IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 9, Issue 3, Aug 2021

SECURED CLOUD COMPUTING

Mr. Sirikonda Vamshi Krushna [1], Mr. Cheruku Murali Krishna [2], Mrs. Palakollu Divya [3]

Abstract—Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. In the cloud, th, 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

Department of Computer Science Engineering, Samskruti College of Engineering and Technology

ISSN 2347–3657
Volume 9, Issue 3, Aug 2021

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 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 data transmission in Section VII. Finally, Section VIII gives the concluding remark of the whole paper.

Figure 1 - general structure of clod 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, consistof both individual consumers and organizations.
- Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building andmanaging 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 nothave, 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

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 9, Issue 3, Aug 2021

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.

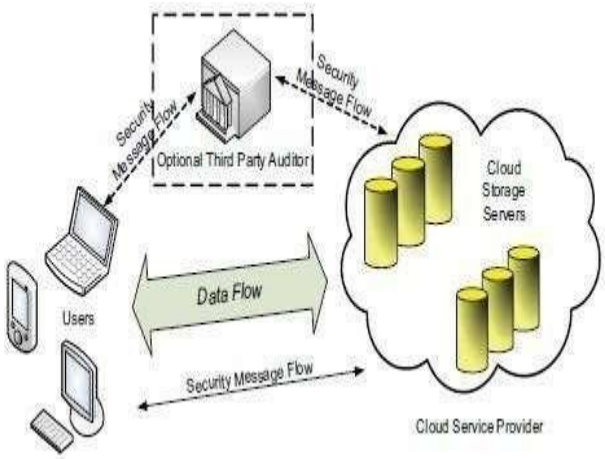

Figure 2 – cloud data storage architecture.

III. Adversary Model

Security threats faced by cloud data storage can come from two different sources. On the one hand, a CSP canbe 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 dataloss 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 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 timein the cloud.
(2) Fast localization of data error: to effectively locate the malfunctioning server when data corruption has beendetected.
(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 andserver 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.

ISSN 2347–3657
Volume 9, Issue 3, Aug 2021

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. **T**here 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.

VI. High-level Cloud Architecture

We provide and architectural view of the security issues to be addressed in cloud computing environment for providing security for the customer. We have defined four layers based on cloud computing services categorization. The cloud computing categorization based on services as Software-as-a- Service (SaaS), Platform- as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). This section elaborates the four layers shown in figure 1 and mapping the different security issues in each layer.

Some of the important components of User layer are Cloud Applications, Programming, Tools and Environments. Some of the popular examples for these applications are B2B, Face Book, MySpace, Enterprise, ISV, Scientific, CDNs, Web 2.0 Interfaces, Aneka, Mashups, Map Reduce, Hadoop, Dryad, Workflows, Libraries, and Scripting. Some of the security issues related to the user layer are Security as a Service, Browser Security, and Authentication as elaborated in next sections.

Some of the important components of Service Provider Layer are SLA Monitor, Metering, Accounting,Resource Provisioning, Scheduler& Dispatcher, Load Balancer, Advance Resource Reservation Monitor, and Policy Management.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 9, Issue 3, Aug 2021

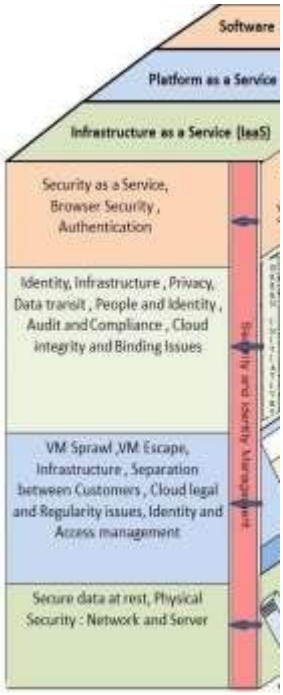

Figure 3: Security Architecture of Cloud Computing

Some of the security issues related to Service Provider Layer are Identity, Infrastructure, Privacy, Data transmission, People and Identity, Audit and Compliance, Cloud integrity and Binding Issues.

