Cloud Computing Hybrid Security from Single to Multi-Cloud Servers

DEEPIKA K[1], DEEPIKA M[2], ARUNPRIYA C3

[1, 2, 3] *Assistant Professor, Department of Computer Science, PSGR Krishnammal College for Women, Coimbatore, Tamil Nadu, India*

Abstract- Nowadays, storing and accessing data in multi-cloud infrastructure is a common solution adopted by large organizations. In this paper it presents two components mainly Administration Management and User Management. It contains the list of branches available for the bank in different countries and tree view which shows the country names under each country created. End User has manifested by administrator with the ability to identify and control the state of users logged into the account. The saving/current account holders can check person's own account balance; list of transactions done by the user, account personal information can be edited efficiently by giving request to the admin. The account holder can view that information only with the unique user id and password provided by the bank. After those process completed successfully a message will be displayed to the user about the transaction. If the account holder provides the wrong user ID or Password it will provide an error. If the intruder deletes the database, the database will be backed up by checking the nearest server, traffic and available storage of the multi-server. The encrypted key will be received immediately by the admin through mail to restore the deleted database. Data security for such a cloud service encompasses several aspects including secure channels, access controls, and encryption. And, when it considers the security of data in a cloud, it also must consider the security triad such as: confidentiality, integrity, and availability. In the cloud storage model, data is stored on multiple virtualized servers.

Indexed Terms- Cloud Computing, Data Security, Personal banking and Multi Cloud.

I. INTRODUCTION

Cloud computing and storage solutions give users and enterprises with various abilities to store and process the data in third-party data centres. It depends on sharing of resources to achieve consistency and economies of scale, similar to a utility over a network. The goal of cloud computing is to allow users to take advantage from all of these technologies, without the need for more knowledge about or expertise with each one of them. The cloud aims to cut costs and helps the users to concentrate on their core business instead of being impeded by IT obstacles [1]. Cloud computing can enable a user to access applications and data from any computer at any time since they are stored on a remote server. Various distinct architectures are introduced and discussed according to the security and privacy capabilities and prospects. Checking of data is called data integrity so that data must be defined, exact and changed by allowable people only. The idea on reducing the risk for data in a cloud is the simultaneous usage of multiple clouds. Multi cloud computing creates a large number of security issues and challenges. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. Different services are accessed from the multi-cloud user. The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. Various approaches for multi-cloud security differ in portioning and distribution patterns, technologies, cryptographic methods and security levels [2].Cloud computing can permit the user to access data and applications from any computer at any time since that are stored on a remote server. It also reduces the need for associations to buy top-of-the line servers and hardware or hire people to run that since it is all maintained by a third party. Software licenses do not have to buy for every user as the cloud stores and runs the software remotely [3]. File can also be stored with cloud computing so companies do not have to house servers and databases themselves. By bandwidth, storage, centralized memory processing in an offsite condition for a fee, cloud computing can significantly reduce costs. Multi cloud providers have been used to affect privacy and data integrity challenges. Multi-cloud model described the combination of various clouds where user data is distributed and executed in those clouds simultaneously. It is observed that multi–clouds improve performance provided by single cloud environment by dividing security, trust and reliability among different clouds. It has made a survey of various techniques available for multi cloud security like use of cryptography, secret sharing algorithm and redundant array of cloud storage [4].It varies from hybrid cloud environment in that it refers to multiple cloud services rather than multiple organization modes such as public, private, and legacy. Various issues are also available in a multi cloud environment. Security and authority is more complicated, and more "moving parts" may create resiliency issues. Selection of the right cloud products and services can also be a challenge, and consumers may suffer from the contradiction of choice. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the Software as a Service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale.

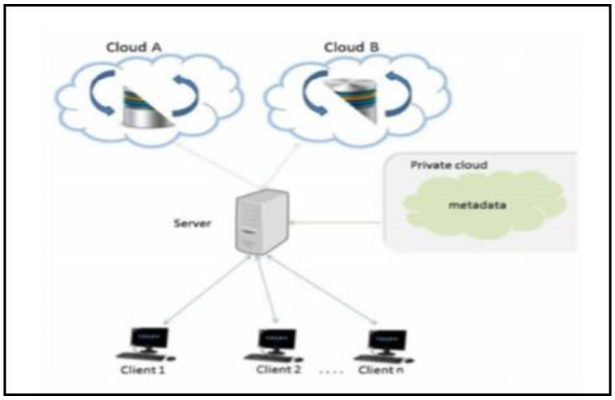


Figure 1: Multi cloud architecture

The increasing network bandwidth and reliable yet flexible network connections make it even possible that users now subscribe high quality services from data and software that reside solely on remote data centers [5].

