ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
August 2014,
Vol. 7, No. (2):
Pgs. 297-302

Multi Layer Security System for Cloud Computing

SYED MINHAJ ALI and ZUBER FAROOQUI*

Department of Computer Science & Engineering, ASCT
RGPV University, Bhopal, India.

(Received: August 15, 2014; Accepted: August 30, 2014)

ABSTRACT

Cloud computing is an up-and-coming architecture with strengths and room for improvement. Cloud computing is an extension of grid computing and distributed computing, which is a software concept indeed, it works through variety of technologies such as software technologies, integration, management, and the use of various hardware resources. The progress of cloud computing for information processing creates significant technological opportunities and economic benefits. Many organizations and individuals will use cloud platform as data storage and in the mean times as their publishing environment, i.e. public and private clouds can be combined into a hybrid cloud. Cloud storage is an important part of cloud computing, which is used to achieve the target of storing data in the cloud. In our this research work researcher tries to deal with problem of security of store data in a Cloud Computing provider which would be handle by ensemble cryptography methods.

Key words : Cloud Computing, Data Security, Cryptography, Ensemble.

INTRODUCTION

Cloud computing is well-known for its pay-as-you-go utility computing and provides applications with access to large-scale cluster resources initiated by Google, IBM, Microsoft, Amazon and National Science Foundation (NSF) etc[1]. It supplies an easy-deployment, low-energy and wide distributed computing environment.

Cloud architectures are designs of software systems for enabling on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[2] Typically a cloud architecture abstracts away system level details for the user, leaving the user with a parallel black-box to program in. While this eases the difficulty of high performance computing, it sometimes leaves users clueless as to what is actually happening behind the scenes, especially when breach comes for security of storage data.

Cloud storage is an important part of cloud computing, which is used to achieve the target of storing data in the cloud. The network cloud disk, which is popular in recent years, is one of the ways to realize the target. Logged users can store data in the cloud in a browser without any additional storage media, and the user can obtain the data wherever they are by ordinary computers,

mobile phones, laptop, iPad, etc .Cloud disk can make the storage simple, fast, and convenient, but the users are not allowed to upload confidential data for security reasons. Security problems restrict cloud disk from making progress and development. The security problems of cloud disk are not only the traditional problems but also new problems in cloud computing[3] Described the security threats and challenges of the cloud computing with its three basic patterns (Saas, Paas, Iaas)[4, 5, 6] Analyzed and summarized the threats being faced from different aspects. Cloud disk's weak security mainly occurs in the following aspects:

a. Transmission security: data in transmission process may be intercepted, but the data transmission is not working with the strong encryption protection measures.
b. Access control: access control authority is weak, the user data stored in the clouds without setting access authority, the user lost absolute right to monitor.
c. Data storage: user upload data after the clouds, it is likely to be distributive stored, users do not know the specific position where the data is stored. And the confidential data and non-confidential data stored is not classified, which may cause the leakage of data.
d. Data verification: the cloud makes no verification and inspection on the data uploaded. It can't guarantee that the uploaded data is corresponding to the right user's data or the original data from the user.

To solve the existing security problems, There are so many solutions.

The remainder of the paper is organized as follows. In Section II, Researchers briefly overview about the Cryptography and in Section III, Researchers briefly overview about Cloud Security. Section IV talks about literature review. Researchers Propose a model of Data Security in Section V, Finally Section VI concludes the paper.

Cryptography: security technique

Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with.

Cryptography is the science of writing in secret code and is an ancient art, the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any entrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals:

a. Secret key (or symmetric) cryptography
b. public-key (or asymmetric) cryptography and
c. Hash functions.

Each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party.

In the process of encryption and decryption there are various parameters which have to be taken into consideration:

- Authentication: In the process of authentication process it is checked that weather the Sender of the message is authentic or not.
- Confidentiality: The secret of the encoding the message is kept constant and the message is not accessible to any third user.
- Integrity: Integrity means no data in the message has been altered in data/ message passage.
- Non-repudiation: It means the authentic information to prove that the sender has sent the message. Digitized proof for this pre requisite is very necessary.

