International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-12)

Research Article | **December 2015**

Technical Review on Security Issues & Cryptographic Algorithm in Cloud Computing

Rohit S. Bhore
Dept: CSE, M.Tech.,
R.C.E.R.T. Gondwana University
Maharashtra, India

Dr. Rahila Sheikh
Dept: CSE,
R.C.E.R.T. Gondwana University
Maharashtra, India

Abstract—

Data storage security refers to the security of your personal or official work on the storage media. Security has been a number one issue within the Information Technology space as a result of as users knowledge or work we have a tendency to don't wish anyone to use our data or hinder our privacy and as developers we have a tendency to don't wish anyone to use our work as their own. Range of users stores their data on Cloud Server and with passage of your time cloud computing grows in no time. Information should not be taken by the third party therefore authentication of consumer becomes a compulsory task. Security doesn't solely mean Arcanum protection or adding extra firewalls or hide the information. It additionally suggests that having complete information concerning your data or information i.e. wherever hold is on on-line or offline and who all read it. To safeguard from passive attacks the assorted cryptanalytic technique area unit used and hold on the encrypted data on cloud server. This paper is targeted on the safety problems with cloud computing. Before analyzing the safety problems, the definition of cloud computing and transient discussion to beneath cloud computing is given. Then discusses the part that has an effect on the safety of the cloud then mention inaccessible techniques or cryptographic algorithm to employed in cloud & propose the new theme for offer the safety to cloud storage.

Keywords— Cloud Computing, Cryptography Algorithms, Security, Data Storage, Data Integrity.

I. INTRODUCTION

In computer networking technology, cloud computing may be a part that is describe totally different computing ideas that contains number of computers system that hooked up through a time period communication network like web. The word "Cloud" is nonliteral to "Internet or Network". The cloud computing is web or network primarily based computing model wherever virtual shared server provides computer services, infrastructure, platform, devices and alternative resources. Cloud computing technology is growing quick with relevancy time in computing technology. Cloud computing delineated the data technology as a essentially various operative model that takes advantage of the maturity of internet applications and networks and therefore the rising ability of computing systems to supply IT services. Information security is turning into a basic obstruction in cloud computing. There square measure some sorts of resolution that square measure providing some security with model, some technology [1].

The design of the Cloud Computing involves multiple cloud elements interacting with one another regarding the varied knowledge they're holding on too, therefore serving to the user to induce to the specified knowledge on a quicker rate. Once it involves cloud it's a lot of centered upon the frontend and therefore the rear. The face is that the user needs the information, whereas the backend is that the various knowledge memory device, server that makes the cloud. There square measure numerous security problems whereas planning the cloud however necessary issue is knowledge security [1-2]. To shield our knowledge from the licensed users and that we don't need anyone to use our work as their own work. The cryptographic algorithms are method to encipher our work or data and store it on cloud.

The remainder of this paper is organized as follows: A brief review of Cloud Computing is given in section 2. Section 3 describes security issues in cloud computing. Section 4 proposed cloud computing security issues solution. In section 5 & 6 discussed & propose the scheme for cloud storage. Paper is concluded in section 7.

II. CLOUD COMPUTING

2.1. What is Cloud Computing?

Cloud computing is an industry transformation. Cloud computing enables businesses, of all sizes to deliver IT as a service, offering new possibilities to focus more on business success and less on operational costs and maintenance. There are many advantages a user can leverage from cloud computing [2]. They are listed as follows,

- Cloud computing user avoids capital expenditure on building up an infrastructure to support their application. Instead, they pay the provider only the amount they consume.
- The user need not invest on the maintenance of the Infrastructure of the application. The provider maintains the infrastructure for the user.
- The user can access the multiple data servers from any location at a go.
- Enhancement of the application is easy, as the user need not worry about the infrastructure enhancement.
- Cloud computing is an eco-friendly incentive which will replace the hardware components with services.

2.2. Cloud computing Features

Cloud Computing brings features that distinguish it from classical resource & service provisioning environments, they are as follows [2].

