INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

CRYPTOGRAPHIC CLOUD COMPUTING AND STORAGE

ROHIT S. BHORE[1], DR. RAHILA SHEIKH[2]

1. Dept.: CSE, M. Tech., C.E.R.T. Gondwana University.
2. Dept.: CSE, C.E.R.T. Gondwana University.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: 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. Data storage security refers to the security of your personal or official work on the storage media. 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. In this paper, we proposed the new architecture for providing the security to cloud data of users. Before proposed the architecture, the definition of cloud computing and transient discussion to beneath cloud computing is given. Then discusses cryptographic algorithm to employed in cloud & propose the architecture for offer the safety to cloud storage.

Keywords: Cloud Computing, Cryptography Algorithms, Security, Data Storage, Client MAC ID.

Corresponding Author: MR. ROHIT S. BHORE

Access Online On:

www.ijpret.com

How to Cite This Article:

Rohit S. Bhore, IJPRET, 2016; Volume 4 (9): 265-272

PAPER-QR CODE

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 analysing 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.

1. 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 [2].

1.1. 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 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 [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.

3. Architecture For Cryptographic Cloud Computing & Storage

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

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 Registered

Authentication 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 registered user MAC ID on cloud. 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 Application Database Architecture –

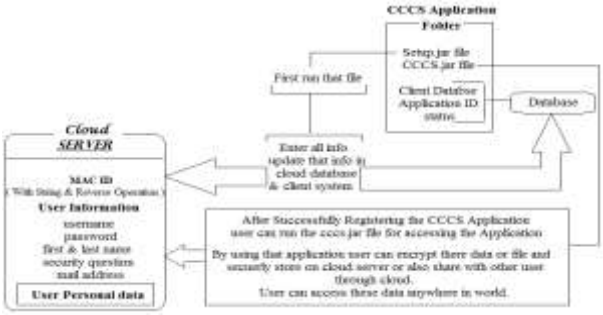

Figure1. Application Database Structure

The above fig described the Application Database Architecture in which we maintained the client information on Cloud Server. First we provide the application folder to client on cloud. User need to download that folder. In application folder there are total four contents;

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. User need to fill all the required information in registered window for registering with application on cloud. After successfully installation user can access the CCCSApp.jar file for accessing the application.

3.2 Architecture of Cloud Storage Service-

Here we proposed the novel scheme which is the combination of cryptography and fragmentation technique with authentication. The following Fig. described architecture 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. After that user need to run the CCCS.jar file and enter new username/password in login window for accessing the application. The user has only three chances for entering the correct username/password, after 3rd attempt the user system shutdown automatically and in client system database set status =1. When user login next time, it shows the message of "someone trying to access the account" and you need to

change the password for accessing the application and when user change the password successfully, the status in client system database is again set to 0.

The user can access their account on other system, it first check for MAC ID of system if user is registered but MAC ID is not matched then the One time Password (OTP) is send on user registered mail. The user simply enters that OTP in authentication and access the application.

The below figure illustrates the architecture for cryptographic cloud storage in which we will do the following operations.

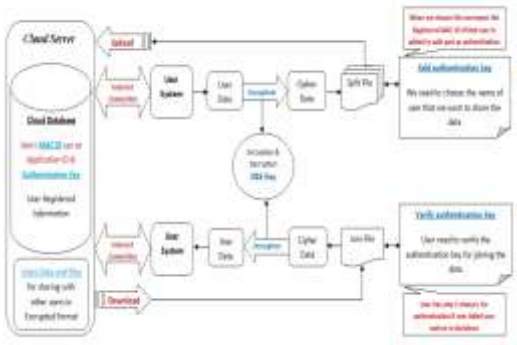

Figure 2. Architecture of Cryptographic Cloud Computing and Storage

1. At first we can encrypt the data using DES algorithm (Data Encryption Standard) and also generate the key which is used to decrypt the same data. Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data [8].

2. After that user can split (Fragment) the cipher (encrypted) data into multiple parts. When we convert any file into byte-size 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 DES algorithm. For split the data into multiple parts we simply used the formula that split the given file into multiple parts.

Split File = Byte Size * 1024 * 1024;

The Bytesize is variable which contain the user specified value for split the file in particular size. For ex- if Bytesize is 2 and given file size is 5 MB then it split the file into 3 parts in which 2 files has 2 MB size and remaining one is of 1 MB size i.e. total of 5MB.

3. After that we add the authentication key i.e.

MAC ID of the client system that user want 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 MAC and stored it on 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, all parts of file are zipped in folder then user can share that 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 will done the

same procedure in reverse order i.e. first download that data from cloud server then verify the authentication key with registered client MAC ID, after successfully verification, 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.

6. Here we provide the option to user that they can share the file with all users or with the particular user. If they share the file with particular user then the registered MAC ID is added to file as authentication or if user share file with all users then the own user MAC ID (the user which share the data) is added as authentication key in file. The user has only two chances to verify the authentication key, if it failed to authenticate then after two consecutive attempts the user system is shutdown automatically.

Here we developed the novel scheme for cloud storage which provides the security and authentication to cloud users. It prevents the users from passive attack.

IV. Benefits of Cryptographic Cloud Storage Scheme

1) The main advantage of cryptographic cloud computing & storage, it maintains the privacy and security of user data. In that architecture we encrypt and also add the authentication that provide the stronger security to user on cloud

2) By using cloud storage, improving data storage capacity and processing power. It reduces the chance of losing data by hardware failures. It also maintains the user data integrity and reliability data.

3) By using the concept of splitting and add MAC ID as authentication key it increases the security of user personal files and also increase the strength of DES algorithm.

4) By adding the client MAC ID as authentication, only particular user/ client can read that file.

5) The fragmentation technique can maintain the reliability of data and it easy to transfer that file on cloud server.

V. Disadvantages of Cryptographic Cloud Storage Scheme

1) This scheme is totally based n cloud computing, so it continuously required high bandwidth internet connection.

2) We used the fragmentation technique in which the data is split into multiple parts, so it is difficult to handle that multiple parts. If one of the parts is loss then file does not join.

VI. Result and 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.

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

Table 1: Result & Discussion for Developed Architecture

CONCLUSION

In this paper we discussed the developed 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 and authentication on cloud server. 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 servers.

ACKNOWLEDGEMENT

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. And help to develop the new scheme Cryptographic Cloud Computing & 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.
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.