Trusted Third Party Authentication in Cloud Computing

Susmita J A Nair[1] , Anitha K L[2], Rosita F Kamala[3]

Assistant Professor, [1,2,3] Department of MCA,
Acharya Institute of Technology, Bangalore - India

Abstract

Cloud computing is an emerging approach in the field of distributed computing that provides web based services, computation and storage for the community(including business, healthcare and government). The customers are offered dynamically scalable resources and thus the cloud users are economically benefited to a large extent. However, security is a huge concern for cloud user. Some of the areas of security concern in cloud computing are: stored data, data during transmission, user authentication etc. In cloud environment anyone can access the data over the internet. Hence user authentication and access control is very important in the cloud. Trusted third parties are independent service providers and are assumed to have a certain level of trust. The trusted third party facilitates secure communication between two parties who trust this third party. The cloud service providers have the control of the user data and the computational resources. The trusted third party ensures the integrity of the stored data.

Index Terms: Trusted Third Party, Cloud Service Provider, Authentication Check

1. INTRODUCTION

Cloud computing provides internet based services on a utility basis to the business process. The tenants share a pool of resources that are dispersedly owned and managed. Hence security is a major concern in the cloud environment. The consumers will loss the control of data in the cloud environment and hence a proper trust mechanism is necessary to ensure data security and privacy [1]. As the cloud computing is composed of different local systems and includes the members from multiple environments, therefore the security in cloud is complicate. In one side, the security mechanism should provide guarantees secure enough to the user, on the other side, the security mechanism should not be too complex to put the users into an inconvenient situation. The openness and flexibility of the computer and popular commercial operating systems have been important factors supporting their widespread adoption. However, that very same openness and flexibility have been proved to be a double edged sword, because it brings complexity, reduces trust degree and threat against security. So there should be a balance between the security and the convenience [2]. While downloading files from the internet, the users unknowingly downloads harmful software such as key logger. The user-sensitive data such as login and password gets hacked with the software such as Spyware, Trojans etc. while the user works with the user interface in order to access the web services. The data in the infected computer is no longer safe. Thus even after taking all the safety measures such as installing antivirus software also, there exist the risk of our sensitive data getting hacked when we use the web-service of cloud computing [3].

The five essential elements of cloud computing are the following:

a) on-demand self-service: The cloud computing provides the cloud resources to the users whenever they are required without any human interaction.

b) Broad network access: The computing resources are available over the network (e.g. Internet) and for access heterogeneous platforms, such as tablets, PCs, Macs and smart phone.

c) Resource pooling. The cloud providers serve multiple customers with computing resources. With the pool based model the clients will not know the location of their stored data.

d) Rapid elasticity. For consumers, computing resources can be scaled as per the requirement.

e) Measured Service. The cloud infrastructure has the mechanism to measure the services provided for the customers in the shared pool of resources [4].

1.1 Security in Cloud Computing

Cloud computing faces various security threats for several reasons: a) Loss of control - the user's loss the control of data in the cloud environment and hence the usual cryptographic techniques cannot be directly applied for the purpose of data security. To ensure continuous and long term data security of the various kinds of data stored in the cloud, the problem of integrity and correctness of stored data in cloud becomes more challenging. b) Integrity of data – The stored data need to be frequently updated. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important area remains to be fully explored in the literature [5].

In cloud computing, many users and even the resources join or leave the cloud at random. There should be a trustworthy relationship among the users, resources and the cloud. Establishing the trustful relationship is a challenge because of the different security policies of the users and the resources in the cloud. In fact, there will be a Service Level Agreement between the cloud participants to maintain the confidentiality of their data [6].

The traditional way to ensure security of data during transmission and storage is to compress the data and encrypt it [7]. Unencrypted data of the client cannot be stored in the cloud because the cloud provider will have access to the data and hence the confidentiality of the data will be lost. Also, a malicious cloud provider can modify the client's data and hence, the integrity of the data will be lost. An encrypted file system is used to encrypt the user's data, manage and create keys which are used for data encryption and decryption. The encryption and decryption of files is transparent to the user and the application [8]. The dependable and secure computing includes not only security and confidentiality, but also reliability, availability, safety and integrity [9]. Considering these facts, we propose a new way that is conducive to improve the secure and dependable computing in cloud.

Cloud computing provides Internet-based services to customers and business and also provides significant cost effective IT resources as cost on demand IT based on the actual usage of the customer. The cloud computing technology helps companies with much more efficient computing by centralizing resources, but at the risk of data privacy. The diversity of users multiplies the associated risk. Identity management (IDM) is one of the key components in cloud privacy and security. This can improve security and user satisfaction and help reduce some of the problems associated with cloud computing. The identity management can be deployed by a centralized component processing authentication and authorization requests [10].

