International Journal of Engineering Research and General Science Volume 5, Issue 2, March-April, 2017
ISSN 2091-2730

A Comparative Review Of Various Approaches To Ensure Data Security In Cloud Computing

Kiran, Sandeep Sharma
Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, India-143005
Email: kirangndu15@gmail.com , sandeep.cse@gndu.ac.in

Abstract— Cloud Computing is a rising field in the history of computing. The cloud computing is a collection of clouds that act as the large pool, inside which there are several, accessible and virtualized resources. These resources include hardware, development platforms. It provides gigantic storage for data and faster computing to customers over the internet. It shifts the database and application software to the large data centers, as a result management of data and services trustworthiness becomes a major problem. In existed cloud computing system there comes many security problems as number of organizations increases. So, cloud security becomes essential part for securing the data which resides on the cloud. This paper has presented a comparison between some well known data security techniques. The review has clearly shown that each technique has its own benefits and limitations. And none of each is perfect if we take security parameters into consideration.

Keywords— cloud computing, data security, cryptography, steganographic, survey.

INTRODUCTION

Cloud computing is an on-demand and self-service internet infrastructure that provides delivery of computing services. It is considered to be the combination of virtualization and automation. It separates the operating system from the physical hardware. User can pay for the services it wants form the cloud and it is also scalable as shown is fig-1. It can be divided into three major categories: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). It has deployment models: Public Cloud, Hybrid Cloud, Private Cloud, Community Cloud. Public Cloud can be accessed by everyone therefore a more secure mechanism is needed to secure it. E.g Amazon EC2, Google Cloud, etc. Private cloud is accessibility and services are provided by particular organizations. Hence, it is more secure than public clouds. Hybrid cloud which is the amalgamation of private and public cloud in which there are two sections: critical and non-critical activities. Critical activities are performed by private cloud and non-critical activities are performed by public cloud. These deployment models help organizations and businesses to secure user applications as well as cost benefits by keeping applications and shared data on the public cloud. [9]

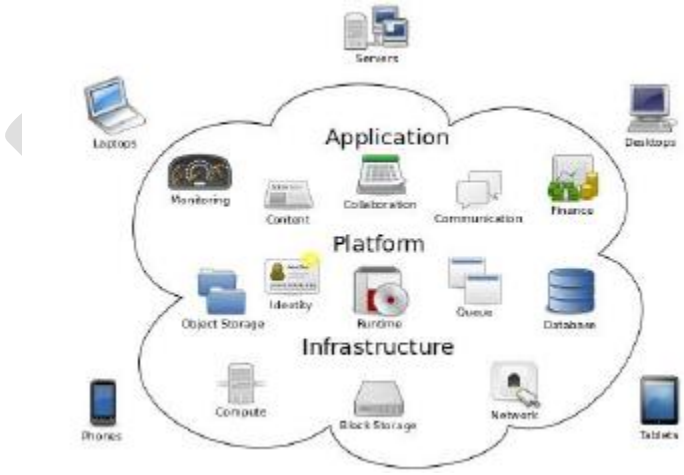

Fig-1 [10]
A general view of Cloud Computing

The cloud computing model has three functional units or components as listed below:

1. ***Cloud service provider:*** It is an entity which manages Cloud Storage Server (CSS). It has a large pool of storage space that preserves the clients' data. It has high computation power.
2. ***Client/Owner****:* it can either be classified as an individual consumer or organizations. It is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation.
3. ***User:*** It is a unit, which is register with the owner and uses the data of owner stored on the cloud. The user can be an owner itself as well.[1]

The distributed nature of cloud makes it a major concern about security and privacy. The Cloud Security Alliance's (CSA) emphasizes that cloud computing needs more security than traditional IT solutions. This is due to the fact that security responsibilities for both the service provider and consumer are different in deployment and delivery models. These security solutions need to address the three aspects of computer security: Confidentiality, Availability and Integrity [10]

1. ***Confidentiality:*** it ensures that the assets are accessed only by authorized parties. Only those have the access will actually get the access. For example: access of reading, viewing, modifying etc. this can also be called as secrecy or privacy. The encryption and cryptography techniques are the access control mechanism for preserving and supporting confidentiality in the Cloud.
2. ***Integrity:*** It means that modification can be only done by authorized parties or in authorized ways. Modification can be of any type like: writing, deleting, creating, changing, and changing status.
3. ***Availability:*** It means that assets are accessible to authorized parties at appropriate times. If some person or system has legitimate access to a particular set of objects, that access should not be prevented. For this reason, availability is sometimes known by its opposite, denial of service.[10]

We provide here an overview of cloud computing. The rest of this paper is arranged as follows: Section II introduces cloud data security issues; Section III describes scope of comparative study; Section IV discusses literature survey; Section V shows the comparison table; Section VI discusses gaps in literature survey; section VII describes conclusion and future scope.

