IJCSN International Journal of Computer Science and Network, Volume 5, Issue 1, February 2016
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

Secure Data Storage Scheme Using Cryptographic Techniques in Cloud Computing

[1] Rohit Bhore, [2] Dr. Rahila Sheikh

[1,2] Department C.S.E.(M.Tech.), R.C.E.R.T. Gondwana University.
Chandrapur, Maharashtra 442401, 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 user's knowledge or work. 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 numbers of 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. Before proposed the scheme, the definition of cloud computing and transient discussion to beneath cloud computing is given. Then discusses 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, Client MAC ID.*

1. Introduction

Nowadays Data Security is a major field in Networking. Data security has been a leading issue in the Information Technology arena because as users we don't want anyone to hinder our privacy and as developers we don't want anyone to use our work as their own. Data Security does not only mean password protection, data hiding or adding additional firewalls it also means having complete information about your data i.e. where is your data kept and who all view it [1]. The Cryptographic Cloud Computing and Storage has two basic parts i.e. Cryptography and second one is Cloud or Network Storage. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. And the term "Cloud" is analogical to "Internet"[4]. The cloud computing is Internet based computing where virtual shared server provides software, infrastructure, platform, devices and other resources. We consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. We describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal [1].

The remainder of this paper is organized as follows: the introduction about the security in networking & cloud computing. The definitions & features about Cloud Computing is given in section 2. Section 3 describe the proposed architecture for cryptographic cloud computing & storage. Section 4 is analyzing the result of proposed scheme. Paper is concluded in section 5.

2. Cloud Computing

In computer networking technology, cloud computing 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 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 [2].

2.1 Cloud Computing Features

- ✓ Highly Scalable–Cloud computing provides resources and services for users on demand. The resources are scalable over several data centres.
- ✓ 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 quality of service 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 [3].
- ✓ Mobile Accessible- Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere

2.2 Cloud Computing Service Model

2.2.1 Software as a Service

It is a model of software deployment whereby the provider licenses an application to the customers for use as a service on demand. The end users do not manage or control the underlying cloud infrastructure including storage, or even individual application capabilities & Configurations.

2.2.2 Platform as a Service

It is the delivery of computing platform. The end user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

2.2.3 Infrastructure as a Service

It is the delivery of computer infrastructure as a service. IaaS delivers computer infrastructure typically a platform virtualization environment as a service. Fundamental computing resources where the end user is able to deploy and run arbitrary software, which can include operating systems and applications

2.3 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. Proposed Architecture

We proposed the new scheme for providing the security to cloud storage users which is based on two techniques. First is the cryptography, that we used the DES algorithm for encrypting the user data. User can provide the any file format as input for encrypting the file [6]. And second one is split the encrypted file into multiple parts & add client MAC ID to which we share the data or file as authentication key to one of split part of file.

We proposed the new scheme in which we bind the MAC ID of client system to application database and also update that ID to cloud server. This MAC ID is used as the Authentication Registered Key that we added in split parts of file to which we want to share the data. The advantage of that authentication key as the unauthorized person can't join that file until and unless it verify with client system MAC ID. Also we bind the MAC ID of client system with application database so user does not share that application with other users. For security purposed we concoct the MAC ID with some string and performed the reverse operation on it. So it is hard to identify the MAC of client system for hackers.

3.1 Proposed Database Architecture

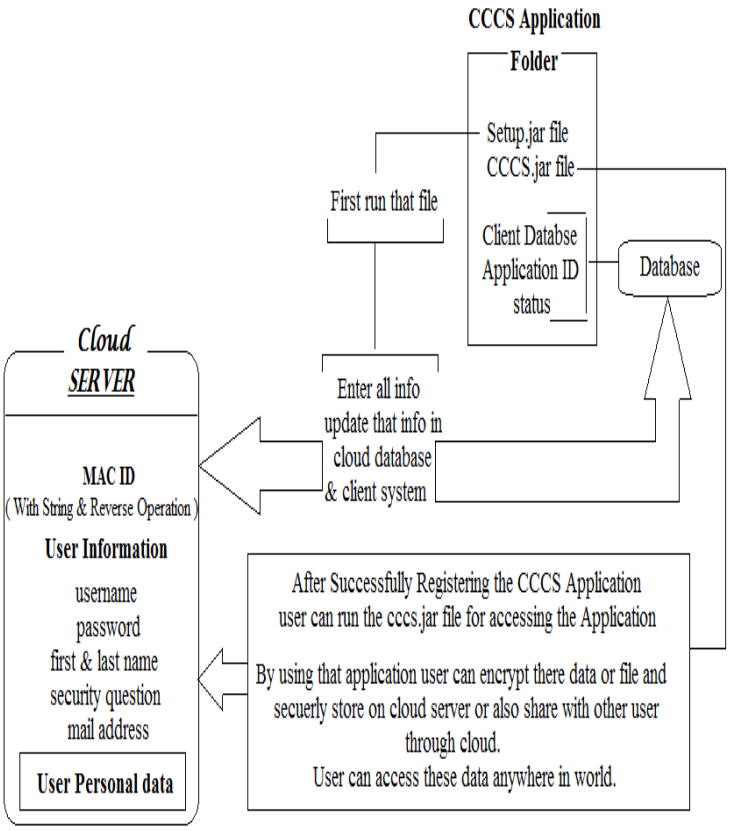

Fig 1 Proposed Cloud Database Structure

The above fig described the proposed Cloud Database Architecture in which we maintained the client information in Cloud Server. First we provide the application folder to client on cloud. User need to download that folder for registering the username/password for accessing that application. In

application folder there are total four files; CCCSApp.jar and Setup.jar are the java executable files. And one is lib folder which contains the libraries and other one is data folder which used to store the MAC ID of the client system.

