

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Paper / Case Study

Available online at: www.ijarcsms.com

Multi-Clouds Security: Using Access Control

Belhekar Vipul Krushna¹

Dept of Computer Engg
Dr. D.Y.Patil IET
University of Pune
Ambi-Pune – India

Dhawal Kumar Balu²

Dept of Computer Engg
Dr. D.Y.Patil IET
University of Pune
Ambi-Pune – India

Karale Bhanudas Laxman³

Dept of Computer Engg
Dr. D.Y.Patil IET
University of Pune
Ambi-Pune – India

Kohinkar Bhushan Chandrakant⁴

Dept of Computer Engg
Dr. D.Y.Patil IET
University of Pune
Ambi-Pune – India

Abstract: *The era of cloud computing has become very popular in IT culture. Low cost and accessibility of data are the main traits of cloud computing. The traditional processes of IT industries has been incredible changed by the means of cloud computing. The cloud computing has benefited the IT industries with less infrastructure assets and maintenance Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users stores vital data with cloud storage providers but these providers may be non trusted.*

This paper tends to provide a large review on the essentiality of SAS (Security-as-Service) in cloud computing scenario. We are developing a technique through cloud computing in which user will store sensitive information onto database server with a secure infrastructure.

Keywords: *single cloud, multi-clouds, security, access control, service availability.*

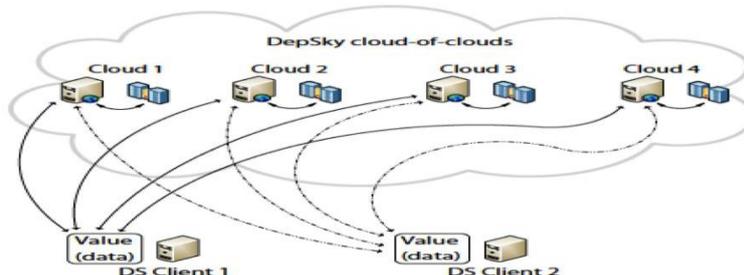
I. INTRODUCTION

The use of cloud computing has rapidly grown in many firms these services provide quick access to their applications and reduce their infrastructure costs. Cloud Computing provides convenient on-demand network access to a shared pool of configurable computing resources that can be rapidly deployed with great efficiency and minimal management overhead.

This paper focuses on issues related to security aspect of cloud computing. As data is shared with a third party, the user of cloud computing want to avoid non trusted provider of cloud. Protecting important and private information, such as electronics card details or medical records of any particular patient from hacker or malicious insiders is of critical importance.

This paper refers to DepSky architecture to implement above mentioned technique, But in DepSky architecture admin stores a single data on every database server in contrast we divide that data and then store on multiple database servers. Following figure shows the architecture of DepSky architecture:

Figure 1 DepSky Architecture



II. SYSTEM OBJECTIVES

The intension of this project is:

1. To design and implement a system for sharing software and hardware in cloud from which user can access applications anytime, anywhere in secured environment.
2. The system should be robust & secure in case of malfunctioning attacks.
3. To prohibited unauthorized person from taking access of system & database by providing access control facility.

III. LITERATURE SURVEY

Existing System

The most critical security issues related to user data are privacy preservation and data integrity. In traditional paradigm, the organizations had the physical possession of their data and hence have an ease of implementing better data security norms. But in contrast of cloud computing, the information is stored on different service providers which provide data storage as a service. The users have to trust the service provider (SP) with security of their data.

The figure given below shows the working of single cloud system. Suppose assume that three users store their data on three different service providers. Each customer can access his/her own data from the CSP who it has a contract with. If a failure occurs at CSP1, due to some internal problems the user 1's data which was stored on CSP1's server will be lost and can't be accessed.

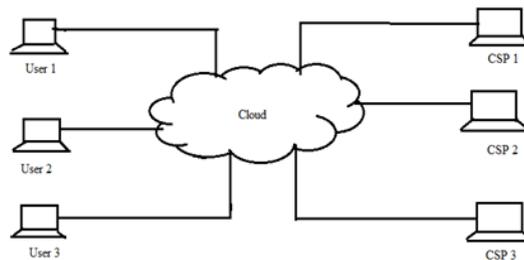


Figure 2 Single Cloud System

Single cloud service provider results in following disadvantages:

- **Data Integrity:** Data integrity is the major concern with the cloud providers. The simple way to explain data integrity, suppose a person needs hospital treatment that includes taking a daily medication dosage of 10 milligrams. By accidental or deliberate intervention, the electronic record of the treatment is changed to a dosage of 100 milligrams with fatal consequences.
- **Data Intrusion:** Another security attack associated with a single cloud provider is data intrusion. Recently red hat detected an intrusion on certain its computer systems and they took immediate actions. While they are investing on the intrusion that took place in the system. The reports say that an intruder was able to sign a small number of OpenSSH packages that were related to Red Hat Enterprise Linux 4 and Red Hat Enterprise Linux 5.
- **Service Availability:** Customers of cloud save their important data with the cloud service provider. Coping with a single cloud provider result in service availability failure. Most cloud related companies many a times deal with service unavailability.

