Security Services of Data Storage in the Cloud considering Third Party Servers

Tuvyam Jain [1], Priyanka Soni[2]

[1] Student, class of IX , St.Michael's School, Bhind, MP
[2]Teacher of Computer Science , St.Michael's School, Bhind, MP

ABSTRACT-*Cloud environment plays an important role in deploying enterprise software applications; hence cloud security for information systems had become a major issue. Large scale applications which are distributed components are stored in the cloud. This gives rise to implement several security strategies which should be efficient. Since Cloud Service Provider (CSP) holds and maintain the information in the existing systems, there is possibility of misbehave which affects the integrity and availability of data. Although the lack of security assurance the CSP should promise on smooth and correct functioning of data of enterprise applications. This means that a server failure or error should not have any impact on the operation. This demands the need for fault tolerance. In this paper we handle the various security issues by developing a framework in cloud based architecture. An optimal security service is being developed as a service offered to cloud systems. This project mainly focuses on implementation of two major aspects i.e; integrating and maintenance of data storage and fault tolerance. Also offers support for fast error localization and correction, dynamic data operations, and the same concept can be applied for more perfect security for the users file by extending this concept to a different entity called Third party Server, who considers the data and declares whether the data is in correct form from the local server where the users files is totally hidden from the TPS by using authentication algorithms. This TPS is a very powerful trusted system where it declares the user about his files on the cloud where internally we can provide a ranking engine and parallel processing engine virtually to find how many percentage of data is changed.*

Keywords: Cloud Computing, Security, Fault Tolerance, data storage integrity,TPS.

1. INTRODUCTION

The internet and central remote servers to maintain data and applications are used in cloud computing technology. Personal files are accessed through internet by consumers and businesses without installation of applications easily with cloud computing. Centralization of data storage , memory, processing and bandwidth can be computed in a much more efficient way through this technology.

In spite of the numerous benefits, cloud architecture poses certain threats to the users. The Cloud Service Provider (CSP) controls the overall data and applications in the cloud. Several cases have been observed where the CSP has behaved in an unfaithful manner exposing the system to both internal as well as external threats. Deployment in multiple cloud components involves larger applications which are complex in nature.

Component failure should not affect the functioning of the application in any way.

A critical challenge in providing services which urgently need of research problem on the demand of highly reliable cloud applications. This paper proposes a solution to this problem by suggesting the design of a security service which operates on the cloud as a separate entity, interacts with the application and takes care of security issues, mainly, data integrity and fault tolerance. Both CSP and users will have the control in providing assurance to the data in the cloud.

2. PROBLEM DEFINITION

2.1 Existing System

Local machines relinquishes the control of data where cloud based operation provides huge amounts of storage space and customizable computing resources. The availability and integrity of information is being handled by CSP. Since the users do not possess a local copy of outsourced data, the CSP may give wrong information to the users regarding the status of their outsourced data. In order to maintain a reputation a CSP may even attempt to hide data loss incidents. The lack of integrity data assurance and availability which may impede outsourcing data adoption by individual and enterprise users where the outsourcing of data is attractive for the cost and complexity of long-term large-scale data storage in the cloud. Also, the cloud applications are usually large scale, very complex and typically involve multiple cloud components communicating with each other. Enterprises need to be reliable of the cloud application in order to transfer their critical systems to the cloud. Thus the concept of TPS is not at all applied in any system .thus we apply the same concept to have double fun security in both terms of data and trusted system of TPS.

2.2 Proposed System

Security service to be developed that promises to handle the limitations discussed in the previous section which reflects two major concerns. There is a need in the design of efficient methods so as to cloud users can correctness verification on on-demand data. Therefore, the cloud users no need to have physical possession of data that prohibits the direct adoption of traditional cryptographic primitives for data integrity protection purpose. Without explicit knowledge of the whole data files the verification of cloud data storage correctness must be conducted. The proposed handles all these issues and provides an overall security service system for cloud applications and there after it handles to the TPS of the cloud to further authenticate the files of the system, and have double the security by having the same concepts in both the CSP and TPS, to ensure the maintenance and integrity of the users file on the cloud, where it is done virtually only the obstacle is transparently seen by the clients but not the TPS itself. This is the main advantage of these proposed schema.

2.3 Problem Statement

The major goal of this project is to provide security as a service with more enhanced concept called TPS in cloud based architectures. It comprises of three-fold strategy:

- Data storage security.
- Fault tolerance of cloud running applications.[1]
- Data storage security considering Third Party
- Servers where the maintenance is done virtually.

Large application components are complex in cloud which are identified and framework that is rank based is used to build fault-tolerant and the same concept can be applied to the TPS server virtually , where the clients can determine the files security. Then it implements Parallel Processing technique for fault tolerance.

Data storage security is implemented by performing data integrity checks over the cloud. It employs a challenge token computation for the same. It also provides support for dynamic data operations, error localization, and error recovery in the cloud network. Thus, effective application operations are done over the cloud even if it is ensured in case of faulty servers and data errors.

