An Improved End to End System for Sharing and Managing Data in Cloud Storage

Sumiti Joshi
CSE Department
AITR, Indore [M.P]
India

Shiv Dubey
CSE Department
AITR, Indore [M.P]
India

ABSTRACT

Cloud Computing is one of the emerging area in modern times. It is providing excellent facilities due to its adaptable infrastructure and features, but the issues related to trust management and security are key challenges in various applications. Whenever data or information is shared or transmitted from one host to another in cloud storage there is a need for security and trust assurances to prevent data from unauthorized hosts. In this article we present a survey which addresses the various challenges of cloud storage along with the different trust computation models to identify important research issues in the hotfoot growing area of computer technology. In order to resolve those issues the proposed methodology incorporates the trust evaluation and Digital Envelope techniques for preserving data against the un-trusted hosts and networks.

Keywords

Cloud Storage; Security; Trust Management; Digital Envelope; AES Encryption.

1. INTRODUCTION

Cloud computing, involves delivery of on-demand computing resources or hosted services from applications to data centre such that it rely on *sharing computing resources* instead of having local servers over the Internet on a pay-for-use basis [1] [2].Cloud computing model is classified into: Deployment model and service model. Deployment model consist of four clouds: Public Cloud, Private Cloud, Hybrid Cloud, Community model. Service model is divided into three layers i.e., bottom layer, middle layer and top layer referred as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)[3].

Traditional applications in business have always been very cumbersome and expensive as software and hardware required to run them are disconcerting. You need a whole team of specialist to install, configure, test, run, secure, and update them. With cloud computing, you get rid of those headaches [4] because due to shared infrastructure, upgrades are automatic. Cloud computing provides scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Though cloud computing, are providing various potential gains the organizations are slow in adopting it [5] due to security and trust issues associated with it which hamper the growth of cloud. The handing of important data to another company is troublesome such that the consumers need to be watchful in understanding the risks of data breaches in this new environment [5]. Modern attacks on cloud storage providers have aggravated these concerns. Thus, whenever data is outsourced from one server to a remote server lying in different trust domain lack of trust management could lead to severe access of authorized data by the un-trusted host. For example, to access Facebook account we need a Google account. In such case Google always want that Facebook should access only that information for which they are authorized. Here, lack of trust management can lead to access of such data for which Facebook is not authorized.

Thus, design and development of new security standard for protecting the data from un-trusted network is needed which can evaluate the trust level of intermediate host and manages the privacy and data integrity in a secure manner. In this paper, we present a survey of cloud storage security along with state-of-the-art research challenges [6]. Our aim is to provide a better understanding of trust computation methods and focus on the research ongoing in this tremendously developing arena using digital Envelope technique [6].

2. BACKGROUND

This section is organized as follows. In Subsection 2.1 we discussed about cloud storage and its security needs in current scenario. Subsection 2.2 provides various models that are used for trust computation.

2.1 Cloud Storage & Security

The Cloud computing technology is a scalable and reliable method of providing online multiple resources or services as per the need of the user with no spending involved for the cloud user. The cloud computing have some underlined issues such as cross border data storage issues, compliance, multi-tenant and down time issues. The principal issues are related to cloud storage [7]. Due to increasing popularity of cloud storage, many people choose to outsource data to cloud storage server, which brings many benefits for clients such as accessing data from anywhere and never worrying about the backups [8].

Recent understanding into this technology has examined various critical aspects of security. Various categories of such security concerns are trust, data protection, confidentiality, Integrity, availability and identity management. All these security weakness leads to various threats on the cloud such as authentication, misuse of cloud infrastructure, eavesdropping, denial of service attack, etc. Because of these security concerns sectors such as banking, healthcare, finance and defence are suspicious to use cloud services and hence are underprivileged of its advantages. Thus, Security issues in cloud computing threaten confidentiality, integrity and availability [9]. There are number of cloud security related issues associated with cloud storage:

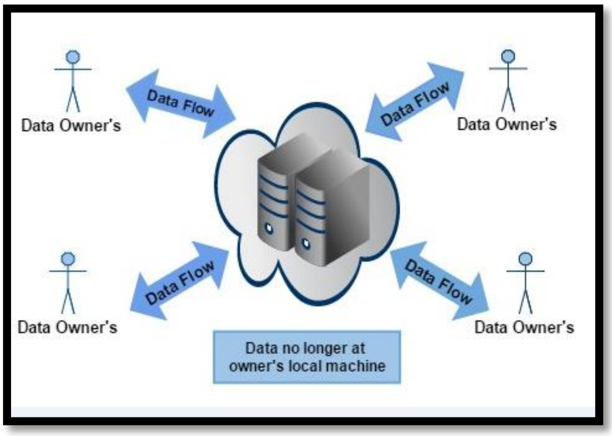

Fig 1: Cloud Storage[10]

- The cloud service providers give access to their local government and their authorities as per their jurisdiction regulations and standards.
- The service provider may bankrupt or vanish from the service providing market.
- The access to unauthorized data cannot be avoided in an effective manner.
- Illegal use of the client data can be done by data holding or storing service provider to develop their business [7].

Several security issues with cloud user and CSP [Cloud Service Provider] are as follows:

- **Cloud Service Provider (CSP):** Organization provides various services to cloud users. The confidentiality and integrity of cloud data should be preserved by CSP. The Provider should ensure that user's data and application are secure on a cloud and CSP may not disclose the information or else cannot modify or access user's content.
- **Cloud Server (CS):** The cloud server where data being stored and accessed by cloud data owner or users. Here, data should not be retrieved by unauthorized users, no modification or loss of data should occur.
- **Cloud User:** Attackers can access basic information like username and password. Key management is major issue in encryption techniques. In addition, CSP should also consider Data dynamic issues.

Thus it is important to have secure access to cloud services by having a system for secure access to cloud which includes security measures for protecting confidentiality, integrity and authorized access.

Hence, various new concepts arrive such as Third party auditor (TPA) in which based on the request of user's it will audit the user data stored on the cloud.

In this case, the cloud service provider does not have to worry about the correctness and integrity of the data. In this technique, to check the integrity or correctness, the TPA will audit the cloud data in two ways:

- Firstly download all files and data from the cloud for auditing. This may include Input/output and network transmission cost.
- Secondly auditing process is applied only for accessing the data but again in this case, data loss or data damage cannot be defined for inaccessible data. Public audit ability allows user to check integrity of outsource data under different system & security models. As TPA can see the actual content stored on a cloud during this phase privacy cannot be achieved. Also TPA itself may disclose the information stored in the cloud which violate data security. To avoid this, various Encryption techniques is used where data is encrypted before storing it on the cloud[11].

There are several other methods of security for cloud computing storage. Thus, if the cloud computing industry would acquire better and clearer approaches and practices, users would be better able to determine risk they face regarding privacy and confidentiality [11].

2.2 Models of Trust Computation

Trust plays a crucial role in cloud environment. It is the approximation based on security, reliability, capability and availability of ability of a service provider to complete a work in the context of distributed environment. Both in the diverse grid and cloud infrastructure it allows users to choose the optimum resources. Trust is referred to the recognition of entity's identity and the confidence on its behaviours. Trust behaviour is subjective since entity's judgement is usually based on its own experiences. Trust is stated by trust value [12].

Trust value is used to measure the degree of trust whose value depends on special time and special context. Trust that is obtained by entities direct interaction is known as Direct Trust. On the other hand trust that is obtained from credible third party who has direct contact with the designated one is known as Indirect Trust. Indirect trust is one important way to obtain trust degree of unknown entities [12].

Trust can be classified into various categories according to different levels like as:

- Based on attributes: Identity trust and Behaviour trust.
- Based on way of obtaining: Direct Trust and Recommended trust.
- Based on role: Code trust, Third party trust and Execution trust, etc.
- On basis of based theory: Subjective trust and Objective trust [12].

An overview on previous trust models designed for distributed systems are:

- **PKI [Public Key Infrastructure] Based Trust Model:** In this trust model, few head nodes secure the whole system. The validity of leader's node certifications are signed by CA [Certified Authority]. PKI model may cause a single point of failure or uneven load since it depends on leader nodes too much.
- **Network Topology Based Trust Model:** This trust model is built on the basis of network topology. According to entity location in system topology each entity's trust is calculated and it usually uses tree or graph traversal algorithm. Trust management system in this model is relatively simple but due to the high complexity of network environment, trust values are often inaccurate which may cause system security risks.
- **Basic Behaviour Based Trust Model:** This model uses pat trade records to compute trust such that one

entity's trust is gained by considering both prior trade experiences and other nodes recommendation. Trust value is somewhat complete and reliable in this model but at the same time with large-scale computation and other loads.