IV. DESIGN AND IMPLEMENTATION

What is to be implemented?

To overcome the failures of single cloud provider system, we are moving towards a multi cloud system, in which we do not store user important data on a single database server but we distribute the data across multiple database servers. This system will insure the security on user data as well as the user will receive data in a timely manner. The main ingredients of the system are:

1. **Client Module:** In this module we have client registration, login, file uploading, file downloading, file deletion etc. Every user can manage the roles as well access control to his data.
2. **Application Layer:** Application server handles the client enable application where users fill all the details like GUI (Graphical User Interface).
3. **Central Server Layer:** Our crucial task will be on central server, basically we will write all web services here. It includes algorithms with DES, TPS technique etc.
4. **Cloud Servers:** On the cloud servers we will store user's sore information. With a single cloud server the data may get corrupted, as well as single cloud server results in slow processing of data. By distributing the data across multiple cloud servers we will secure the cloud storage architecture.

The workflow diagram of proposed system is as follows:

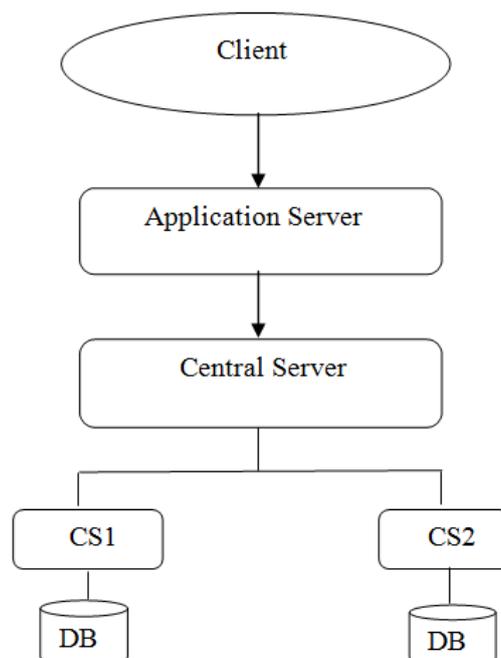


Figure 3 Proposed Systems

V. ALGORITHMS

- **DES(DATA ENCRYPTION STANDERD):**

The Data Encryption Standard (DES) is the name of the Federal Information Processing Standard (FIPS), which elaborate the data encryption algorithm (DEA). The DES has been extensively analyzed since it issued and is the mostly used symmetric algorithm. The Data encryption standard algorithm has a 64-bit block size key during execution.

The DES can also be used for single user encryption, such as to store files on a secondary memory (hard disk) in encrypted form. The DES uses a 56 bit key during running. In CBC (Cipher Block Chaining) mode of operation, each block of ECB

converted cipher text is XORed with the next plain text block to be converted into cipher text, thus making all the blocks dependent on all the descendants blocks .that means in order to get the plaintext of a particular block, you need to know the converted cipher text, the key and the cipher text for the previous block. The first block to be encrypted has no descendants cipher text, so the plaintext is XORed with a 64-bit number called the initialization vector (IV). So if data is transmitted over network and there is a transmission error (TERR), this error will be forward to all the subsequent blocks since each block is dependent upon the last one. This mode of execution is more secure than ECB (electronic code book) because the extra XOR step adds one more layer to the encryption process.

The graphical representation of DES algorithm is as follows:

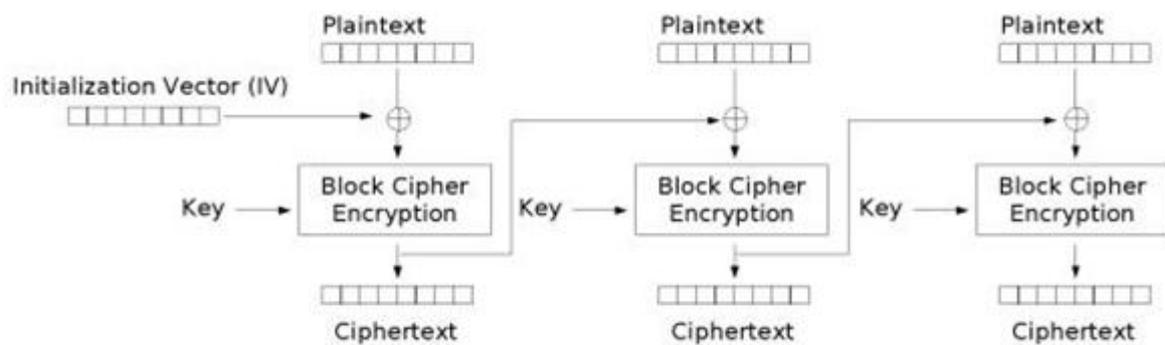


Figure 1 DES for Encryption

- **Transaction Processing System :**

Transaction processing systems (TPS) gather, store, modify and access the transactions of a firm. A transaction is an event that produces or modifies data that is finally stored in a database system. Few examples of transaction processing systems are selling goods using a point of sale system, making a hotel reservation or processing credit card transactions. TPS differ in character from other types of information systems in that they directly support business processes. The main information processes of a TPS are gathering and storing. If a TPS (transaction processing system) is used for recording a sale and creates a receipt, the transaction information is gathered at the POS terminal and then stored using an online database.

Following are the important qualities of a TPS:

1. **Quick response:** Very fast performance with a quick response time is vital. Businesses can't afford to have users waiting for a TPS to give result. The turnaround time from the given input of the transaction to the generation of the result must be some seconds or less.
2. **Reliability:** Many firms rely heavily on their TPS. A breakdown will disrupt processes or even stop the business flow. For an effective TPS, its failure rate must be least. If a TPS does fail, then quick and accurate recovery must be done. This makes good-designed recovery and backup functions essential.
3. **Inflexibility-** A TPS requires every transaction to be processed in the same way no matter of the customer, the customer or the required time. If a TPS (Transaction Processing System) were flexible, there should be too many chances for unacceptable operations. For example, a commercial airline needs to consistently accept airline reservations from arrange of travel agents. Accepting different deal data from different travel agents would be a problem.
4. **Managed processing-** The processing in a TPS must support an establishment operations. For example, if an organization apportions roles and responsibilities to specific worker, then the TPS (Transaction Processing System) should inhibit and manages that requirement.

Work flow diagram of Transaction Processing System:

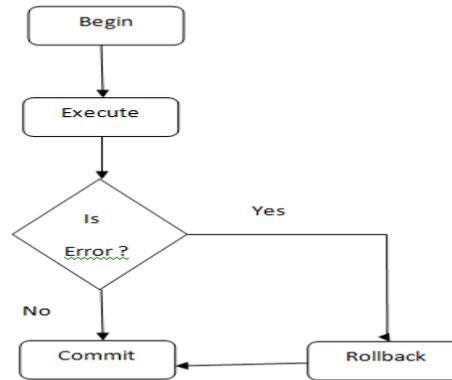


Figure 2 TPS Algorithm

VI. CONCLUSION

This system allows user to access applications, use resources remotely .System is available on internet so that user can access service anytime from anywhere. When any user access any service server will get an appraisal. Service is available for 24*7.user need not to buy license software. As the development of cloud computing, security issue has become a top precedence. System will be developing the cloud computing environment with the safety issues through analyzing a cloud computing model security needs.

Finally conclude a cloud computing model for data security from single to multi-cloud. Cloud computing, while still evolving in all its iterations, can offer IT a powerful alternative for efficient application, infrastructure, and platform delivery. If it is implemented on practice basis it will be very efficient for user. The threshold basis value server response we can do it in future work for the transaction processing (STPS) which improve the data integrity and consistency.

References

1. Mohammed A. AlZain , Eric Pardede , Ben Soh , James A. Thom "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences,2012
2. A. Bessani, M. Correia, B. Quaresma, F. Andre and P. Sousa "Dep-Sky: dependable and secure storage in a cloud-of-clouds ", EuroSys'11:Proc. 6thConf. on Computer systems, 2011, pp. 31-46.
3. Cong Wang, Kui Ren, and Jia Wang " Secure and Practical Out-sourcing of Linear Programming in Cloud Computing ", IEEE trans-actions on cloud computing april 10-15, 2011
4. Zhou Wei, Guillaume Pierre, Chi-Hung Chi "Cloud TPS: Scalable Transactions for Web Applications in the Cloud", IEEE transactions on services computing, special issue on cloud computing, 2011
5. www.Google.com
6. www.aws.amazon.com
7. www.wikipedia.org
8. www.ieeexplorer.ieee.org