CLOUD DATA SECURITY ISSUES

1. ***Threat from cloud service provider****:* The cloud stores the data after being transmitted by the owner. But data is not in the control of owner so CSPs can't be trusted blindly. By encryption of data stored at the cloud this problem can be solved. A certificate as used in the proposed model encrypts private communications over the public Internet. SSL consists of public and private keys for encrypting/decrypting the data, so that only the key owners can read the data. For example: 128-bit SSL encryption encrypts the data in such a way that attackers find it difficult to decrypt the data by brute force attack. [1]

2. ***Loss of user identity and password****:* For unauthorized access, authentication is needed in the cloud security system. Thus, if in any case the user losses or by mistake reveals his/her username and password to any unknown person, the data can be in leaked out. So to protect the data, another parameter is added to make data access in cloud. In this, the user will be asked a security question whose answer is known to the authorized user only, so the unauthorized user will not be able to hack the data. He must have given the correct answer to get the access to the data. Moreover, it is necessarily that the attacker must know the master key for decrypting the data that is received from the cloud. [1]

3. ***Performance Unpredictability:*** For large scale distributed systems, the performance unpredictability is a considered to be a serious problem. It is observed that virtual m/c can share CPUs and RAM quite well but cannot share the network and disk I/O. A better Operating System and architecture can help to improve these problems. And for improving performance Flash (semiconductor) storage should be used rather than mechanical disks. The cloud computing the scalable computation is well performed but there is still an open issue for scalable storage i.e., the ability to scale up or down on demand. [10]

4. ***Confidentiality:*** Data confidentiality becomes a major issue in cloud as user store their data applications on the cloud. User data is stored at remote locations and cloud infrastructures are used for storing backups, monitoring logs or servers. There is shared system where customers can share their data and applications. So sometimes there comes a problem of confidentiality because of malicious attackers, activities or system failures. So there must be powerful mechanism to secure, sensitive as well as less secure data.

5. ***Data Acquisition****:* To acquire data from different hardware we use a technique called data acquisition. For this the users and service providers should know some basic knowledge of data streaming and peer to peer operations to know from where and how we are accessing the data.

6. ***Multi-tenancy****:* Multi-tenant environment let multiple user access resources on the same physical machine. It is where cloud shares resources, networks, storage and services. It provides better utilization and is cost effective. Controlling the data and information becomes difficult when malicious attacker harms the network or system. For secure cloud researches are made to solve these problems.

7. ***Data Integrity and Authenticity:*** It means that modifications can be only done by authenticated parties or in authorized way and refers to data, software, and hardware. These include protecting data from unauthorized modification, deletion. Data integrity is difficult in cloud environment as cloud serves with multiple databases, servers, applications and networks. Authentication is act to control access of data and information. Only authorized users are allowed to access the data. As cloud is open environment so there comes problem of authorization and access of data.

8. ***Cyber-Attacks****:* We use the facilities provided by the internet as technology is growing day-by-day. But many security problems are also arising with it. Cyber-attack is one of them. In this malicious codes are used to change user data and information which results in harmful effects to data which leads to cybercrimes like information and identity theft, malware, phishing, spoofing, password sniffing, Denial-of-service(DOS) and distributes denial-of-services(DDOS) attacks, Trojans and viruses. [5]

Table 1: Represents the types of attack along with its description.