- **Domain Based Trust Model**: This trust model is mostly used in Grid computing which divides Grid environment into several trust domains and differentiate two kinds of trust. One is in-domain trust relationship and the other is inter-domain trust relationship. It set up different strategies for them. The mechanism of this model is feasible since nodes in the same domain usually are much more similar and most of the time has higher trust degree for each other.
- **Subjective Trust Model**: Subjective trust model which is based on cloud model describe the fuzziness and randomness.
- **Dynamic Trust Model:** Dynamic trust mechanism is a new and hot topic of security research for distributed applications. In this model construction of dynamic trust relationship needs to solve mathematics issues such as to decide trust degree space etc [12].

3. LITERATURE SURVEY

This section contributes towards the recent approaches for trust management to improve security in cloud environment.

Wenjuan Li [12] examined various trust models which are used in large as well as distributed environment. They introduced a cloud trust model to solve issues regarding security in cross-clouds environment such that a cloud customer can select different provider's services and resources in heterogeneous domains using domain-based model. They also divide one cloud provider's resource nodes into the same domain and sets trust agent. In addition they, distinguishes two different roles, cloud customer and cloud server and designs different strategies for them. In their model, they consider trust recommendation as one type of cloud services just like computation or storage along with performed emulation experiments to show better results.

Sheikh Mahbub Habib[13] investigated that though SLAs provide services with much same functionality but their descriptions are not consistent among the cloud providers. Therefore, the individuals are not assertive to find a trustworthy cloud provider on the basis of SLAs. Thus, to identify trustworthy cloud providers, they gave a multi-faceted Trust Management (TM) system architecture which provides means to find the trustworthy cloud providers in terms of unlike attributes.

Muchahari [14] observed that though cloud computing entice both the consumers and providers of cloud, but there are several issues related to security, privacy and trust that hinder the adoption of cloud in spite of its various advantages. In this paper, they present a trust management architecture which consists of cloud service registry and discovery. It serves as registry for cloud provider's and enumerates their trust values respectively. There is a trust calculator which on the basis of two parameters i.e., SLA and QoS calculates cloud service provider's trust. A Dynamic Trust Monitor keeps watch on the varying trust values with time and transactions.

Fabrizio Messina[15] observed that in Cloud/Grid system the problem of finding the most promising collaborators emerged. Thus as to obtain the assignment of a task, a node can lie when stating its own ability. Therefore, to complete the task, the lying nodes will need the association of other nodes. In this paper they proposed, a trust-based approach of finding the most reliable interlocutors by a node using a method, called SW-HYGRA (Small World-HYperspace Grid Resource Allocation) focusing at suitably making their source discovery process effective and deficient.

Muttukrishnan Rajarajan[16] identify that the cloud environments are still not enough trustworthy from a view of client. Various challenges such as service level agreements specifications, security measures, computation of trust etc still persists, that concerns the customer .In order to solve this problem and also to provide a reliable environment, a mediation layer may be required. In this paper, they propose a mediation layer, as cloud broker, that operates in different modes to solve the complex decision of choosing a faithful cloud provider which satisfy the service requirements, and also provisions security.

4. LITERATURE ABSTRACTION

This section addresses pros and cons of various approaches as shown in Table 1 that have been used previously for trust management and calculation.

5. PROPOSED WORK

This section includes the identified issues in the existing system and the involved work. Here, we provide an optimum solution to achieve security and trust assurances by using the Digital Envelope approach.