The TPS maintain the same system where it is provided with a protocol to ensure enhanced security for the Maintenance and integrity of the files supporting the data dynamics operation concepts. These all can be maintained by the RSA signatures.

3. SYSTEM DESCRIPTION

3.1 System Architecture

The diagram shows the interation of various components of the security system with each other in the network

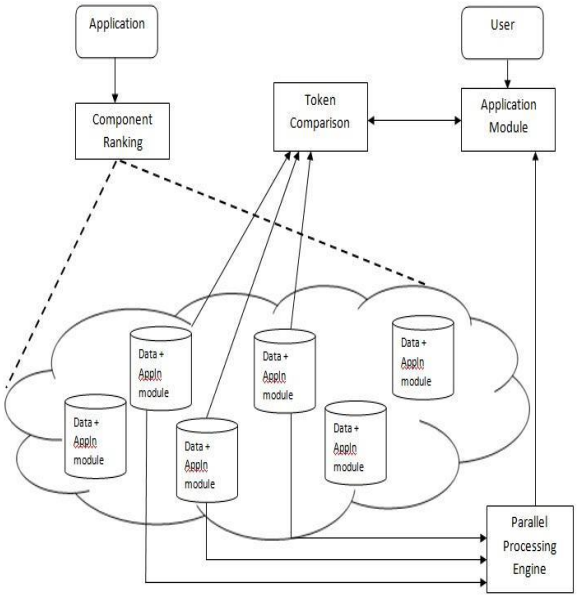

Figure-3: SaaS System Architecture

The figure 4 is combined with the CSP and the TPS where both are for the same purpose but a small similarity change that the CSP provides a data and the same TPS used for the maintenance and verification of information and know the percentage of information changed virtually to the users and to the TPS itself. So that the users will not depend on the CSP, and knows about his data.

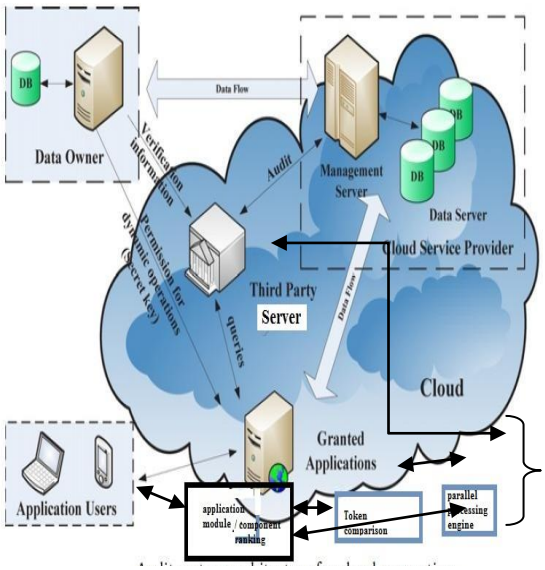

Figure 4: architecture of cloud embedded with TPS

Multiple cloud servers are involved in the clouds which are responsible for data storage as well as execution of application. The data and various application modules are distributed over these servers. The critical and non-critical components which decide the number of cloud servers on which they are deployed raises a component ranking algorithm. Token Comparison Engine (TCE) involves respective cloud servers for the data requirements of the current application module,. Based on a challenge response strategy, tokens are generated on the respective servers and sent to the TCE. Error localization and recovery compare the responses and performs in TCE. Correct data is now sent to the application module. Multiple servers send their responses to the Parallel Processing Engine (PPE) to protect the system from a faulty server. The fastest of these responses is returned to the application module. Thus, the system is able to function efficiently and correctly even in case of a faulty server.[2] and applied to TPS.

The description of the key components is as follows:

A. Component Ranking Engine

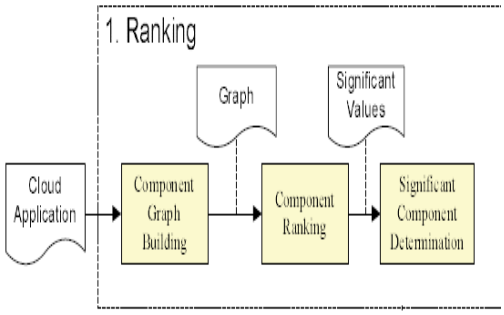

Figure-3.a: component ranking engine

The initial architecture design of a cloud application is provided by the system designer. A component graph is built for the cloud application based on the component invocation relationships. By employing component ranking algorithms significance values of cloud components are calculated. Based on the significance values, the components can be ranked. The most significant components in the cloud application are identified based on the ranking results.[2]