1.2 Trusted Third Party

Employing Trusted Third Party services within the cloud, leads to the establishment of the necessary Trust level and provides ideal solutions to preserve the confidentiality, integrity and authenticity of data and communications [11]. In cryptography, when two parties want to interact with each other and if security is their major concern, they both can depend upon and trust this Third Party. The scope of a TTP within an Information System is to provide end-to-end security services, which are scalable, based on standards and useful across different domains, geographical areas and specialization sectors. The establishment and the assurance of a trust relationship between two transacting parties shall be concluded as a result of specific acceptances, techniques and mechanisms. The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. Introducing a Trusted Third Party can specifically address the loss of the traditional security boundary by producing trusted security domains. As described by Castell, ''A Trusted Third Party is an impartial organization delivering business confidence, through commercial and technical security features, to an electronic transaction. It supplies technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means" [12]. This infrastructure leverages a system of digital certificate distribution and a mechanism for associating these certificates with known origin and target sites at each participating server [13]. TTPs are operationally connected through chains of trust (usually called certificate paths) in order to provide a web of trust forming the notion of a Public Key Infrastructure (PKI) [14].

For a good organization it is very essential to have a cloud that allows investigation from a single party, audit the outsource data to ensure the data security and save the user's computation and data storage. It is very important to provide public auditing service for cloud data storage, so that the user trusts an independent third party. The Trusted Third Party (TTP) checks the integrity of data on the cloud on the behalf of the users, and it provides the reasonable way for the users to check the validity of

data in the cloud. On the whole, enabling public auditing services plays a vital role in establishing cloud economy, where by users need way to assess to risk and gain faith in the cloud. Public auditing, in addition to user provides the external party to verify the correctness of stored data against the external attacks [15].

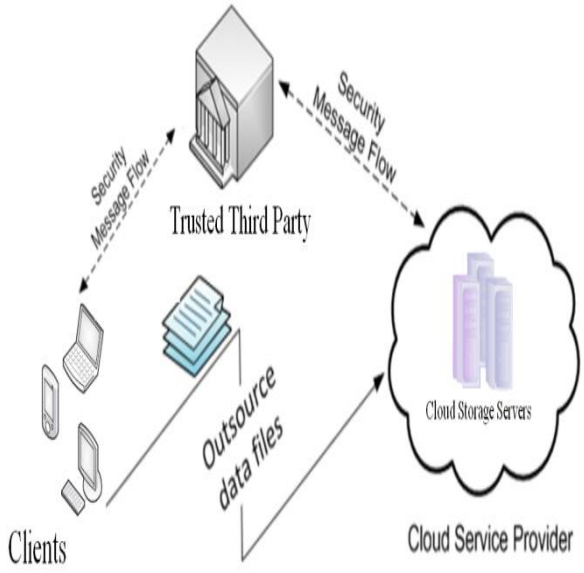

Fig. 1. Network architecture for cloud data storage

Network architecture for cloud data storage is illustrated in Fig. 1. Three different network entities can be identified as follows:

- The Cloud User: is either a single user or an organization that has a large volume of data files to be store in the cloud.
- The Cloud server: has a large storage space and computation resources to provide data storage services.
- The trusted third party (TTP): is a secure and reliable entity who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage[16].

2. PROPOSED FRAMEWORK

A client/user stores his data within the cloud storage servers. We consider the confidentiality and integrity issues of client's data within the cloud and provide a solution to these issues by proposing an algorithm for Authentication Check in order to check the authenticity of user using cloud computing.

2.1 Definitions

A cryptographic hash function is a hash function that maps an arbitrary length input to a fixed size output, the cryptographic hash value. Any change in the input data will change the hash value. It is just a method of compressing strings in which the input is called "message" and the output is called "digest". Cryptographic hash functions have many information security applications. It provides assurance of data integrity. It is used in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions. The hash creates a fingerprint of the data often called message digest [17]. The Digest can be added for redundancy and it also hides the possible structure in message. A cryptographic hash function can be run on a piece of data, often an individual file, producing a value called a checksum. Two files can be assured to be identical only if the checksums generated from each file, using the same cryptographic hash function, are identical.

In security**, salt is a random** string of data used to hash a password. The primary purpose of salt is to defend against dictionary attacks and prevent the usage of rainbow tables [18]. A new salt is randomly generated for each password. A salt makes decryption less efficient for attackers by adding another hashing layer on top of an encryption algorithm. When a passphrase is used to encrypt data, a salt can be additional data that gets concatenated to the passphrase or key. This means that the attacker's dictionary now needs to contain many more entries, one for each possible salt value for each probable passphrase [19].

2.2 Algorithm for Authentication Check

Step 1: Generate Unique Key.
For generating unique key, we propose certain fundamental unique attributes of individuals like:
(i) Name of user, (ii) User's Retina Scan (iii) Thumb Impression of the user (iv) Digital Signature (v) Date of Birth of user (vi) Nationality of user
The data input by the user is of alphanumeric in nature. As per the standard UNICODE scheme, we get its standard equivalent numeric value named *unique*.

Step 2: Trusted Third Party generate ID by encrypting *unique* using salted cryptographic hash function and sends ID back to the client:

Step 3: The Client needs to know:

In order to successfully authenticate to the TTP, the client needs to know the password (may be ask it from the user on each login).