Table-1
Types of Attack [6]

Name of Attack	Description
Repudiation	Sender tries to refuse, or refute the validity of a statement or contract which is send by him/her.
Replay Attack	When an attacker or originator sends a valid data with intention to use it maliciously or fraudulently.
Elevation of Privileges	An attacker may access unauthorized to information and resources.
Viruses and Worms	Very common and well known attacks. These are piece of code that decrease the performance of h/w and application even these malicious codes corrupts files on local file system.
Identity Spoofing	It occurs when an attacker impersonates the users as the originator of the message in order to gain access on a network
Man-in-the Middle Attack	It occurs when an attacks infiltrates the communication channel in order to monitor the communication and modify the message for malicious purposes.
Differential Analysis Threats	When new versions are released, a differential analysis of the new and old version would indicate where difference in the code exists.
Eavesdropping Information Disclosure	It occurs when attacker gains access in the data path and gains access to monitor and read the messages.
Tampering	An attacker may alter information either stored in local files, database or is sent over public network.

SCOPE OF COMPARATIVE STUDY

Data security technique is still an open research in cloud computing and found to be challenging task in cloud research. Scope of comparative study is to improve the performance of various algorithms that are used in improving the data security. This paper has presented review of various data security techniques. The paper has clearly shown that each technique has its own benefits and

limitations over each other. Further, comparison of different research papers in the terms of technique used, its issues discussed, benefits and limitations have been shown in the comparison table. These techniques are as follow:

***RSA**:* It is the most recognizable asymmetric algorithm. And is a public key algorithm. RSA was created by Ron Rivest, Adi Shamir and Leonard Adleman in 1978. It uses two different keys for public/private key encryption and decryption. [9] User data is encrypted first and is placed on the cloud. When the user wants that data it is first checked for authentication. Only the authenticated user gets the access of the data. As RSA has private key which is known by the user and public key is known by all. The encryption is done at the cloud service provider side and the decryption is done at the user side. Once the data is encrypted with the public key, it can be decrypted with the corresponding private key only. [4]

AES: The AES stands for Advanced Encryption Standard. It replaces the DES algorithm. It supports on various small platforms and is fastest, secured and flexible. It is a symmetric-key block cipher algorithm. It has 3 fixed 128-bit block ciphers with cryptographic keys i.e. 128 bits, 192 bits and 256 bits. The size of the keys is unlimited and the block size is maximum upto 256 bits. [8]
DES: The DES stands for Data Encryption Standard which was developed in 1977 by National Institute of Standards and Technology (NIST). 64-bits is used for key size and block size in DES. In 1977 many attacks were found which makes DES as insecure block cipher. [8]

DES: The DES stands for Data Encryption Standard which was developed in 1977 by National Institute of Standards and Technology (NIST). 64-bits is used for key size and block size in DES. In 1977 many attacks were found which makes DES as insecure block cipher. [8]

***3DES**:* the 3DES was an improvement over the traditional DES algorithm. It was developed in 1998. It is similar to the DES but here we apply three times encryption level i.e. Three phase encryption. This makes it slower than other encryption block cipher methods. The block size and key size of 3DES is 64-bits and 192-bits respectively. As it takes more time to encrypt the data so, it is considered to be low in performance, consume more power and throughput is also low. [8]

***KP-ABE**:* It stands for Key Policy Attribute-Based Encryption. It is a public key cryptography primitive for one-to-many communication. Public components are defined for each attributes used in this algorithm. The encryption associates the set of attributes to the message by encrypting it with the corresponding public key components. An access tree over data attributes is defined by each user. If the data structure satisfies then only the user is able to decrypt a cipher text. [3]

PRE: a Proxy Re-Encryption is a cryptographic primitive in which a semi-trusted proxy is able to convert a ciphertext encrypted under Alice's public key into another ciphertext that can be opened by Bob's private key without seeing the underlying plaintext. [3]

LITERATURE SURVEY

In 2015, V. Pant et al. [5] discuss a mechanism for storing the data and information. Cryptography and steganography techniques are used in the paper. The 3 step data security model has been introduce to secure the cloud data. Firstly cryptography is used with RSA then stenography technique is used to hide the data and in final step the data is accessed by decrypting the data using RSA algorithm.

In 2012, SK. Sood et al. [1] proposed a mechanism to ensure security of data from owner of cloud to the user. For better results of security combined approach of MAC, classification of data and index and encryption is used. Also to protect the data check the integrity and authentication, the author has divided the data into 3 sections: index builder 18bit SSL encryption, Message authentication code and a double authentication of user by owner and other by cloud.