The cloud environment provides support for efficient computing but there are several challenges that exist in data handling and security management. The essential and key issues which are desired to resolve in this study are:

- **Identity Management:** Data in cloud storage needs to distinguish the data owner without harming the privacy and with providing the attributes and additional credentials.
- **Privacy Management:** During data transfer man in the middle attack and other kind of security issues can occur therefore data owner privacy is main goal to study.
- **Trust Management:** The data can pass through the un-trusted host or stored in un-trusted host therefore trust identification during file hosting and retrieval is also required in this work.
- **Data Exchange Security and Data Redundancy Management:** During the data exchange the data is copied in more than one place and therefore the redundancy in data or increases with the storage

Table 1. Comparison of various Approaches

Year	Technology	Advantages	Disadvantages
2009	Cloud Trust Model[12]	It constructs trust relationship in safe and fast manner.	It is not available for ultra-large-scale cross-clouds environment
2011	Multi-faceted Trust Management (TM) system [13]	It identifies the trustworthy cloud providers.	Trust Manager, Registration Manager, and Trust Update Engine is needed.
2012	Cloud Service Registry and Discovery [14]	This model helps to identify trustworthy cloud service provider's.	It is not suitable for third party providers.
2013	Trust Based Approach [15]	1. It makes the resource finding process efficient. 2. It allows a node to select the best interlocutors.	It is not suitable for nodes that randomly change their resource capabilities with time.
2014	Cloud Broker [16]	1. Cloud broker helps in selecting a trustworthy cloud provider. 2. It enables a variety of trust assessments and provisions security.	The evaluation of the security reputation and group reputation is needed.

overhead therefore managing the data and security is the key of work. Thus, to solve the above challenges and issues we will provide an end to end system for sharing and managing data in cloud storage.

According to the proposed solution as given in figure 2, the two different servers are required to simulate the process of security and trust management. It includes:

- **Primary Server:** It is a base host, where the user or data owner needs to create their membership. According to their membership policy, user can host their data.
- **Utility manager:** It supports data upload and download, share and data exchange according to the third party or data owner need.
- **User Data Management**: It manages users and its data along with user data manager.
- **Secondary Server:** It sends request to the primary server for desired data.

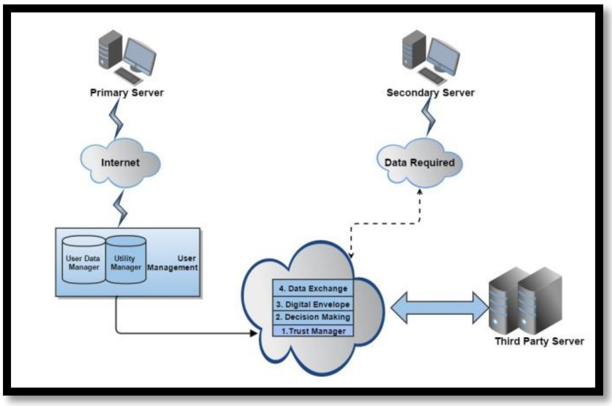

Fig 2: Proposed System

In order to simulate the security management, the secondary server sends request to the primary server for desired data. During this phase the proposed security techniques are initiated:

1. First of all trust values are computed by the trust manager for the requester using the created threshold (threshold values is point of trust rating which is statically fixed to .75 and can vary between 0-1)

2. If the computed trust value found adoptable, than in decision making phase the primary server will agree to send data to requested server otherwise the request will be discarded. If agreed, Digital Envelope initiates the computation .The proposed digital envelope works as follows:

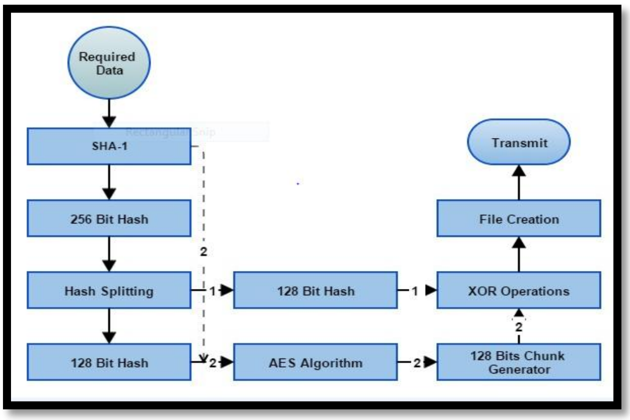

Fig 3: Proposed Digital Envelope

The envelope firstly computes the requested data from the server and produced it into the SHA1 algorithm that returns the 256 bit hash code.