Step 4: Authentication Check:

1. TTP: passes the stored unique on to the client.
2. Client: computes response by Hashing password with *unique* as the salt and passes it on to the TTP.
3. TTP: checks if decrypted *unique* = response, which will mean successful authentication, and if so generates new *unique* and ID

Step 5: For Data Storage, the Client encrypts the file and send to the Cloud Service Provider which generates an id for that file. After confirmation by the TTP, the CSP stores the file.

Step 6: The Client can use the file id and through the TTP it can do Data Verification, Data Retrieval and Data Modification.

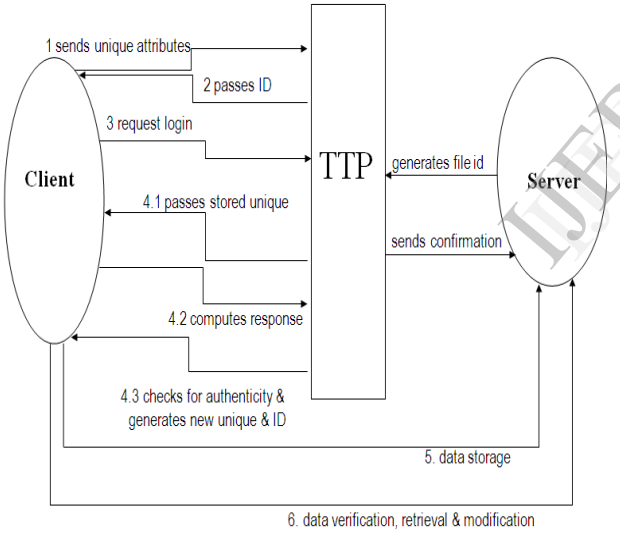

Fig. 2. Algorithm Work Flow

3. CONCLUSIONS

The Cloud is a platform where client (data contributor) remotely stores their data in the cloud to enjoy the high quality applications and services. The client sends their data to data centre and utilizes the service provided by the Cloud Service Provider (CSP). The CSP will manage the data of client at data centre. So the authors use Trusted Third Party (TTP) who not only manage the data but also tells the client that how much CSP is reliable and can keep the data safe. Even sometime client send false data or data is corrupted due to noise or some error, he claims that CSP change his data.

Security in cloud computing can be addressed with Trusted Third Party and without Trusted third Party. In the cloud computing by using the TTP mechanism, we can increase the data security which is essentially a distributed storage system. In this paper, we have proposed a new frame work for user authentication using Trusted Third Party in cloud computing. We will make the actual design more practical and operational in the future. We intend to do so in our forthcoming endeavors.

4. REFERENCES

[1] Zhidong Shen , Qiang Tong , 2010 2nd International Conference on Signal Processing Systems (ICSPS):The Security of Cloud Computing System enabled by Trusted Computing Technology on pages V2-11 to V2-15.

[2] Jason Reid Juan M. González Nieto Ed Dawson, "Privacy and Trusted Computing", Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE, 2003.

[3] K.Mukherjee , G.Sahoo , "A Secure Cloud Computing" IEEE-2010 International Conference on Recent Trends in Information, Telecommunication and Computing, pages 369-371.

[4] Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", 2010 24th IEEE International Conference on Advanced Information Networking and Applications, pages 27-33.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), 2009.

[6] Zhidong Shen, Qiang Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", 2010 2nd International Conference on Signal Processing Systems (ICSPS), pages v2-11 to v 2-15.

[7] Xiaoyu Ruan, Rajendra S. Katti, "A New Source Coding Scheme with Small Expected Length and Its Application to Simple Data Encryption", IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 10, OCTOBER 2006.

[8]http://technet.microsoft.com/en-us/library/ cc700811. aspx

[9] Algirds Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE transactions on dependable and secure computing, vol.1, No.1, January-March, 2004.

[10] Jun Chen ; Xing Wu ; Shilin Zhang ; Wu Zhang more authors, " A Decentralized Approach for Implementing Identity Management in Cloud Computing", 2012 Second International Conference on Cloud and Green Computing (CGC 2012) on pages 770 – 776

[11] D. Polemi, Trusted third party services for health care in Europe. Future Generation Computer Systems 14 1998, 51-59.

[12] S., Castell. Code of Practice and Management Guidelines for Trusted Third Party Services. s.l.: INFOSEC Project Report S2101/02, 1993.

[13] Commission of the European Community. Green Paper on the Security of Information Systems. 1994. ver.4.2.1.

[14] VeriSign. Directories and Public–Key Infrastructure (PKI). s.l.: Directories and Public –Key Infrastructure (PKI).

[15]Farzad Sabahi, "Cloud Computing Security Threats and Responses" ,IEEE confer. 2011, 978-1-61284-486-2/111

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," IEEE INFOCOM 2010, San Diego, CA, March 2010.

[17] William Stallings, "Cryptography and Network Security, Principles and Practice, 5th Edition", on page 329-331

[18] Sharma, N. ; Rathi, R. ; Jain, V. ; Saifi, M.W. , "A novel technique for secure information transmission in videos using salt cryptography", IEEE-2012 Nirma University International Conference on Engineering (NUiCONE), pg 1-6

[19]http://docs.trendmicro.com/all/ent/sc/v2.0/en-us/ Webhelp_OP_WC/sc_ag/sc_ag_glossary/salt.htm