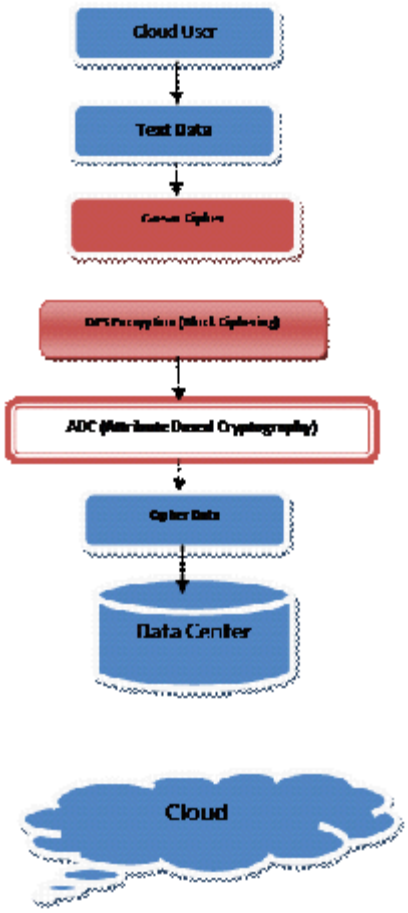

Fig. 1: ABC based Double Layer-Authenticated-Secure Method for data security in Cloud Environment

Cloud security

For good measure the traditional data and communication security, cloud computing data brings on new security threats and precautions. This are discussed below.

Availability

Service Level Agreement (SLA) is a trust between provider and consumer to define maximum time for which resources or applications may unavailable for use[7,8,9]. Because this agreement formalizes the relationship between cloud users and cloud service provider, it must arrange very carefully. An ideal way to reduce unavailability of resources because of a breakdown or an attack is to have backup to protect critical information. In this way consumer's information is available offline[10]. Besides, provider should serve monitoring and notification systems to known instant by consumer.

Integrity

Protecting data from deletion, modification or production without permission is possible with incident response and remediation, fault tolerance, failure recovery and disaster recovery[11]. Furthermore, digital signature is able to data integrity testing and recovers from corruption[12].

Confidentiality

Claiming confidentiality of users' data, allows for security protocols and proper encryption techniques to be enforced at different layers of cloud applications. Also customers can encrypt their information prior to uploading to cloud[11]. Because confidentiality is correlated to authentication, protecting a user's account is the same as controlling access to cloud objects[13]. In addition, the biometric authentication features may connect to anti theft and identity protection features in cloud security.

Trust

In cloud environment trust mostly depends on the selected deployment model according to audit of data and applications are outsourced[11,14]. Organizations must know how to act these situations: how to describe and improve it, how to handle malicious information,

how to consider and ensure different security level of service according to the trust degree and how to manage trust degree change with interaction time and context[15,16]. Another situation, Trusted Third Party (TTP) relationships should rely upon for confidentiality, authentication and authorization[17].

Privacy

Privacy protection mechanisms must be embedded in all security solutions. For the use of encryption process, to store keys of on only either provider or consumer side enhances security, additively customer can encrypt their information prior to uploading to cloud[10,11]. Cloud presents lots of legal challenges towards privacy issues involved in data stored in multiple locations[17]. Because of the changing legal requirements according to country which is hosting servers, organizations should know where their data at all times[18]. Security management operations should involve all security requirements, feedback from environment, policies and standards like Electronic Communications Privacy Act (ECPA), Statement on Auditing Standards 70 (SAS 70), Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), ISO/IEC 27001 and 27002 Cloud Survey Report [19,20,21].

Various methods

There are various methods which are already developed for the security of the data storage. Some oth those are discussed here.

The Cloud Multiple-Tenancy Model

Multiple-tenancy allows multiple applications of cloud service providers currently running in a physical server which partitions and processes different consumer demands with virtualization to offer cloud service for consumers[22]. Although virtualization enables to isolate fault, breach, virus, and malicious applications, this model includes technology difficulties of architecture broadening, data isolation, configuration and performance customization.

Cloud Cube Model

Cloud Cube Model by Jericho is a figuration description of security with feature of internal/external, proprietary/open, perimeterised/ deperimeterised and insourced/outsourced. If providers define clearly security controls and implements for consumer, consumer knows security requirements visually, correct decisions and outcomes acquired[22].

Sood's Combined Approach

A framework proposed that consists of different procedures and techniques to protect data by Sood[23]. Confidentiality, availability and integrity parameters for cryptography plus Message Authentication Code (MAC) for checking data integrity is used in this process. The technique provides confidentiality, integrity, authorization, authentication, non-repudiation and prevents data leakage. The security degree that they provide in ascending order is MAC, classification of data and implementation of index and encryption technique.