Some of the important components of Virtual Machine Layer create number of virtual machines and number of operating systems and its monitoring. Some of the security issues related to Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, Separation between Customers, Cloud legal and Regularity issues, Identity and Access management

Some of the important components of Data Center (Infrastructure) Layer contains the Servers, CPU's, memory, and storage, and is henceforth typically denoted as Infrastructure-as-a-Service (IaaS).

VII. End User Security Issues

End Users need to access resources within the cloud and may bear in mind of access agreements like acceptable use or conflict of interest. The client organization have some mechanism to find vulnerable code or protocols at entry points like servers, firewalls, or mobile devices and upload patches on the native systems as soon as they are found. The cloud should secure from any user with malicious intent that will conceive to gain access to information or pack up a service.

Security-as-a- service

In Cloud environment the security provided by customers using cloud services and the cloud service providers (CSPs).Security-as- a-service is a security provided *as* cloud services and it can provided in two methods: In first method anyone can changing their delivery methods to include cloud services comprises established information security vendors.

The second method Cloud Service Providers are providing security only as a cloud service with information security companies. Almost all the security companies, anti-malware vendors involved in the delivery of SaaS with regard to email filtering and so on.

ISSN 2347–3657
Volume 9, Issue 3, Aug 2021

Browser Security

In a Cloud environment, remote servers are used for computation. The client nodes are used for input/output operations only, and for authorization and authentication of information to the Cloud. A standard Web browseris platform in-dependent client software useful for all users throughout the world. This can be categorized into different types: Software-as-a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryption and host authentication *The Legacy Same Origin Policy* is the insertion of scripting languages into Web pages for access rights for scripts. In is to allow access read or write operations the same *origin* on content, to disallow but from the different origin any access on content. Origin means a "the same application", it can be defined with domain name, protocol, port in a web. But some problems with the SOP, but it could be solved with "origin" definition. In the case of WWW it's not working properly. Security requirements for to protect both data during transport, and to authenticate the server's domain name in Web applications is TLS. *Attacks on Browser-based Cloud Authentication* are one of the security problem with browser-based protocols in Cloud Computing and it is not capable to generate cryptographically valid XML tokens. So, it can possible with a trusted third party. Login is not possible at a server due to the fewer credentials in browser, So HTTP forward it to the Passport login server. After entering username and password from user, then the Passport server convert this authentication into a Kerberos token, it can redirected to the requesting server from other HTTP redirect. Kerberos tokens are not clear to the browser is the security problem with Passport, and it protected by the SOP. But any attacker can access those tokens then he accesses all services of the victim.

Secure Browser-based Authentication is the situation is not suggested, but we can perform for better results by combined SOP and TLS for secure FIM protocols. In Cloud Computing by using TLS Browser Enhancements are very limited in an authentication center. It is not possible for XML Signature, the browser can be added many Web Service functionalities by simply loading an appropriate JavaScript library during runtime. So, the browser security API can be adding the enhancements XML Encryption and XML Signature.

Authentication

In the cloud environment, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Trusted Platform Module (TPM) is a widely available and stronger authentication than username and passwords. Trusted Computing Groups (TCG's) is IF -MAP standard about authorized users and other security issue in real-time communication between the cloud provider and the customer. When a user is reassigned or fired, the customer's uniqueness management system can report the cloud provider in real-time so that the user's cloud access can be revoked or modified within seconds. In cloud any fired user is logged, they can be immediately disconnected. Trusted Computing enables authentication of client nodes and other devices for improving the security in cloud computing. The frequently targeted attack is authentication in hosted and virtual services. The secure mechanisms are used to the authentication process for frequent target of attackers by different ways to authenticate users based on different information know by the user.