- *Highly Scalable*–Cloud computing provides resources and services for users on demand. The resources are scalable over several data centers.
- *Less capital expenditure*-Cloud computing does not require upfront investment. No capital expenditure is required. Users may pay and use or pay for services and capacity as they need them.
- *Higher resource Utilization* - Cloud computing can guarantee QoS for users in terms of hardware or CPU performance, bandwidth, and memory capacity.
- *Disaster recovery and Back up*
- *Device and Location Independence*
- *Maintenance* - Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.
- *Mobile Accessible*- Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

2.3. Cloud Computing Service Models

- *Software as a Service (SaaS)*- It is a model of package preparation whereby the supplier licenses an application to the purchasers to be used as a service on demand. The potential provided to the tip users is to use the provider's applications running on a cloud infrastructure [2]. The applications square measure accessible from numerous consumer devices through a skinny consumer interface like an online browser (e.g., web enabled e-mail). the tip users doesn't manage or management the underlying cloud infrastructure as well as network, servers, operational systems, storage, or perhaps individual application capabilities, with the attainable exception of restricted user specific application configuration settings. These days SaaS is obtainable by firms like Google, business department, Microsoft, Zoho, etc [3].
- *Platform as a Service (PaaS)*- It is the delivery of computing platform and resolution stack as a service [2]. The potential provided to the tip users is to deploy onto the cloud infrastructure user created or non inheritable applications created exploitation programming languages & tools supported by the supplier. The tip user doesn't manage or management the underlying cloud infrastructure together with network, servers, operational systems, or storage. PaaS suppliers provide predefined combination of OS and application servers, like WAMP platform (Windows, Apache, MySQL and PHP), LAMP platform (Linux, Apache, MySQL and PHP), and XAMP(X-cross platform) restricted to J2EE, and Ruby etc. Google App Engine, Salesforce.com, etc. square measure a number of the favored PaaS examples [3].
- *Infrastructure as a Service (IaaS)*- It is the delivery of pc infrastructure (typically a platform virtualization environment) as a service. the potential provided to the tip users is to provision process, storage, networks, and different elementary computing resources wherever the tip user is in a position to deploy and run whimsical code, which might embrace in operation systems & applications [2].The user doesn't manage or management the underlying cloud infrastructure however it's management over in operation systems, storage, deployed applications, and presumably restricted management of choose networking parts. A number of the common examples square measure Amazon, Go Grid, 3tera, etc [3].

2.4. Cloud Computing Deployment models

- *The Public Cloud*- Which describes cloud computing in the traditional mainstream sense; resources are dynamically provisioned on a self-service basis over the Internet. It is usually owned by a large organization (e.g. Amazon, Google App Engine and Microsoft Azure).This is the most cost-effective model leading to user with privacy and security issues since the physical location of the provider's infrastructure usually traverses numerous national boundaries [1].
- *The Private Cloud*- It defers from the traditional data enter in its predominant use of virtualization. It is a single tenant environment they have been criticized on the basis that users still have to buy, build, and manage them and as such do not benefit from lower capital costs and less hand on management. The private cloud is more appealing to enterprises especially in mission and safety critical organizations [1].
- *The Community Cloud*-Thus refers to a cloud infrastructure shared by several organizations within a specific community. It may be managed by any one of the organizations or a third party. A typical example is the Open Cirrus Cloud Computing Tested, which is a collection of Federated data centers across six sites spanning from North America to Asia [1-2].
- *The Hybrid Cloud*- It comprises of a combination of two (or all) of the three models discussed above. Standardization of APIs has lead to easier distribution of applications across different cloud models [1].

III. SECURITY ISSUES IN CLOUD COMPUTING

There are a unit varied security problems for cloud computing because it encompasses several technologies together with virtualization, resource allocation, dealings management, cloud networks, databases, operative systems, load equalization, concurrency management and memory management. The vital issue in cloud computing storage is knowledge privacy or defends our knowledge from unauthorized users. The cloud service supplier for cloud makes

certain that the client doesn't face any drawback like loss or data felony [4]. Cloud computing infrastructures use new technologies and services, most that haven't been totally evaluated with relation to security. The safety problems featured by cloud computing area unit mentioned below.

3.1. Security issues face by Cloud Computing

- *Data Access Control:* Generally confidential information will be illicitly accessed attributable to lack of secured information access management. Sensitive information in an exceedingly cloud computing surrounding emerge as major problem with respect to security in an exceedingly cloud based system. Information exists for an extended time in an exceedingly cloud, the upper chance of unauthorized access [4].
- *Data Integrity:* Data integrity includes the subsequent cases, once some human error occurs once information is entered. Errors might occur once information is transmitted from one laptop to another; otherwise error will occur from some hardware malfunctions, like disk crashes. Code bug or virus can even build viruses. Therefore at constant time, several cloud computing services clients and supplier accessed & modify information [5]. Therefore there's a desire of some information integrity methodology in cloud.
- *Data Theft:* Cloud computing uses external information server for price affection & versatile for operation. Therefore there's an opportunity of information will purloined from external server.
- *Data Loss:* Data loss may be a terribly major problem in Cloud computing. If banking and business transactions, analysis and development concepts are all going down on-line, unauthorized individuals are going to be ready to access the data shared. Albeit everything is secure what if a server goes down or crashes or attacked by a scourge, the complete system would go down & doable information loss might occur. If the seller closes attributable to money or legal issue there shall be loss of information for the client or user. Client won't bready to access those information as a result of data is not any additional obtainable for the customer [5].
- *Privacy Issues:* Security of the client Personal data is incredibly necessary just in case of cloud computing. Most of the server is external, that the seller ought to make certain that's well secured from alternative operators.
- *Security problems in supplier level:* A Cloud is sweet only there's a decent security provided by the seller to the shoppers. Supplier ought to build a decent security layer for the client and user. And may make certain that the server is well secured from all the external threats it's going to come upon [4].
- *User level Issues:* User ought to make certain that as a result of its own action, there shouldn't be any loss of information or meddling of information for alternative users who victimization constant cloud [4-5].