Moving data into the cloud offers great convenience to user since it don’t have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) 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 the data. Recent downtime of Amazon’sS3 is such an example.

II. LITERATURE REVIEW

Ryan K L Ko et.al [6] studied the problems and challenges of the trusted cloud, where the unauthorized user can access the entire data without disturbing the actual user. An unauthorized person may do the two things which is accessing the data and putting duplicate data because cloud storage provides a geographical database. It is not a trusted one to store the data of the users. For this problem Ryan K L Ko et.al proposed a Trust Cloud framework, to achieve a trusted cloud to the user, to provide a service by making use of detective controls in cloud environment. Detecting process has the accountability access with the cloud. Here user is a responsible person for the data, hence user must tell the accountability with the technical and policy based services. By providing the accountability through user it may solve the problem from the untrusted one. Hence this approach provides privacy, security, accountability and auditability.

Muhammad Rizwan Asghar et.al [7] discusses the problems of enforcing security policies in cloud environment. With the high growth of data’s in the cloud, problem arises due to the untrusted person accessing the data. To ensure the security is immature, client didn’t ensure for the safe data in cloud environments. Security problem is a great issue; here to enforce the security for the owner’s data. Providing high security client may high expensive for the users. For the above mentioned problem Muhammad Rizwan

Asghar et.al proposed an ESPOON policy which is Encrypted Security Policies for Outsourced environments. This policy is used to address the above problem and give better confidentiality to the users. It provides a better security by separating the security policy and the enforcement mechanism. Policy deployment is used to exploit the user's guidelines and the policy evaluation is used to estimate the user guidelines. By using this method user can safe their data.

L Ferretti et al [8] studied the problem of data leakage of the legitimate user in cloud environment by the cloud provider; provider didn't give better security to the user for their personal data or internal data. Main problem arise because of no encrypted data were found, and also it provide the security for the frond-end database only and not controlled the backend database, so the malicious attackers may gain the data access to the outsourced data.

S. Kent and R. Atkinson [9] author believe the security issues related to the proposed MoRaRo can be resolved with the security mechanisms available for the MIPv6 protocol and its derivatives such as the NEMO basic support protocol and Hierarchical MIPv6 (HMIPv6) protocol. As both the MR and it's HA belongs to the same administrative domain, client use their pre-established security association (SA). The MNN and MR exchange themutually trusted identities to establish the SA. A trusted identity can be an IP address or a certificate signed by a Certificate Authority (CA) that both the MR and MNN trust. Similarly, the MNN and CN are mutually trusted through the return routability test. However, the MNN can use privacy rules to protect its location information against possible misuse. The privacy rules regulate the CN's activities regarding the collection, use, disclosure, and retention of location information of the MNN. In MoRaRo scheme, the MNN can perform privacy negotiation with the CN by using the privacy protection frameworks being developed.

Ankita Ajay Jadhav [10] Data sharing among cluster members within the cloud with the characters of low maintenance and tiny management price. Meanwhile, author tends to offer security guarantees for the sharing information files since they're outsourced. Author tends to propose a secure information sharing theme for dynamic members. First, author tend to propose a secure manner for key distribution with none secure communication channels, and therefore the users will firmly obtain their non-public keys from cluster manager. Secondly, author can do fine-grained access management; any user within the group of members will use the supply within the cloud and revoked users not able to access the cloud once more once provider revoked. Third, author is able to shield the theme from collusion attack, which suggests that revoked users cannot get the initial record though conspire with the untrusted cloud. In existing approach, by investing polynomial perform; author are able to attain a secure user revocation theme. Finally, author can provide the non-public key for security where the user needn't update, hence no need for a replacement of user joins within the cluster or a user is revoked from the cluster.

III. PROBLEM STATEMENT

The system, which is followed at present, is a scheduled system. The data's will be backed up only on the basis of scheduled update.Important drawback of existing system is time factor and data storage. The data loss is also most important factor in the existing system. Representative network architecture for CLOUD data storage is in three different network entities can be identified as follows: User: users, who have data to store 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 optimal 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 [11].

