is necessary to protect data repositories. One amongst the key questions while using cloud for storing data is whether or not to use a 3rd party cloud service or create a non-private organizational cloud. Sometimes, the information is just too sensitive to be stored on a public cloud, for example, national security data or highly confidential future product details.

This type of data will be extremely sensitive and therefore the consequences of exposing this data on a public cloud is serious. In such cases, it is highly recommended to store data using internal organizational cloud. This approach can help in securing data by enforcing on-premises data usage policy. However, it still does not ensure full data security and privacy, since many organizations are not qualified enough to add all layers of protection to the sensitive data. This paper discusses the potential threats to data in the cloud and their solutions adopted by various service providers to safeguard data. There are two widely used methods to retrieve the cipher text. First, there is a safety index-based approach which establishes a secure cipher text key words indexed by checking the existence of key words. Second, there is a cipher text scanning-based approach which confirms the existence of key words by matching each word in cipher text. The article discusses and analyses the data security and storage issues along with its solutions and its future development of cloud computing.

**Corresponding author; Computer Science teacher, Department of IT, Sachdeva Public School, Pitampura, New Delhi, Delhi, India. (Email: dimpy.jindal23@gmail.com)*

***Director, Department of IT, Trinity Institute of Professional Studies, New Delhi, Delhi, India. (Email: barkha69@rediffmail.com)*

2.0 Classification of Cloud Computing

The main attributes of cloud computing are Multi-tenancy, massive scalability, elasticity and self-provisioning of resources.[2] The services model of cloud computing is split into three categories (1) IaaS (infrastructure as a service) provides the utilization of virtual computer infrastructure environment, online storage, hardware, servers and networking components; (2) PaaS (platform as a service) provides platform for developing applications by using different programming languages; (3) SaaS (software as a service) facilitates the user to access online applications and software that are being hosted by the service providers. The deployment model of cloud computing include (1) public cloud, that owned by service provider and its resources are rented or sold to the general public (2) private cloud, that is owned or rented by a company (3) community cloud, that's just like private cloud but cloud resources is shared among number of closed community (4) hybrid cloud, exhibits the property of two or more deployment models. [3] Figure1 shows the NIST definition framework for cloud computing.

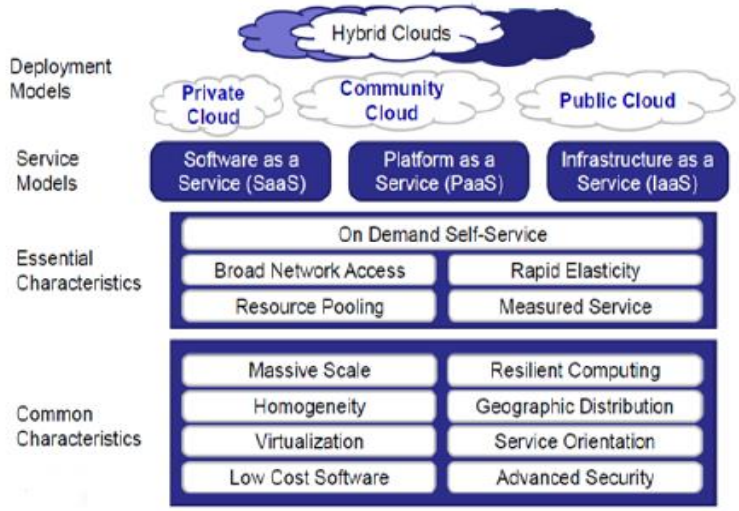

Fig1: NIST cloud definition Frame work

3.0 Data Security in Cloud Computing

Data security in cloud computing involves more encoding. Requirements for data security depends upon on the three service models SaaS, PaaS, and IaaS.

Two states of data normally have threat to its security in clouds; Data at Rest which implies the information stored within the cloud and Data in Transit which suggests data which is moving in and out of the cloud. Confidentiality, and Integrity of information is predicated upon the character of knowledge protection mechanisms, procedures, and processes. The foremost significant matter is that the exposure of knowledge in above mentioned two states.

A. Data at Rest

Data at rest refers to data in cloud, or any data that may be accessed using Internet. This includes backup data additionally as live data. As mentioned earlier, sometimes it's very difficult for organizations to safeguard data at rest if they're not maintaining a non-public cloud since they do not have physical control over the information. However, this issue will be resolved by maintaining a personal cloud with carefully controlled access.