3.2. Data Storage Security in Cloud Computing

Cloud storage services may be accessed through a web service application programming interface (API), a cloud storage gateway or through a Web-based user interface. Cloud storage is:

- made up of many distributed resources, but still acts as one
- highly fault tolerant through redundancy and distribution of data
- highly durable through the creation of versioned copies
- Typically eventually consistent with regard to data replicas.

Data storage security refers to the safety of knowledge on the storage media, which suggests non-volatile or quick recovery once loss. This security ought to be taken into consideration by code engineers in style stage of cloud storage services. It includes not solely knowledge redundancy and dynamic, however additionally isolation. Redundancy is that the most simple measures to shield knowledge storage security, and dynamic suggests that user knowledge could typically modification, therefore effective measures square measure required to make sure knowledge consistency [6].

IV. AVAILABLE SOLUTIONS FOR CLOUD SECURITY ISSUES

4.1. Available Techniques for Provide the Security in Cloud Storage

The various techniques area unit out there for offer security in cloud computing and shield the cloud from higher than securities threats. These techniques area unit as follows:

- *Identity and access management guidance:* Identity and Access Management steering that provides an inventory of suggested best practiced to assure identities and secure access management. This report includes centralized directory, access management, identity management, role-based access management, user access certifications, privileged user and access management, separation of duties, and identity and access reportage [5].
- *Fragmentation Techniques:* this method consists in 1st breaking down sensitive information into insignificant fragments; therefore any fragment doesn't have any important data by itself [5]. Then, fragments are unit scattered in an exceedingly redundant fashion across totally different sites of the distributed system. Secret Encryption: Encryption techniques are used for long term to secure sensitive information. Causing or storing encrypted information within the cloud can make sure that information is secure. However, it's true presumptuous that the secret writing algorithms area unit robust. There is a unit some well known secret writing schemes like AES (Advanced secret writing Standard). Also, SSL technology is often wont to shield information whereas it's in transit. Moreover, described that secrete writing are offend wont to be stop facet channel attacks on cloud storage de-duplication, however it should cause offline lexicon attacks reveling personal keys[5-8].

- *Digital signatures:* It proposes to secure information victimization digital signature with RSA algorithmic program whereas information is being transferred over the web. They claimed that RSA is that the most recognizable algorithmic program and it are often wont to shield information in cloud environments [5].
- *Homomorphic encryption:* The 3 basic operations for cloud information area unit transfer, store, and method. Secret writing techniques are often wont to secure information whereas it's being transferred in and out of the cloud or keep within the provider premises. Cloud supplier has to be compelled to decipher cipher information so as to method it raises privacy consideration. They propose a way supported the applying of totally homomorphic secrete writing to the safety of clouds. Totally homomorphic secret writing permits acting arbitrary computation on cipher texts while not being decrypted. Current homomorphic secret writing schemes support restricted variety of homomorphic operations like addition and multiplication [10]. The authors in provided some real-world cloud applications wherever some basic homomorphic operations are a unit required. However, it needs a large process power which can impact on user interval & power consumption.
- *Web application scanners:* Web applications are often a straightforward target as a result of they are exposed to the general public as well as potential attackers. Web application scanner is a unit program that scans net application through the online front end so as to spot security vulnerabilities. There also are different net application security tools like net application firewall. Net application firewall routes all net traffic through the online application firewall that inspects specific threats [5-6].

