



## Security in Data Storage and Transmission in Cloud Computing

Pradnyesh Bhisikar <sup>#1</sup>,<sup>#1</sup>M.E (Scholar),G.H.Raisoni College of Engineering and Management,  
Amravati.Prof. Amit Sahu <sup>\*2</sup><sup>\*2</sup>M.E (CSE),G.H.Raisoni College of Engineering and Management,  
Amravati.

**Abstract**—Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. In the cloud, the data is transferred among the server and client. High speed is the important issue in networking. Cloud security is the current discussion in the IT world. This research paper helps in securing the data without affecting the network layers and protecting the data from unauthorized entries into the server, the data is secured in server based on users' choice of security method so that data is given high secure priority. Cloud Computing has been fancied as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage and transmission security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. [1]Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. This article explores the barriers and solutions to providing a trustworthy cloud computing environment.

**Keywords-** *Cloud, Private Cloud, Security, Secure data Transmission.*

### I. INTRODUCTION

Cloud computing is a recent trending in IT that where computing and data storage is done in data centres rather than personal portable PC's. It refers to applications delivered as services over the internet as well as to the cloud infrastructure – namely the hardware and system software in data centres that provide this service. The sharing of resources reduces the cost to individuals. The best definition for Cloud is defined in [9] as large pool of easily accessible and virtualized resources which can be dynamically reconfigured to adjust a variable load, allowing also for optimum scale utilization. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The key driving forces behind cloud computing is the omnipresence of broadband and wireless networking, falling storage costs, and progressive improvements in Internet computing software. The main technical supporting of cloud computing infrastructures and services include virtualization, service-oriented software, grid computing technologies, management of large facilities, and power efficiency. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [1] are both well known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon's S3 is such an example [2]. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. On this paper work is among the first few ones in this field to consider distributed data storage in Cloud Computing. And secondly secure data transmission. The key features of the cloud are agility, cost, device and location independence, multi tenancy, reliability, scalability, maintenance etc. following fig shows the general structure of cloud computing.

The rest of the paper is organized as follows. Section II introduces the system model section III introduce adversary model, section IV introduce our design goal. In Section V security architecture. Then we provide Security

framework for server-client network in section VI. Then we provide the detailed design of the system and detailed about data transmission in Section VII. Finally, Section VIII gives the concluding remark of the whole paper.

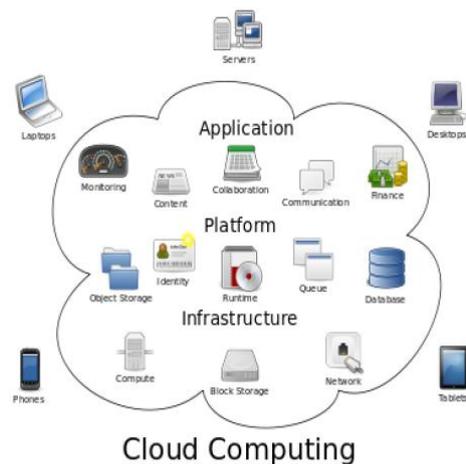


Figure 1 - general structure of cloud computing

### II. System Model

In [1] and [2] Representative network architecture for cloud data storage is illustrated in Figure 2. Three different network entities can be identified as follows:

- User: users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.
- Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.
- Third Party Auditor (TPA): an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user’s data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations we are considering are block update, delete, insert and append. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead. Note that we don’t address the issue of data privacy in this paper, as in Cloud Computing, data privacy and storage is orthogonal to the problem we study here.

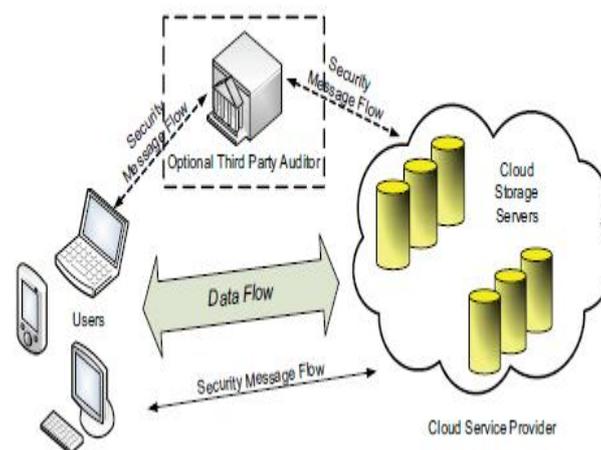


Figure 2 – cloud data storage architecture.