B. Data in Transit

Data in transit normally refers to data which is moving in and out of the cloud. This data may be within the variety of a file or database stored on the cloud and may be requested to be used at another location. Whenever, data is uploaded to the cloud, the data at time of being uploaded is named data in transit. Data in transit can be very sensitive data like user names and passwords and may be encrypted sometimes. However, data in unencrypted form is also data in transit. [4] Data in transit are often sometimes more exposed to risks than the data at rest because it has to travel from one location to another. [5] There are several ways in which intermediary software can eavesdrop the data and sometimes have the ability to change the data on its way to destination. [6]

4.0 PROTECTING DATA USING ENCRYPTION

Encryption techniques for data at rest and data in transit is different. For examples, encryption keys for data in transit are often short-lived, whereas for data at rest, keys are often retained for extended periods of time. Different cryptographic techniques are used for encrypting the info nowadays days. Cryptography has increased the extent of data protection for assuring content integrity, authentication, and availability.

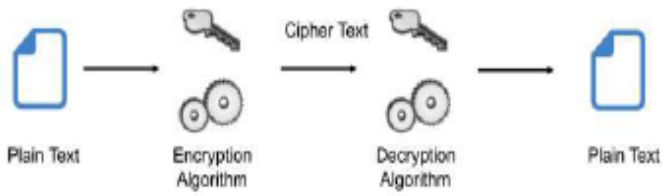

Fig2: Basic Cryptography Process

In the basic sort of cryptography, plaintext is encrypted into cipher text using an encryption key, and also the resulting cipher text is then decrypted employing a decryption key as illustrated in Fig2. Normally there are four basic uses of cryptography:

A. Block Ciphers

A block cipher is an algorithm for encrypting data (to produce cipher text) within which a cryptographic key and algorithm are applied to a block of information rather than per bit at a time. [7] During this technique, it is made sure that similar blocks of text do not get encrypted the identical way in an exceedingly message. Normally, the cipher text from the previous encrypted block is applied to the subsequent block during a series.

The plain text is split in to blocks of information, often 64 bits. These blocks of data are then encrypted using an encryption key to create a cipher text.

B. Stream Ciphers

This technique of encrypting data is additionally called state cipher since it depends upon this state of cipher. During this technique, each bit is encrypted rather than of blocks of information. An encryption key and an algorithm is applied to every and each bit, one at a time. [8] Performance of Stream ciphers is often faster than block ciphers due to their low hardware complexity. However, this system will be susceptible to serious security problems if not used properly. Stream cipher uses an encryption key to encrypt each bit rather than block of text. The resultant cipher text is a stream of encrypted bits that may be later decrypted using decryption key to supply to original plain text.

C. Hash Functions

In this technique, a mathematical relation called a hash function is employed to convert an input text in to an alphanumeric string. Normally the produced alphanumeric string is fixed in size. This method makes sure that no two strings can have same alphanumeric string as an output. Whether or not the input strings are slightly different from one another, there's a clear stage of great difference between the output string produced through them.

Identified Challenges

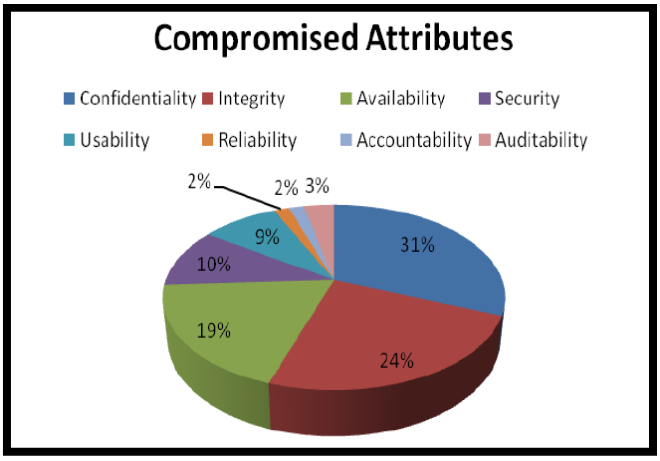

Fig3: List of Compromised attributes

In the part of the analysis, we find some of the Cloud Computing attributes which are threats to Cloud Computing. As a part of the result the compromised attributes in Cloud Computing is described above, they are Confidentiality, Integrity, Availability, Security, Accountability, Usability, Reliability and Auditability. The records of the most threaten attributes are in fig 3. Shows that Confidentiality 31% and Integrity 24% recorded most threaten, while comparing with usability, reliability, accountability and auditability which recorded less than the 10%.

5.0 Identified Mitigation Techniques

The summary include Identity based authentication, AES algorithm, RSA algorithm, Dynamic Intrusion detection system, Multi tenancy based access control model, Third party auditor, probabilistic sampling technique, MACs, Data coloring and water marking, A novel Cloud dependability model, Security assertion markup language, Proof of retrievability, Redundant array of independent Net storages, Handoop distributed file system, self cleansing intrusion tolerance, searchable symmetric encryption, Provable data possession, Privacy manager, Security Access Control Service, The Service Level Agreement, Intrusion detection system.

The above mentioned mitigation techniques have strong impact on the Performance, Security, Efficiency, QoS, Privacy and Access control of Cloud Computing. The defined mitigation techniques somehow improve the overall services in Cloud Computing environment. The result is shown in fig 4.