4.2. Available Cryptographic Techniques for Provide the Security in Cloud Storage

Cryptographic method is one of the best ways to protect the user data in cloud server. In cryptography, the encryption techniques have been used for long time to secure sensitive data. Sending or storing encrypted data in the cloud will ensure that data is secure. The Cryptographic algorithm also protect the cloud from passive attack , for example user store the encrypted data in cloud server and suppose unauthorized user access the cloud and want to read data but data is in encrypted format so unauthorized user cannot read it. The various algorithms are used for encrypt the data in cloud computing is as follows:

- *Implementing DES Algorithm in cloud for data security*- This cipher block chaining system is to be securing for purchasers and server. The protection design of the system is meant by victimization DES cipher block chaining that eliminates the fraud that happens now a day with taken information. There's no danger of any information sent among the system being intercepted, and replaced. The system with coding is so-so secure, however that the amount of coding has got to be stepped up, as computing power will increase.

The algorithmic rule steps square measure follows.

1. Get the Plaintext.
2. Get the Password.
3. Convert the Characters into binary form.
4. Apply the Formula to get the encrypted and decrypted message.

In order to secure the system communication between modules is encrypted victimization even key. Although several solutions are projected earlier several of them solely think about one aspect of security: the author projected that the cloud data security should be through about to investigate the information security risk, the information security necessities, readying of security functions & also knowledge security method encoding [12].

Data Security in Cloud computing using RSA Algorithm- RSA algorithmic rule to code the information to produce security so solely the involved user will access it. The aim of securing information, unauthorized access doesn't enable. User information is encrypted initial and so it's hold on within the Cloud. Once needed, user places asking for the information for the Cloud supplier; Cloud provider authenticates the user and delivers the information. RSA may be a block cipher, within which each message is mapped to associate whole integer or number. RSA consists of Public-Key and Private-Key. Within the cloud, Public-key is known to any or all, where as Private-key is solely to the user that originally owns the information. Thus, cryptography finished by the cloud service supplier & decipherment is finished by the cloud user or client. Once the information is encrypted with Public-key, it may be decrypted with corresponding Private-key solely. [8-9].

Homomorphic Encryption Applied to the Cloud Computing Security- Homomorphic secrete writing system are wont to perform operation on encrypted data or information while not knowing the non-public key (without decryption), the client is that the solely holder of the key. Once the author decrypts the results of any operation, it's a similar as if they'd dispensed the calculation on the information. The cloud computing security supported totally homomorphic secrete writing, could be a new conception of security that allows providing result of calculation on encrypted information confidentiality. The author work relies on the appliance of totally Homomorphic secret writing to the cloud computing security considering analyse and therefore the improvement of the present cryptosystems to permit servers to perform varied operations requested by the client. To improvement of the complexness of the homomorphic secret writing algorithms and compare the reaction time of the requests to the length of the general public-key [10-11].

V. DISCUSSION

By analyzing and studding the assorted security problems in cloud computing, offered techniques and scientific discipline rule are two ways in which to produce the safety to cloud. However the scientific discipline rule is one best

thanks to shield the user information from passive attack in cloud. By analyzing the scientific discipline algorithms, the subsequent results generated. The subsequent table characteristic precedes the insecure problems. Thus we have a tendency to be victimization the effective authentication decides to give stronger security for each cloud suppliers and customers.

Table 1: Characteristics of existing Cryptography Algorithms use in Cloud

Characteristics	DES Algorithm	RSA Algorithm	Homomorphic Encryption
Platform	Cloud computing	Cloud computing	Cloud computing
Keys Used	Same key is used for encryption and decryption Purpose.	Different keys are used for encryption and decryption Purpose.	private key is used(without decryption)
Scalability	It is scalable algorithm due to varying the key size and Block size.	Not scalable	scalable decryption
Security applied to	Both providers and client side	Client side only	Cloud providers only
Authentication Type	Message authentication used	Robust authentication implemented	Authentication never used

VI. PROPOSED METHODOLOGY

The main contributions of this paper are as follows:

- We propose a novel scheme to provide the data security in cloud storage. In this scheme we will use the cryptographic algorithm for encrypt the data & stored it on the cloud server.
- We proposed the scheme which will the combination of fragmentation technique and cryptographic algorithm and provide the security to user mainly from passive attack and user safely transfer, store & share the data on third party cloud. The following fig. illustrates that scheme.