### III. Adversary Model

Security threats faced by cloud data storage can come from two different sources. On the one hand, a CSP can be self-interested, un-trusted and possibly malicious. Not only does it desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data loss incident due to management errors, convoluted failures and so on. On the other hand, there may also exist an economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and

subsequently is able to modify or delete users' data while remaining undetected by CSPs for a certain period. Specifically, we consider two types of adversary with different levels of capability in this paper: *Weak Adversary*: The adversary is interested in corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user. *Strong Adversary*: This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident.

#### IV. Design Goals

To ensure the security and dependability for cloud data storage under the aforementioned adversary model, we aim to design efficient mechanisms for dynamic data verification and operation and achieve the following goals:

- (1) Storage correctness: to ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.
- (2) Fast localization of data error: to effectively locate the malfunctioning server when data corruption has been detected.
- (3) Dynamic data support: to maintain the same level of storage correctness assurance even if users modify, delete or append their data files in the cloud.
- (4) Dependability: to enhance data availability against Byzantine failures, malicious data modification and server colluding attacks, i.e. minimizing the effect brought by data errors or server failures.
- (5) Lightweight: to enable users to perform storage correctness checks with minimum overhead.

#### V. Security Architectures

The above discussion is on certain review literature by many research people on different aspects of security. The aspects went on describing the problems and threats in related to security in cloud. The literature in detail explains about the issues like security for data, virtualization security and prescribed format of SLA etc. There are many research people have keen interest in designing certain security architectures help for secure cloud computing. The following are described below: Gary Anthes [14] has described the various security research works in cloud are discussed. He brought forward the research works done in popular companies like IBM, HP, and Microsoft. There are many security risks involved in cloud computing, and also some good solutions are also been designed by the researchers which are pointed below.

- 1) Researchers at HP laboratories are prototyping cells as a service to automate security management in cloud. A cell is single administrative domain using security policies containing virtual machines, storage volumes across physical machines
- 2) IBM research people doing virtual machine introspection which puts security inside protected VM running on same machine. This employs number of protective methods listing the kernel functions. It can make reduce of running virus scanners on system.
- 3) Microsoft research described about cryptographic cloud storage where the data is secured by user by encrypting format such that the provider cannot get what the data is present.

Flavio Lombardi and Roberto Di Pietro has discussed [15] about a secure virtualization technique for ensuring security at hypervisor level. In a general system at base OS level, there is a problem like a user at one guest OS may interact with other Guest OS, which may lead to data loss if they are any attackers. So the new proposal ACPS (Advanced Cloud Protection System) was introduced. This will maintain security by preventing unnecessary logins into the other guest OS by weak passwords or weak SSH. Cong Wang [5] has proposed their work on Data Storage security with respect to Quality of service. They have proposed approach which checks whether their data has been attacked or any integrity loss is done or not over the cloud. They will generate a homomorphism token which will ensure that the data is not lost. It is like a simple hash function which will be enabled to fast recover and storage errors. These works help in securing the cloud systems, Virtualization, Data confidentiality and data storage security, there are still issues need to be discussed in secure data transmission between cloud Provider, service provider and cloud User. The secure data transmission is anyhow achieved by protocols like IPSec, SSL over web and the data over are also through web applications these current methods can be used for secure data transmission. The secure data transmission works designed for storage networks are discussed by Kikuko Kamiasaka [8] who discussed in his paper for secure data transmission over IP Networks by developing Middleware works below application layer and selects suitable security approach based on the cluster of data items available in Application. This was proved that will help in securing the data as well as this works well than IPSec. Sudha M [3] has proposed an idea for secure data transmission in cloud computing using transport layer techniques, the idea proposed in that is used is socket programming for secure data transmission over the client and server. This paper has compared the general secure data transmission by applying socket programming, a key exchange and secure data over cloud. The comparison is done response time and processing time.