IV. PROPOSED METHOD

In the proposed system, the saving/current account holders can check their account balance; list of transaction done by the user, and the account personal information can be edited efficiently. Each account holder will be provided with the unique user id and password by the bank, through which it can view their personal information. If the intruder deletes the database, the database will be backed up by checking the nearest server, traffic and available storage of the multi-server. The encrypted key will be received immediately by the admin through mail to restore the deleted database. The security can also be given as per the requirement of the users. Security threats faced by CLOUD data storage can come from two different sources. On the one hand, a CSP can be self-interested, untreated 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, Byzantine failures and so on [12, 13]. On the other hand, there may also exists 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 CSP for a certain period. Proposed modules are:

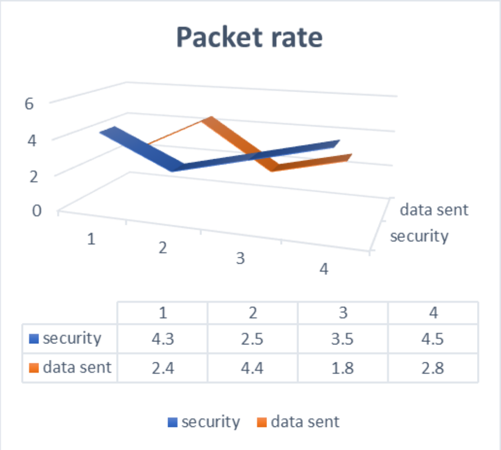
a. Administration: Administrator owns the overall determination of controls, setting of major objectives, and the identification of general purposes, guidance, leadership & control of the efforts of the groups towards some common goals. Admin has the privileges to create the new branches in all of the countries, update the new customer details, existing customers, money transactions, and money deposition. Admin also have the rights to restrict the users and give the access justices to the user to register their details to access the bank account. Admin only set the data backup path for one server to another server.
b. Branch Creation: In this module it will takes admin to create country zone. While creating the country admin need to specify the unique country code and code number for each and every state. According to this project, some limits such as country can have only 10 branches. If it tries to insert more than 10 branches it will provide a message about the limits. If the same country code was used create a new country it will provide a message as country code already exists error message. When proper data was entered for the branch, bank will be creates in that particular country successfully and an acknowledgement will be received.
c. Create Customer: In this module creating the customer's need to specify various information's such as name, address, id proof, pan card number, passport number and branch code. If the customer has any existing account or not, the existing account details of those accounts and the referral account holder information has to be specified. After providing all those information when create customer is clicked in the background process it creates the customer account number, customer ID, card number, and the CRV number.
d. Money Integrity: In this module, it is needed to pass the account number, name of the account holder, branch code, account mode such as credit or debit of the person who is going to deposit. When that information's are passed successfully and when deposit amount button is clicked the amount will be deposited to that account number. A message will appear for the conformation of the deposited amount. Particular account holder bank details will be displayed in the form.
e. Money Transfer: In this module, it is needed to specify the both customers information such as account number, name of the account holder, branch code, account mode credit or debit, and the sender has to specify the amount of transfer. When the user clicks transfer in the back ground process the customer account balance will be checked with the transfer amount. If the customer balance is lower than the amount specified for transfer means an error message is specified for the user and the transaction will be incomplete. When the user has the sufficient balance the transaction will take place successfully the transfer amount will be reduced from the sender amount and that amount will be added to the receiver amount. After those process completed successfully a message will be displayed to the user about the transaction.
f. Personal Banking through cloud: In this module, the saving account holders can check persons own account balance; list of transaction done by the customer, account personal information can be edited efficiently. Each account holder will be provided by a unique user id and password. By using client user id and password, client can view account details of own as well as personal information's. Change password rights are provided to the customer to make own security password.
g. Corporate Banking through cloud: In the Corporate bank the current account holder has the rights to

check account information, list of transaction done in account, Account balance, and Account holder's personal information's. The account holder can view that information only with the unique user id and password provided by the bank. The account holder has the rights to change the password according to the wish to maintain the security. If the account holder provides the wrong user ID or Password it will provide an error.

h. Cloud Formation: Cloud Formation from Web Servers provides an easy mechanism to create and manage a collection of data resources. To use Cloud Formation you create and deploy a template which describes the resources in your stack via your link. Cloud Formation templates are simple JSON formatted text files that can be placed under your normal data source control mechanisms, stored in private or public location servers. When will data lose has appeared while cloud template will call for data security.