CCMDSM

Cloud Computing Multi-dimension Data Security Model (CCMDSM) involves three layers with blocks, chunks and matrix structures[23]. First layer manages users' authentication and permission. Second layer protects users' data via encryption and last layer regenerates data. Notwithstanding its performance, privacy and safety advantages, this solution is not widely accepted.

proposed framework for data storage security

Here after study of various data storage security methods, researcher is proposing hybrid method for the same with following features:

1. Stream Ciphering with Hashing
2. Block Ciphering with Encrypted Key
3. ABC (Attributed Based Cryptography)

CONCLUSIONS

The cloud computing became a hot topic in industry, academia and government services with the development of technology. In this paper we discussed cloud computing properties, security issues and security models. By focusing more on security, privacy and policies cloud computing can be best applicable information technology solution.

The articles in the literature about cloud computing security are examined from different perspectives and assumptions or proposed new security models. However, the academic literature and the business environment need to real life implemented applications or systems and their security analysis. As a subsequent work, researchers plan to compose a more elaborate based Double Layer-Authenticated-Secure Method for data security.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, *et al*. A view of cloud computing. *Communications of the ACM,* **53**(4):50–58, 2010.
2. B. E. and G. Timothy, "The NIST definition of cloud computing," in National Institute of Standards and Technology (NIST). U.S. Department of Commerce, 2011, pp. 1–7.
3. MUNIER M.Self-Protecting Documents for Cloud Storage Security[C].Trust, Security and Privacy in Computing and CommuÿLiverpool,1231-1238 (2012).
4. SHAIKH F B. Security threats in cloud computing[C].Internet Technology and Secured Transactions (ICITÿAbu Dhabi, 214-219 (2011).
5. Security of Cloud Computing Providers Study," Ponemon Institute,(2011).
6. V. Winkler, "Securing the Cloud Computer: Security Techniques and Tactics," *Elsevier Inc.,* ISBN: 978-1-59749-592-9, (2011).
7. F.B. Shaikh, S. Haider, "Security Threats in Cloud Computing", Internet Technology and Secured Transactions, Abu Dhabi, 214-219, (2011).
8. Y. Demchenko, T.W. Wlodarczyk, W. Ziegler, "Security Infrastructure for On-demand Provisioned Cloud Infrastructure Services", *Cloud Computing Technology and Science, Athens,* 255 –263, (2011).
9. B.R. Kandukuri, R.V. Paturi, A. Rakshit, "Cloud Security Issues", *Services Computing*, Bangalore, 517-520, (2009).
10. A. Behl, K.Behl, "An Analysis of The CloudComputing Security Issues", *Information and Communication Technologies* (WICT),Trivandrum, 109-114, (2012).
11. H.Tianfield, "Security Issues In Cloud Computing", IEEE International Conference on Systems, Man, and Cybernetics, COEX, Seoul, (2012).
12. W. Liu, "Research on Cloud Computing Security Problem and Strategy", Consumer Electronics, Communications and Networks (CECNet), Yichang, 1216-1219, (2012).
13. A. Bhardwaj, V. Kumar, "Cloud Security Assessment and Identity Management", Computer and Information Technology (ICCIT), 387 – 392, Dhaka, (2011).
14. M. Mackay, T. Baker, A.Yasiri, "Security-oriented cloud computing platform for critical infrastructures", Computer Law & Security Review, 28, 679-686, (2012).
15. D.Sun, G. Chang, L. Sun, X. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", *Procedia Engineering,* **15**, 2852 –2856, (2011).
16. L. Xiao-hui, S. Xin-fang, "Analysis on Cloud Computing and its Security", The 8th International Conference on Computer Science & Education (ICCSE 2013), Colombo, Sri Lanka, 839-842, (2013).
17. D. Zissis, D. Lekkas, "Addressing cloud computing security issues", *Future Generation Computer Systems,* **28**, 583–592, (2012).
18. N.J. King, V.T. Raja, "Protecting the privacy and security of sensitive customer data in the cloud", *Computer Law & Security Review,* **28**, 308-319, (2012).
19. M.A. Morsy, J.Grundy, I.Müller, "An Analysis of The Cloud Computing Security Problem", In Proceedings of APSEC Cloud Workshop, Sydney, Australia, (2010).
20. W. Liu, "Research on Cloud Computing Security Problem and Strategy", Consumer Electronics, Communications and Networks (CECNet), Yichang, 1216-1219, (2012).
21. S. Sengupta, V. Kaulgud, V. S. Sharma, "Cloud Computing Security - Trends and Research Directions", Services (SERVICES),

Washington, 524 – 531, (2011).

22. J. Che, Y. Duan, T. Zhang, J. Fan, "Study on the security models and strategies of cloud computing", *Procedia Engineering,* **23**, 586–593, (2011).

23. S.K. Sood, "A combined approach toensure data security incloud computing", *Journal of Network and Computer Applications,* **35** (6), 1831-1838, (2012).