At first user need to run the Setup.jar file for installing & registering with the cloud database. Once user run the setup.jar file client MAC ID is bind with application database & also with cloud database. After that user need to fill all the required information for registering with application. After successfully installation user can access the CCCSApp.jar file for accessing the Application.

Here we bind the MAC of client system so user does not share the application with other users.

3.2 Proposed Scheme

Here we proposed the novel scheme which is the combination of cryptography and fragmentation technique with authentication. The following Fig. described the proposed scheme for cryptographic cloud computing & storage. For using that application user need to registered and create the new username/password by running the setup.jar file. User need to enter new username and password in login window and click on login button for access the application.

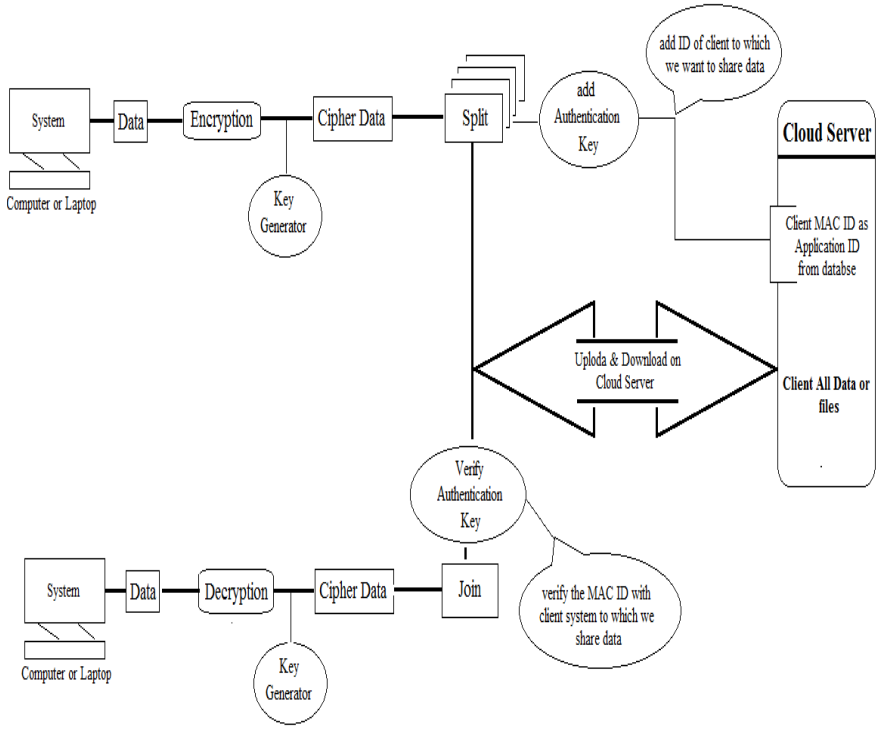

Fig 2 Proposed Architecture for Cryptographic Cloud Computing and Storage

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

1. At first we can encrypt the data using DES algorithm (Data Encryption Standard) and also generate the key which is used to decrypt that data.
2. After that user can convert that cipher data into bytesize or split (Fragment) into multiple parts. When we convert any file into bytesize or split the file, it is in the unreadable format i.e. it also used as the cryptography technique which is used with the DES Algorithm that increased the strength of that algorithm.
3. After that we add the authentication key i.e. MAC ID of the client system that user wish to share the data. The authentication key is choosing by the user from cloud server where all registered user MAC ID are available. User simply needs to choose the client name from which MAC ID of that client is added as authentication. No one can identify that MAC ID's because at the registration time we add some string with that MAC & performed the

reversed operation on that and stored it into cloud server. In somewhat conditions if unauthorized user successfully accesses that cloud database, it's difficult to identify that MAC ID of client systems.

4. After authentication user share that file or data to on cloud server. ***We done the same operation in vice-versa manner i.e. first split the original file & add authentication then encrypt one of the parts of spited file.***

5. To get the original data we done the same procedure in reverse order i.e. first download that data files then verify the authentication with client MAC ID, after successfully authentication spited parts of file are joined. After that using the DES key we decrypt the data and get the original file which is in readable format.

Here proposed the novel scheme for cloud storage which provides the security and authentication to cloud users. And it also increased the strength of cryptographic algorithms.

4. Result & Discussion

The results of the proposed scheme for cryptographic cloud computing & storage are summarized in Table 1 which shows a summary of the topics and concepts considered for each approach. As it is shown in Table 1, most of the approaches discussed identify, classify, analyze, and list in below table. 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: Result & Discussion for Proposed Architecture

Characteristics	***Exiting Scheme***	***Proposed Scheme***
Platform	Cloud computing	Cloud computing
Keys Used	Same key is used for encryption and decryption Purpose.	Same key used for encryption & decryption but additional authentication key is used
Scalability	It is scalable algorithm due to varying the key size.	It is scalable scheme due to varying the key size and used of different keys for authentication.
Security applied to	Both providers and client side	only from providers side
Authentication Type	Key authentication used	Key authentication and client MAC ID authentication is used
Security	Single encryption used	Double encryption and authentication also used

5. Conclusions

In this paper we discussed the proposed architecture for cryptographic cloud computing & storage. On that discussion we developed the novel scheme which is the combination of fragmentation technique (Split & Join) and cryptographic algorithm (DES) which is remove the drawbacks of previous architecture. The Proposed scheme provides the security on cloud server as well as a single client or user which stores the data on their computer system. This scheme also used authorization for user identity, so it increases the security of user data and the application. Our scheme was developed to reduce the computational and storage overhead of the client as well as to minimize the computational overhead of the cloud storage server.

Acknowledgments

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 Springer Open Journal).

[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.