On this 256 hash code, hash splitting is performed which further divide the hash code into two parts of 128 bit each. Each part is processed as follows:
The first 128 bits are used as key in AES Algorithm as shown with arrow 2 to encrypt the data. After encryption of file the data is divided into 128 bits chunks so that it can be

transmitted faster. On these chunks XOR operation is performed with the remaining 128 bits hash as shown by arrow 1 of SHA algorithm. Lastly the XORed data (data on which XOR operation is applied) is incorporated into a file and ready to transmit to the secondary server in a secure manner.

5. CONCLUSION AND FUTURE WORK

The barrier and hurdles towards the rapid growth of cloud computing are the security and trust issues associated with it. No organization can transfer its data or information to a third party system until and unless trust is build between the parties. A number of approaches have been developed by the analysts to obtain high level of security as well as data protection. But there are still many rifts that need to be filled by forming these methods more beneficial. In this paper, the proposed scheme offers three significant features such as Identity Management, Security and Trust Management while exchanging data on cloud. The System provides an environment which is useful for secure transmission channel on cloud. After successful implementation of the presented solution it provides enhanced security and improves performance .Our future work will attempt to enhance this feasible solution with more results by implementing it in cloud environment. It will be conducted for improved, efficient and secured framework for data protection and prevention to gain trust in cloud computing by providing maximum data security.

6. ACKNOWLEDGEMENT

We would like to thank everyone who helped us directly or indirectly and motivated us to pursue the research work in this area .The Proposed scheme is only for technical study not for Industrial use. So whosoever want to use for industrial purpose should check it on his constraints before use.

7. REFERENCES

[1] Cloud Computing from IBM Link: http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html

[2] Cloud Computing Link from Webopedia: http://www.webopedia.com/TERM/C/cloud_computing.html

[3] Saini, S., & Mann, D. (2014). Identity Management issues in Cloud Computing .arXiv preprint arXiv: 1406.1033.

[4] Cloud Computing Link: https://www.salesforce.com/in/cloudcomputing/

[5] CSC Journal Link: http://www.cscjournals.org/manuscript/Journals/IJCN/volume3/Issue5/IJCN-176.pdf

[6] Ahmed, M., Chowdhury, A. S. M. R., Ahmed, M., & Rafee, M. M. H. (2012). An advanced survey on cloud computing and state-of-the-art research issues. IJCSI International Journal of Computer Science Issues, 9(1), 1694-0814.

[7] Boopathy, D., & Sundaresan, M. (2015, January). Enhanced Encryption and Decryption Gateway Model for Cloud Data Security in Cloud Storage, In Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2 (pp. 415-421). Springer International Publishing.

[8] Li, M., Jia, W., Guo, C., & Zhang, L. (2015, January). Encrypted Searching with Adaptive Symmetric Searchable Encryption Security in Cloud Storage. In 2015 International Symposium on Computers & Informatics. Atlantis Press.

[9] Shetty, J., Anala, M. R., & Shobha, G. (2015). An Approach to Secure Access to Cloud Storage Service. International Journal of Research, 2(1), 364-368.

[10] Cloud Storage Link: http://www.cs.cityu.edu.hk/~congwang/images/storage.jpg

[11] Badhe, M. V., & Ramteke, P. L. (2015). A Survey on Privacy-Preserving Public Auditing for Secure Cloud Storage Using Third Party Auditor.

[12] Li, W., & Ping, L. (2009). Trust model to enhance security and interoperability of cloud environment. In Cloud Computing (pp. 69-79). Springer Berlin Heidelberg.

[13] Habib, S. M., Ries, S., & Muhlhauser, M. (2011, November), Towards a trust management system for cloud computing, In Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on (pp. 933-939). IEEE.

[14] Muchahari, M. K., & Sinha, S. K. (2012, December), A New trust management architecture for cloud computing environment, In Cloud and Services Computing (ISCOS), 2012 International Symposium on (pp. 136-140). IEEE.

[15] Messina, F., Pappalardo, G., Rosaci, D., Santoro, C., & Sarné, G. M. (2013), A trust-based approach for a competitive cloud/grid computing scenario, In Intelligent Distributed Computing VI (pp. 129-138). Springer Berlin Heidelberg.

[16] Pawar, P. S., Rajarajan, M., Dimitrakos, T., & Zisman, A. (2014). Trust Assessment Using Cloud Broker. In Trust Management VIII (pp. 237-244). Springer Berlin Heidelberg.