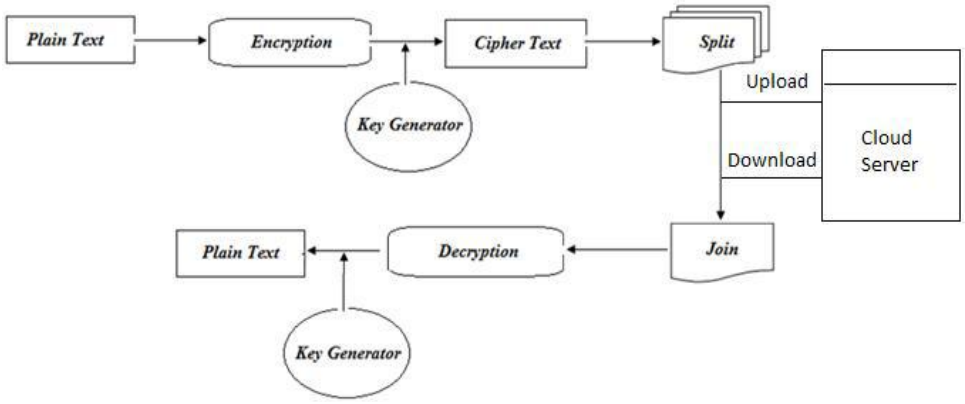

Fig 1: Proposed Methodology for Cloud Computing Storage

The Above scheme illustrate the propose methodology in which we will done the following operations.

1) First we take the data from user then apply the cryptographic algorithm on that data.
2) Then cipher text and key will generate.
3) Then we fragment or split the cipher text data into multiple part or we will done the same operation in vice versa manner i.e. first we split the file and encrypt the one of the part of the splited part.
4) The fragmented or splited parts will store on cloud.
5) When user wants the data, first download the files from cloud then join the file parts and by applying the key on cipher data we will generate the original data.

This scheme maintains the data security and also increases the strength of cryptographic algorithm that uses in cloud computing.

VII. CONCLUSION

In this review totally different quite cloud computing security problems are mentioned that exploit the protection system. From the entire survey, the notion of knowledge privacy is self-addressed that's not possible to take care of while not security and also the degree of trust afforded to a cloud service supplier is analyzed. Therefore it's needed for the cloud service suppliers to secure data transmission at cloud data centers. The various approaches are planned for security as mentioned in connected work. This paper analyses the importance of security to cloud. We tend to compared three algorithm particularly DES, RSA, Homomorphic secrete writing for information security in cloud. They're compared supported four characters; key used measurability, security applied to, and authentication kind. There on comparison basis we tend to planned the system which is combination of fragmentation technique & one in every of the cryptanalytic

algorithm that will be offer the protection to cloud & take away the disadvantage of exiting system This work are going to be extended for brand spanking new formula defend the prevailing work or provides a lot of economical results than existing ways in close to future.

ACKNOWLEDGEMENTS

We would like to thank Department of Computer Science & Engineering, RCERT Chandrapur for providing infrastructure and guidance to understand the security issues & cryptographic algorithm in cloud storage.

REFERENCES

[1] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "***Ensuring Data Storage Security in Cloud Computing***", Department of ECE, Cong Wang, Illinois Institute of Technology.

[2] "***Introduction to Cloud Computing Architectures***", white paper 1st edition June 2009 by Sun Microsoft Technologies.

[3] Pankesh Patel, Ajith Ranabahu, Amit Sheth, "***Service Level Agreement in Cloud Computing***", Knoesis Center, Wright State University, USA.

[4] Anitha Y, "***Security Issues in Cloud Computing-A Review***" International Journal of Thesis Projects and Dissertations (IJTPD), Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013.

[5] Keiko Hashizume1*, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1,"***An analysis of security issues for cloud computing***", Journal of Internet Service and Applications 2013(a SpringerOpenJournal).

[6] RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "**Design *of Privacy-Preserving Cloud Storage Framework***" 2010 Ninth International Conference on Grid and Cloud Computing.D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in SP '00: Proceedings of the 2000 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 2000, p. 44.

[7] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"**Comparison *of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures***" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[8] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. M. Lee, G. Neven, P. Paillier, and H. Shi. "***Encryption Revisited: Consistency properties, relation to anonymous IBE, and extensions***". In V. Shoup, editor, Advances in Cryptology CRYPTO '05, volume 3621 of Lecture Notes in Computer Science, pages 205{222. Springer, 2005}.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In P. Ning, S. De Capitani di Vimercati, and P. Syverson, editors, ACM Conference on Computer and Communication Security (CCS '07).ACM Press, 2007.

[10] G. Ateniese, S. Kamara, and J. Katz. "***Proofs of storage from homomorphic identification***". In To appear in Advances in Cryptology ASIACRYPT '09, Lecture Notes in Computer Science. Springer, 2009.

[11] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik. Scalable and e_cient provable data possession. In Proceedings of the 4th international conference on Security and privacy in communication netowrks (SecureComm '08), pages 1{10, New York, NY, USA, 2008. ACM.

[12] J. Baek, R. Safavi-Naini, and W. Susilo. "***On the integration of public key data encryption and public key encryption with keyword search***".In International Conference on Information Security (ISC '06), volume 4176 of Lecture Notes in Computer Science. Springer, 2006.