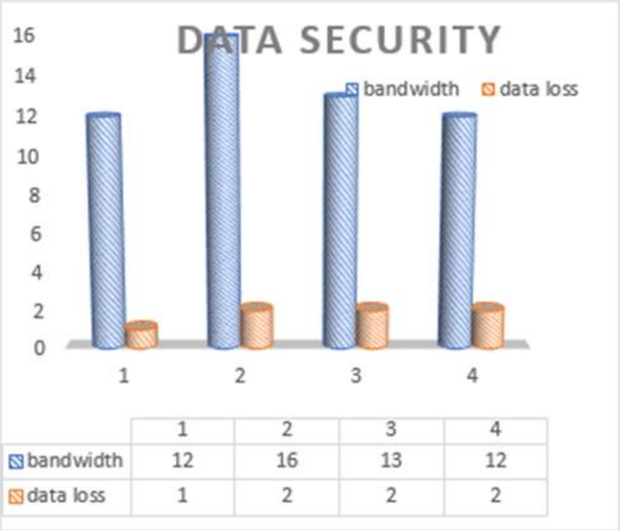
V. EXPERIMENTAL RESULT

The system, which is proposed, now computerizes all the details that are maintained manually. Once the details are fed into the computer there is no need for various persons to deal with separate sections. Only a single person is enough to maintain all the reports. The security can also be given as per the requirement of the users. It also helps client to give timing task then could give the receipt also in print out format. Security threats faced by CLOUD data storage can come from two different sources. On the one hand, a CSP can be self-interested, untreated and possibly malicious.



	1	2	3	4
■ security	4.3	2.5	3.5	4.5
■ data sent	2.4	4.4	1.8	2.8

Chart 1: Data Packet rate



	1	2	3	4
▨ bandwidth	12	16	13	12
▨ data loss	1	2	2	2

Chart 2: Data security

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, Byzantine failures and so on.

VI. CONCLUSION

It is concluded that the application works well and satisfy the users in cloud computing. The application is tested very well with security issues and errors are properly debugged. The site is simultaneously accessed by more than one system in cloud. Simultaneous login from more than one place is tested. The site works according to the restrictions provided in their respective browsers. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one. The speed of the transactions become very high compared with normal. The account holder can view that information only with the unique user id and password provided by the bank. After those process completed successfully a message will be displayed to the user about the transaction. If the account holder provides the wrong user ID or Password it will provide an error. If the intruder deletes the database, the database will be backed up by checking the nearest server, traffic and available storage of the multi-server. The encrypted key will be received immediately by the admin through mail to restore the deleted database. It also generates the key that will be mailed to admin, so that the admin can back up the deleted files to its original server using the encrypted key. The main concentrate on security issues and explain about using homomorphism token with distributed verification of ensure code data. Using homographic token improves security in terms of finding out misbehaving servers, security operations on data blocks including security for updating, deleting and modifying data.

REFERENCES

[1] Q. Wang, K. Ren, W. Lou, and Y. Zhang, “Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance,” Proc. of IEEE INFOCOM, 2009.

[2] Amazon.com, “Amazon Web Services (AWS),” Second Edition.

[3] D. Carman, P. Kruus, and B. Matt, “Constraints and Approaches for Distributed Sensor Network Security,” Technical Report 00-010, NAI Labs, 2004.

[4] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom’ “Cloud Computing Security: From Single to Multi-Clouds”, International Conference on System Sciences, 2012.

[5] SMEStorage: smestorage, Multi-cloud storage provider.[online]http://code.google.com/p/smestorage/ . [cited: January-2014].

[6] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg , Qianhui Liang , Bu Sung Lee, “TrustCloud: A Framework for Accountability and Trust in Cloud Computing” 2011 IEEE World Congress on Services.

[7] Muhammad RizwanAsghar, Mihaela Ion, Bruno Crispo, “ESPOON Enforcing Encrypted Security Policies in Outsourced Environment”, 2011 Sixth International Conference on Availability, Reliability and Security.

[8] Luca Ferretti, Michele Colajanni, and MircoMarchetti, “Access control enforcement on query-aware encrypted cloud databases” IEEE 2013.

[9] S. Kent and R. Atkinson, “Security architecture for the Internet protocol,” IETF RFC 2401, November 1998.

[10] Ankita Ajay Jadhav, “Anti Collusion Data Sharing Schema for Centralized Group in Cloud”.

[11] Saranya.J, “Design for secure data sharing in multi clouds using Luby Transform codes with DES”.

[12] Alisha Jindal, “Enhancing Data Integrity in Multi Cloud Storage”, ISSN: 2248-9622, Vol. 4, Issue 9.

[13] Namita N. Pathak, “Enhanced Security for Multi Cloud Storage using AES Algorithm”, Vol. 6 (6), 5313-5315, 2015.