VIII. 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 application user level so that the data will be secured and transferred where there is need to disturb any lower layers of the network.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 9, Issue 3, Aug 2021

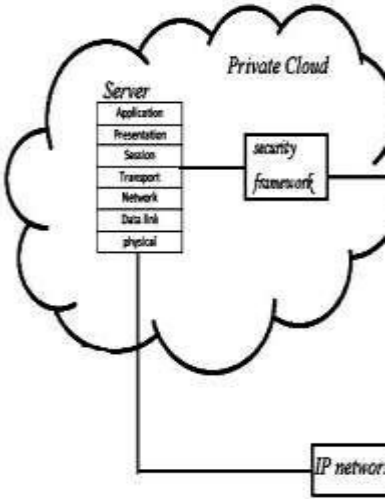

Figure4– high level design

IX. 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,

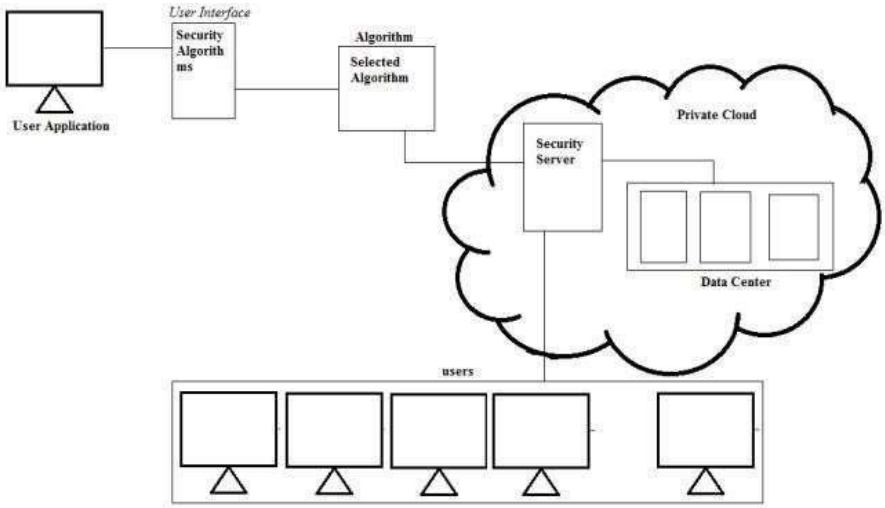

Figure 5– system architecture

Security Algorithm based on the privacy level of the document, if he needs more security there must be a strongsecurity 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 toget the original document. This helps in security and privacy of the documents.

ISSN 2347–3657
Volume 9, Issue 3, Aug 2021

- Process at sender

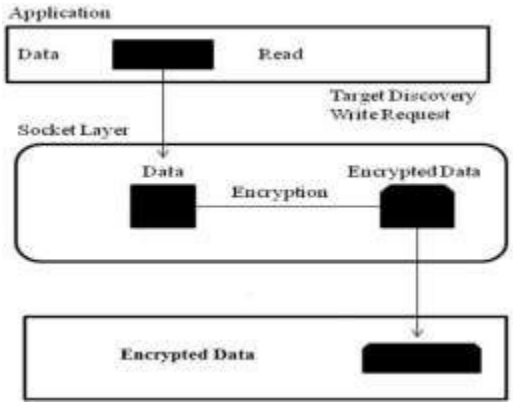

Figure6: process at the sender

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

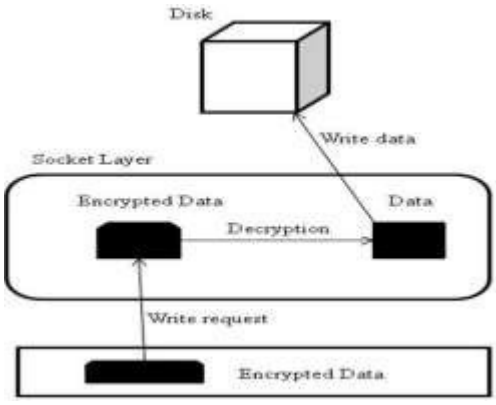

Fig 7: process at the receiver

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.

X. 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 WangKui 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,

ISSN 2347–3657
Volume 9, Issue 3, Aug 2021

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 Tomas1and Bojan Vuksic2 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 ieee 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. 517-5.