In 2013, P. Yellamma et al. [4] proposed RSA technique to provide data storage and security in cloud. In this paper first key is generated, then encryption, decryption is applied in virtual environment.

In 2016, A. Bhandari et al. [9] proposed a framework which considers the time and memory limitations with the help of AES algorithm and encrypting it with RSA algorithm. The aim is to preserve sender, receiver authentication, integrity and confidentiality. Error localization algorithms are also applied.

In 2015, A. Dhamija et al. [2] discuss a secure migration of data by combining cryptography and steganographic techniques. For cryptography process, we use simple technique of one's compliment SCMACS. For encryption, decryption symmetric keys are used. The main advantage of this approach is that it generates private key so that no one can gain the access to the data.

In 2013, Rewagad et al [6] They have proposed an architecture to protect confidentiality of data stored in cloud by making use of digital signature and Diffie Hellman key exchange with (AES) Advanced Encryption Standard encryption algorithm .Even if the key

in transmission is hacked, the facility of Diffie Hellman key exchange make it useless because key in transit is of no use without user's private key, which is provided only to the legitimate user.
In 2010, C. Wang et al. [3] discuss the problem of fine-grainedness, data confidentiality and scalability in cloud. The KP-ABE, proxy re-encryption and lazy re-encryption techniques are used. Moreover, the data owner can delegate most of computation overhead to powerful cloud servers.

In 2015, N. Surv et al. [8] presented a secured data mechanism to solve the data security problem in cloud. AES encryption and decryption scheme is used to make cloud users secure and to guarantee the privacy of their data.

In 2010, Somani et al. [7] In this RSA algorithm is used to ensure the confidentiality aspect of security whereas Digital signatures were used to enhance more security by authenticating it through Digital Signatures. The approach used carryout encryption in 5 steps. In first step, key is generated. In second step, digital signing is performed and in step 3 and step 4 encryption and decryption is carried out. In last step Signature verification is performed.

In 2012, Sherif et al. [12] discuss the main problem of data security. They presented the data security model of cloud computing based on cloud architecture. They use various encryption algorithms (RC4, AES, DES, 3DES, MARS) for analyzing the most suitable technique and determine its performance. The most suited software is applied in Amazon EC2 Micro instance for evaluation process.

In 2011, Prasad et al. [13] discuss a new approach for authentication. This 3-dimensional approach is capable of removing various existing problems like denial of services, data leakage etc. the technique is more flexible and capable to meet the rising demand of today's complex and diverse network.

In 2012, Volker et al. [11] presents a security architecture that enables a user of cloud networking to define security requirements and enforce them in cloud networking infrastructure. This allows various kinds of optimization, like reducing latency, network load, etc.

COMPARASION TABLE:

Table 2: Following are some of the details of literature survey paper which includes the published year of the paper, techniques names that is been used in the paper, the major issues that paper discussed followed by benefits and limitations that is been observed in the paper.

Table-2
Summary of data security models papers

Ref no.	Year	Techniques	Issues	Benefits	Limitations
[5]	V. Pant et al. (2015)	Cryptography, steganography	To tackle security problems	Provide security for image data	Algorithms are not robust, data hiding capacity poor
[4]	Yellamma et al. (2013)	RSA	To protect data from unauthorized attackers	Improve security of high potential data	Slow due to large mathematical computations.
[9]	A. Bhandari et al. (2016)	HMAC, RSA, AES	To design a secure framework	Searching is easy due to indexing, Study of various cryptography tech, Gives better execution of time.	Algo not proven mathematically, Time complexity is not given
[1]	SK. Sood et al.(2012)	Combination of MAC, classification of data indexing	Data leakage, modification, privacy of users confidentiality, etc	The combine tech provides better security than executing them individually, Better flexibility,	Time consuming