#### VI. Security framework for server-client network

The Fig 3 is the design architecture where a new security layer is designed for private cloud. The new security framework is present in between session layer and transport layer such that it is transparent to application layer and the lower layers. So whenever a data is transferred by the client it is first secured by certain authentication protocols and saved at the server end. With this, the data will be stored in a secured way at server end. Those who want to download

the data or view it should be connected or have access through same framework to view the data. This is done in application user level so that the data will be secured and transferred where there is need to disturb any lower layers of the network.

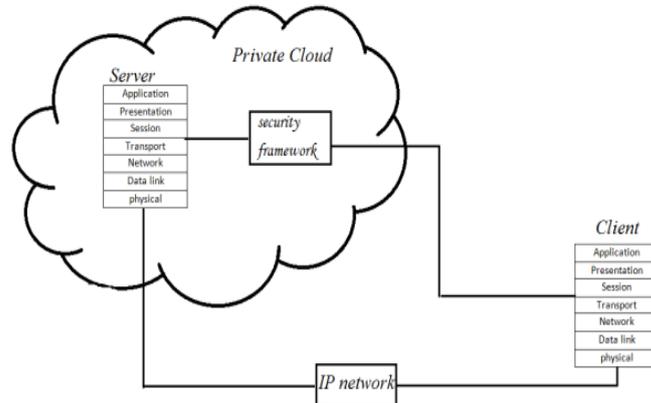


Figure 3– high level design

VII. DESIGN OF THE SYSTEM

- Security Framework Model

The detailed design of the framework is in the below Architecture Figure 4. The nodes which are connected to server will be connected to the security layer. When an Application user wants to send data to private cloud, he needs to select a

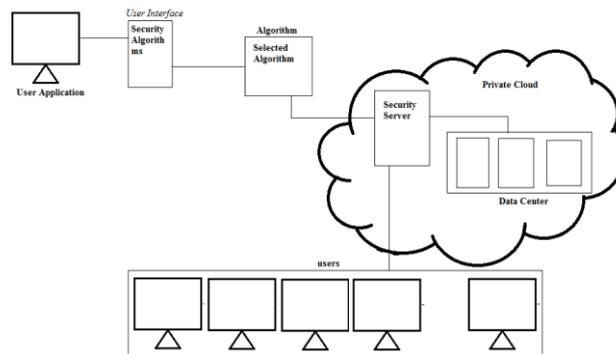


Figure 4– system architecture

Security Algorithm based on the privacy level of the document, if he needs more security there must be a strong security algorithm to be selected. The security server will secure the document and save it in database. Here all the systems which belong to that network are connected to the same architecture. When any other user wishes to select any document from the data center, he is required to be connected to the same security server to get the original document. This helps in security and privacy of the documents.

- Process at sender

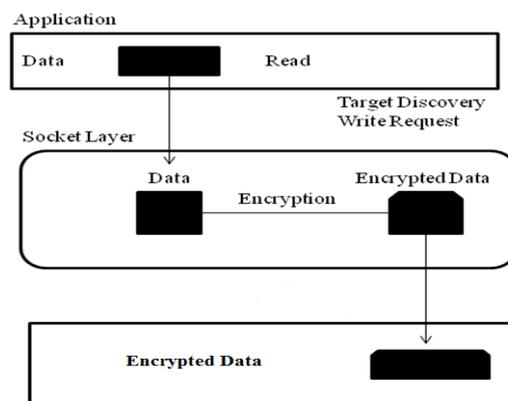


Figure 5: process at the sender

The data at the initiator end (client) will all set his data. He encrypts the data by selecting the appropriate approach from the interface and sends it to the server end. As shown in the above figure, at the client end the data is read, ready to send data. At socket layer, before sending it to the remote end the data will be encrypted for each byte and send encrypted data. The data is carried by the protocol to process the other commands which happens in a network. The data will be secured at the sender end by the security framework which helps in secure data transfer.