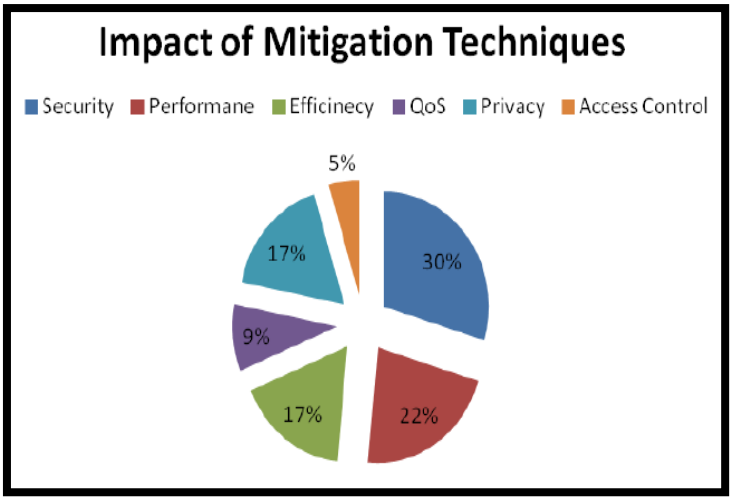

Fig4: Impact of mitigation techniques

6.0 Different Algorithm for Data Security Mechanism:

 3DES: - 3DES is precisely what it's named–it performs 3 iterations of DES encryption on each block. Because it is an enhanced version of DES so is predicated 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 employed in reversed for decryption [9].

 RSA: - The RSA (Rivest-Shamir-Adleman) algorithm is that the most significant public-key cryptosystem. It is best known and widely used public key scheme. It uses large integers like 1,024 bits in size. It's just one round of encryption. It is asymmetric block cipher. RSA is an algorithm employed by modern computers to encrypt and decrypt messages. RSA is an asymmetric cryptographic algorithm. This is often also called public key cryptography, because one in every of them will 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 decide on 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) may be a symmetric block cipher utilized by the U.S. government to guard classified information and is implemented in software and hardware throughout the globe for sensitive encryption. AES is truly, 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 [10].

 Blowfish: - Blowfish was developed by Bruce schneier in 1993. It's basically a symmetric block cipher having variable length key from 32 bits to 448 bits. It operates on block size 64 Blowfish may be a variable key length algorithm and it is having 64-bit block cipher. The algorithm encompass of two sub parts, one is vital expansion part and second encryption part. Encoding is finished by completing 16 rounds fiestel network. It's a 16-round Feistel cipher [11].

 DES: - DES is symmetric key algorithm supported on the backbone concept of Feistel Structure. The DES may be 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 because of block size), but in every byte 1 bit in has been selected as a 'parity' bit, and isn't used for encryption mechanism [12].

 Diffie-Hellman: - It's the primary public key encryption algorithm, using discrete logarithms during a finite field. Allows two users to exchange a secret key over an insecure medium with none prior secrets. Diffie-Hellman (DH) may be a widely used key exchange algorithm. In many

cryptographically protocols, two parties wish to start communicating. The key exchange by Diffie-Hellman protocol, by allowing the development of a typical secret key over an insecure communication channel. [13].

7.0 Comparative Analysis of Security Algorithms

The Table 1 shows the comparison of varied cryptographic algorithms for securing data over cloud based on supported various parameters made within the survey. The parameters considered are key size, block size, number of rounds, execution time, key used and memory usage. The benefits and downsides are also stated.

AES algorithm is vital for electronic sensitive data, cyber security and government computer security. AES has been created for and implemented by U.S government to guard sensitive information [14]. Blowfish algorithm has been implemented on various formats of files like image, audio, video, text, document and portable document format [15]. The result has proved to be stable.

Table i. Comparison of cryptographic algorithms in cloud

Algorithms/ Parameters	AES	RSA	Blowfish	IDEA	DES
Key size	128, 192 or 256 bits	>than 1024 bits	32-448 bits	128 bits	56 bits out of 64 bits
Block size	128, 192 or 256 bits	Variant	64 bits	64 bits	64 bits
Rounds	10, 12 or 14 depending on key size	1	16	8.5	16
Encryption Type	Symmetric	Asymmetric	Symmetric	Symmetric	Symmetric
Key used	Same key for encryption and	One key for encryption and	Same key for encryption and	Same key for encryption and	Same key for encryption and

8.0 Gaps in Literature Survey

Subsequent cryptographic algorithm contains the varied limitations.

1) Existing techniques haven't implemented mathematically to supply time complexity, security theorems and proofs.
2) Automatic classification of information isn't tired previous methods.
3) Safer cryptographic algorithms can be employed in combinations so on to provide confidentiality to user data.