[2]	A. Dhamija et al. (2015)	Cryptography, steganography	Secure migration of data	Provides a multilayered protection to data, Less costly app.	Poor Implementation , Comparisons with other approaches not given.
[3]	Wang et al. (2010)	KBE, Proxy re-encryption, Lazy re-encryption	To remove heavy computational overhead when fine grained data	Achieve fine – grainedness, scalability, Efficient data sharing framework	User access privilege is not protected from the proxy server. Do not support User secret key accountability.
[6]	Rewagad et al.(2013)	Diffie hellman key exchange, AES	To protect confidentiality	Provide 3 way mechanism which is tough to crack	Time consuming
[8]	N. Surv et al. (2015)	AES	To ensure integrity in the network.	Fast, flexible, secured mechanism Support all types of data(text, audio, video, etc),	Too many keys to distinguish.
[7]	Somani et al. (2010)	RSA	To access cloud storage methodology and data security	Improves security of network	Slow technique, Not efficient for large for large data.
[13]	Prasad et al. (2011)	3 dimensional technique	To prevent denial of services and data leakage, etc	Flexible, capable to handle complex network problems.	Unencrypted data can be easily retrieved by unauthorized user.
[11]	Volker et al. (2012)	Security architecture for cloud networking	To preserve the security goals of service users	Allows various kinds of optimizations like reducing latency or network load.	Need for Extension of architecture by auditing techniques, More transparency is required for service users.
[12]	Sherif et al. (2012)	Various encryption algorithms (RC4,RC6, AES, DES, 3DES,MARS)	To implement various encryption techniques and analyzing them in cloud security	To implement software in enhancing cloud security and apply this s/w in Amazon EC2Micro instance.	Time consuming.

GAPS IN LITERATURE SURVEY

Subsequent section contains the various limitations in earlier techniques.

1. Existing techniques have not implemented mathematically to provide time complexity, security theorems and proofs.
2. Automatic classification of data is not done in previous methods.
3. More secure cryptographic algorithms should be used in combinations so as to provide confidentiality to user data.

CONCLUSION

Data security has found to be challenging task in cloud computing. This paper has presented a review on various data security techniques. The review has clearly shown that some each technique has it benefits and limitations. But none of technique is found to be effective in all cases. In future, the data classification will be implemented so that the user efforts in recognizing the category of data become less. This will help them in saving the time and more accurate results will come. Moreover, the more attention will be on users highly confidential data by combining different data security algorithms.

REFERENCES:

[1] Sandeep K Sood, "A combined approach to ensure data security in cloud computing", Journal of Network and Computer Applications 35(2012)1831-1838, Elsevier.

[2] V. Dhaka, A. Dhamija ," A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration", In International Conference On Green Computing and Internet of Things(ICGCIoT) (pp.1-6) IEEE,2015.

[3] S. Yu, C. Wang, K. Ren, Wenjing Lou, " Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE INFOCOM,2010.

[4] Yellamma P, Narasimham C, Sreenivas V, "Data Security In Cloud using RSA", In Computing Communication and Networking Technologies (ICCCNT), Fourth International Conference on 2013 july 4(pp. 1-6) IEEE,2013.

[5] V. Pant, J. Prakash, A. Asthana, " Three Step Data Security Model for Cloud Computing Based on RSA and Steganography Techniques", In International Conference On Green Computing and Internet of Things(ICGCIoT) (490-494) IEEE,2015.

[6] P. Rewagad, Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," In International Conference on Communication System and Network Technologies(ICCCNT), (437-439), IEEE,2013.

[7] U. Somani, K. Lakhani, M. Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", In 1st International Conference on Paralle, Distributed and Grid Computing (PDGC), (211-216), IEEE,2010.

[8] N. Surv, B. Wanve, R. Kamble, S. Patil, J. Katti, "Framework for Client Side AES Encryption Techniques in Cloud Computing", In International Advance Computing Conference (IACC), (525-528), IEEE,2015.

[9] D. Das, A. Bhandari, A. Gupta, "A Framework for Data Security and Storage in Cloud Computing", In International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), IEEE,2016

[10] N. Sinha, L. Khreisat, "Cloud Computing Security, Data, And Performance Issues", In Wireless and Optical Communication Conference (WOCC), (pp. 1-6), IEEE,2014.

[11] V. fusenig, A. Sharma, "Security Architecture for Cloud Networking", International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium, IEEE,2012.

[12] S. Etriby, E. Meslhy, H. Elkader, "Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing", In the third International Conference on Communications and Information Technology (ICCIT), 2012.

[13] P. Prasad, B. Ojha, R. Shahi, R. Lal, "3 Dimensional Security in Cloud Computing", In Computer Research and Development(ICCRD), IEEE,2011;3:198-208.