B. Token Comparison Engine

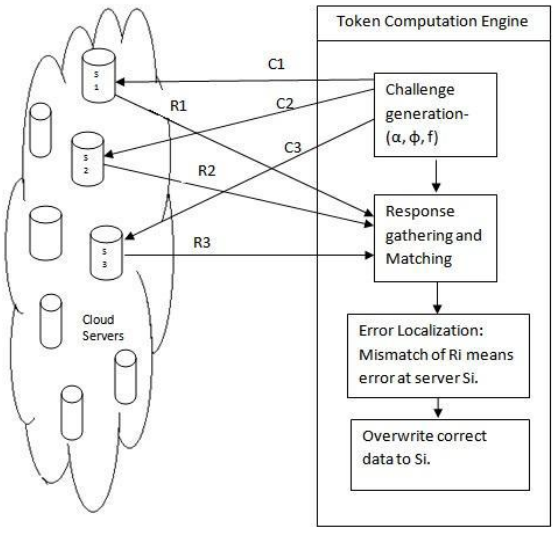

Figure-3b: Token Comparison Engine

With randomly generated block indices the servers storing of relevant data are challenged. A token is being produced trough each server by applying a specific token generation function to the indices. All servers send their respective tokens to the token comparison engine which compares the received values and locates inconsistencies. The server with erroneous data. Holds inconsistent value which is determined. Thus error localization is achieved. A verified server is overwritten on the faulty file to recover from this error, correct data from.[4]

Thus, data integrity is ensured.

C. Parallel Processing Engine (PPE)

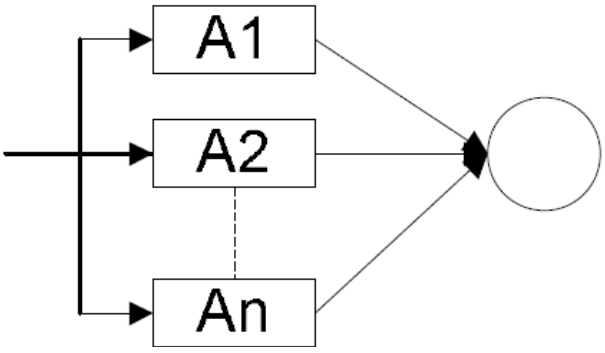

Figure-3c: Parallel Processing Engine

A strategy employed for fault tolerance is Parallel Processing Engine (PPE). Servers from which a particular application module is deployed which collects the processed results from the end. Since many servers return a result, even a faulty server does not hamper the

performance of the application. PPE forwards the result from that server which gives the fastest response.

4. IMPLEMENTATION

A specialized cryptographic algorithm is used for data files, required by the application are encrypted and are then distributed over multiple cloud servers. Various modules of the application are performed with component ranking algorithm. Fault tolerance is implemented only for the critical components identified in this phase. Over multiple cloud servers based on the obtained results these modules are deployed.

Computation of tokens takes place at the cloud servers. Now a critical task challenge is sent to multiple data servers whose data checking is needed. The responses are compared and any deviation or mismatch indicates error at that particular server. This can be corrected by overwriting from a correct source. Correction is facilitated to error localization as well, and then passed to the very trusted system called TPS after all the cloud servers checks the data. Thus finally it calculates the percentage of data changed and is transparent to the users at the same time. Whereas the content of data is hidden from the TPS.

A (PPE) parallel processing technique is employed to implement fault tolerance. Their result are returned to the parallel processing engine on which the application module is deployed which perform the computations on multiple servers. The response which is received first is returned as the final result. The application is still able to run efficiently and correctly even in case a server becomes faulty. Thus, the scheme gives a guarantee about correct functioning of the application even in a case of component failure.[5]

5. CONCLUSION

In spite of the numerous benefits, cloud architecture poses certain threats to the users. This paper proposes the issue of centralized data storage on cloud, an efficient scheme to address. The user , CSP and TPS have exclusive control on independent data security service. The approach compiles on token generation and parallel processing techniques to realize its functionality. Identification of faulty servers also facilitates simultaneous for error localization and error correction on stored data. The proposed system provides double high-end security service in both the terms of CSP and TPS and thus better performance in the cloud which has been missing in the current systems.

Acknowledgement

It is my honored privilege to express with immense pleasure my deep sense of gratitude devotion and regard to Fr.Lawrence D'Souza, Principal St.Michael's School, Bhind for extending unstinted support untiring constant help and encouragement proficient guidance. I would like to record my gratitude to Priyanka Soni for her supervision, advice, and guidance in the research design.

REFERENCES

1. Component Ranking for Fault-Tolerant Cloud Applications Zibin Zheng, Tom Chao Zhou, Michael R. Lyu, Irwin King.[1]

2. Towards Secure and Dependable Storage Services in Cloud Computing Cong Wang, Qian Wang, Kui Ren, Ning Cao, Wenjing Lou.[2]

3. http://searchsecurity.techtarget.com/definition/Security-as-a-Service[3]

4. http://www.wikinvest.com/concept/Cloud_Computing#_note-versionOneStudy[4]

5. http://msdn.microsoft.com/en-in/ff380142[5]

6. http://searchcloudcomputing.techtarget.com/definition/cloud-computing[6] .

BIOGRAPHY:

Tuvyam jain , currently studying in class IX from Bhind, mp, India. He is very much interested in computer science areas, having knowledge of cloud computing, image processing

Priyanka Soni, currently working as a teacher in Bhind, MP, India. Her 2 papers on Image processing was published in the international journals. Her interest areas include Web Technology, Digital Image Processing ,Cloud computing, operating system and DBMS.