- Process at receiver end

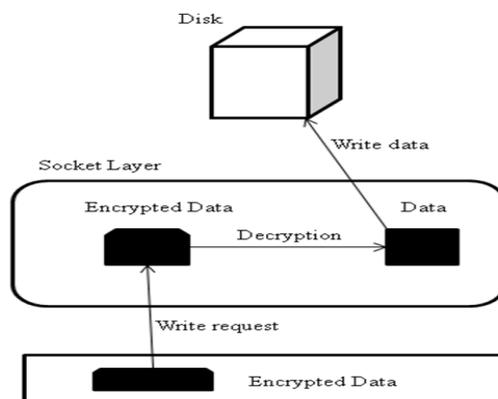


Fig 6: process at the receiver

At the receiver end when the data is received, the data will be decrypted and written on the disk. The data will be decrypted by the security approach used at encryption end. This is again worked above transport layer just where the packets arrive at end application. As before the write request is given by the protocols, the security framework decrypts the data and saves on to the disk. In the similar way when the client requests a file from server the same process as mentioned will be happened. This will make sure that data is secure over the network. We can have confidentiality and integrity checks at the receiver end.

### VIII. Conclusion

In this paper, we investigated the problem of data security in cloud data storage and data transmission, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, we proposed an effective and flexible distributed scheme. our scheme achieves the integration of storage correctness insurance and data error localization. In the data transmission proposed, method transferred data is encrypted in the upper-layer on top of the transport layer instead of using IPSec or SSL. Thus, the scheme for the performance improvement can be applied without modifying the implementation of IP layer, and efficient secure communications by pre-processing of encryption in the upper-layer are realized. We have used file uploading as service as web application, the security is applied over to the data at the background using the encryption algorithms like AES, Triple DES and DES. Through detailed security and performance analysis, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks. We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. Adding secure cloud storage using the proposed cryptographic solution and with a searchable encryption technique for the files to be accessed, it will work as a better approach to the user to ensure security of data. The cloud security using cryptography is already in use for secure data storage which can be enhanced for secure data transmission and storage. An interesting question in this model is if we can construct a scheme to achieve both public verifiability and storage correctness assurance of dynamic data. Besides, along with our research on dynamic cloud data storage, we also plan to investigate the problem of fine-grained data error localization.

### References

- [1] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE transactions on services computing, vol. 5, no. 2, april-june 2012
- [2] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011
- [3] Boris Tomasian and Bojan Vuksic "Peer to Peer Distributed Storage and Computing Cloud System" International conference on information technology interfaces, june 25-28, 2012, cavtat, croatia
- [4] "Security and Privacy Challenges in Cloud Computing Environments" co-published by the IEEE computer and reliability november/december 2010
- [5] Subashini S, Kavitha V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011) vol. 34 Issue 1, January 2011 pp. 1-11.
- [6] Balachander R.K, Ramakrishna P, A. Rakshit, "Cloud Security Issues, IEEE International Conference on Services Computing (2010)," pp. 517-520.

- [7] Kresimir Popovic, Željko Hocenski, "Cloud computing security issues and challenges," MIPRO 2010, pp. 344-349.
- [8] Amazon.com, "Amazon Web Services (AWS)," Online at <http://aws.amazon.com>, 2008.
- [9] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres1, Maik Lindner, "A Break in Clouds: Towards a cloud Definition," ACM SIGCOMM Computer Communication Review, vol. 39, Number 1, January 2009, pp. 50-55.
- [10] Patrick McDaniel, Sean W. Smith, "Outlook: Cloudy with a chance of security challenges and improvements," IEEE Computer and reliability societies (2010), pp. 77-80.
- [11] Sameera Abdulrahman Almulla, Chan Yeob Yeun, "Cloud Computing Security Management," Engineering systems management and its applications (2010), pp. 1-7.
- [12] Steve Mansfield-Devine, "Danger in Clouds", Network Security (2008), 12, pp. 9-11.
- [13] Anthony T. Velte, Toby J.Velte, Robert Elsenpeter, Cloud Computing: A Practical Approach, Tata Mc GrawHill 2010.
- [14] Gary Anthes, "Security in the cloud," In ACM Communications (2010), vol.53, Issue11, pp. 16-18.
- [15] Lombardi F, Di Pietro R. Secure virtualization for cloud computing. Journal of Network Computer Applications (2010), doi:10.1016/j.jnca.2010.06.008.