9.0 Research Motivation

To exchange sensitive or counsel between a browser and an online server, Encryption is a plain tool to guard protect communication. Proper encryption of knowledge and encryption of transmission is critical. The mitigation techniques identified from the survey is as follows:

1) SSL (Secure Socket layer)

2) VPN (Virtual Private Network)
3) IPSec (Internet Protocol Security)
4) A proper use of encryption can give good protection against active attacks. So as to safeguard against Man-in-the-middle attacks, one should observe if there are any delayed response times, so as to detect if there's any "Middle-Man".
5) A proper use of encryption can give good protection against eaves dropping. Traffic analysis is harder, but on the opposite hand, not only the several need protection against this type of threat.

10.0 Proposed Work

The proposed model provides different options for security of data, so the options:
 High level of security, for very sensitive data. In this part of measurements we can conclude that high level of security of data from the proposed model uses the method of sending partitions in cloud (file is partitioned then encrypted) and scenario from (use of asymmetric algorithms) that are safer.
 Moderate level of security for less sensitive data. For data that the level of security is moderate, we still propose that partitions be sent to cloud and, also hybrid algorithms as well, as a better solution for data encryption.
 Lower level of security for data that are least sensitive. For data that is not required a high level of security and big data, then we suggest that partitions should be sent to the cloud, (the file is encrypted then sent to clouds) we believe that this method is faster for big and less sensitive data. Also for this case we suggest that symmetric algorithms for the encryption of the partitions, tend to be much faster.
In future work, we could design a framework which will satisfy the security issues related to Multi-tenancy. Multi-tenancy occurs when varied consumers using the same cloud to share the information on a single server.

11.0 Conclusion and Future Challenges

There are many benefits of using cloud computing like cost efficiency, quick deployment, improved accessibility etc. However, there are yet many practical problems which must be solved. The information confidentiality is one in every of them. Many researchers contributed their efforts to attenuate the information security issue during this domain with different solutions that described during the work. One amongst the most important concern of this paper was data security and its threats and solutions in cloud computing. Data in several states has been discussed together with the techniques which are efficient for encrypting the information within the cloud. The study provided an outline of block cipher, stream cipher and hash function which are used for encrypting the information within the cloud whether it's at rest or in transit.

Although our review has explored the sphere, further studies are needed to verify the obtained results. Future work includes the extension of this review by including more sources (conferences, journals and workshops) and questions. A future plan is to explore the opposite security issues within the cloud computing environment and that we also are reaching to design a security model using some encryption techniques for data concealment in cloud computing.

References

P. S. Wooley, February, 2011. "Identifying Cloud Computing SecurityRisks," Contin. Educ., vol. 1277, no.

NIST SP 800-145, (Accessed: 23 December 2013) "A NIST definition of cloud computing", [online]

2012, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.
T.Mather and S.Latif, (Accessed: 4September 2013) "Cloud Security and Privacy, [online] 2009, http://www.slideshare.net/USFstudent1980/cloud-computingsecurity-concerns

IBM, (Accessed: 14 December 2013)"what is cloud computing" [online] http://www.ibm.com/cloud-computing/in/en/what- is-cloud-computing.html

F. Yahya, V. Chang, J. Walters, and B. Wills, 1–6, 2014 "Security Challenges in Cloud Storage," pp.

Ion, I., Sachdeva, N., Kumaraguru, P., & Capkun, (2011, July) "Home is safer than the cloud: privacy concerns for consumer cloud storage." In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13). ACM.

Lipinski, T. A. (2013, September) "Click Here to Cloud: End User Issues in Cloud Computing Terms of Service Agreements." In International Symposium on Information Management in a Changing World (pp.92-111). Springer Berlin Heidelberg.

H. Qian, J. He, Y. Zhou, and Z. Li, 7–9, 2010 "Cryptanalysis and improvement of a block cipher based on multiple chaotic systems," Math. Probl. Eng., vol. 2010, pp.

P. Gope and T. Hwang, 2015"Untraceable Sensor Movement in Distributed IoT Infrastructure," IEEE Sens. J., vol. 15, no. 9, pp. 5340–5348.

Singh "COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS", International Journal of Advanced Engineering Technology E-ISSN 0976-3945

2015.9.4.27 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.

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

AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram May-Jun2012 International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, pp.3033-3037.

NIST, (accessed Aug. 07, 2020) "What is AES Encryption and How Do it work?"Searchsecurity.techtarget.com.https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard.

R. Cordova, R. L. Maata, and A. Halibas, (2019) "BlowfishAlgorithmImplementation on Electronic Data in a Communication Network," 2019 Int. Conf. Electr. Comput. Technol. Appl. ICECTA, pp. 6–9, 2019,doi:10.1109/ICECTA48151.2019.8959702.