Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.303 – 310

RESEARCH ARTICLE

A Security Integrated Data Storage Model for Cloud Environment

Sonia Rani
Student, M.Tech (CSE)
GITAM, Kablana, Jhajjar, Haryana
Soniya_sharma84@rediffmail.com

Neetu Sharma
HOD, CSE Department
GITAM, Kablana, Jhajjar, Haryana

Abstract: Security is one of the basic aspects required in any network model. But when the access is on some shared system such as Cloud, the security criticality is increased. This kind of system is defined along with service and resource sharing services as well as to perform the data management effectively. These services are integrated with public as well as private environment. Cloud System, increases the criticality because of available limited resources in mobile devices. In this present work, a three stage security model is presented for Cloud Environment. The work is applied on secure file management and distribution over the secure Cloud environment. The paper included the exploration to the proposed security model.

Keywords: Cloud Computing, Security, Data Security, Data Management

I. INTRODUCTION

Cloud computing is the evolutionary distributed platform to provide the services, resources and the hardware in an integrated environment to cloud users. It helps a user to use the storage system, hardware and these application software without performing any deployment or installation. Cloud computing is becoming one the most popular technology among the business enterprises because of infrastructure reduction and cost reduction. The users are also attracted to this environment because of fast and integrate service access over the cloud system. The cloud system itself defines different platforms, services, applications to all public, private and limited users. Beyond the effective

integration between the cloud servers and clients, it also suffers from security challenges because of its global virtual environment[1][2].

Security is the key issue associated with cloud system that is required on client side as well as on vendor side. The security requirements in this public environment are shown in figure 1. The main consideration among these issues is the authentication and the authorization issue. This security concern shows the threats again the hacking and the malware activity in the cloud system[3][4]. Once the authentication is proven, the next work is to perform the secure communication so that the reliable data will be transferred to cloud server and to client side in secure way. Another security concern of cloud system is the authorization as well as access control. Authorization is about to avail the services, products or the resources based on the profile match as well as to keep safe the information from others. The profile match defines the user level identification to achieve the security. The trust level analysis also comes under the security specification. The trust is analyzed for the customer as well as the vendor.

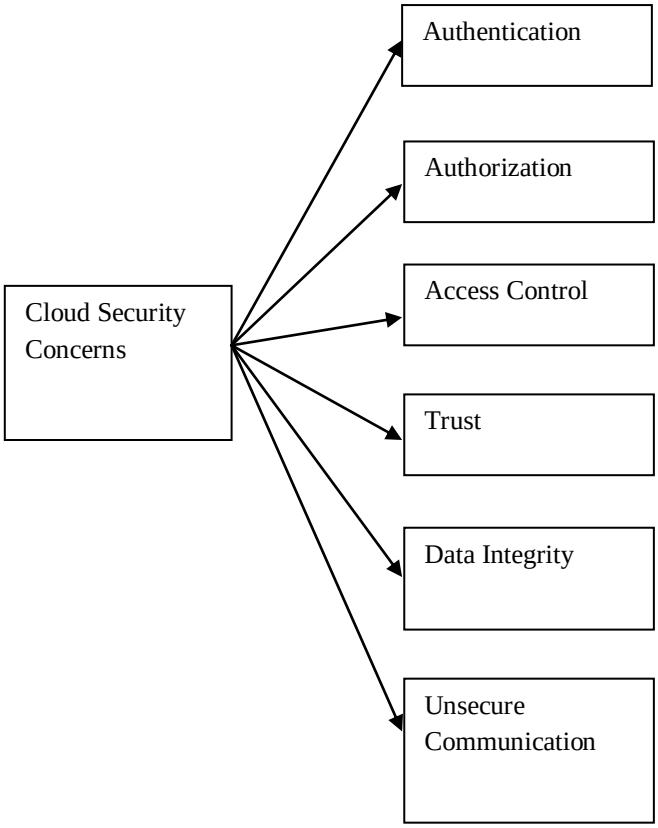

Figure 1 : Security Concerns in Cloud System

The trust certificates are distributed to proven the trust. The data integrity is the security issue that deals with the data distortion or the error generation in the data communication or the availability. The most concerned issue in the security system is the communication level security[5][6]. When the data is being transferred, the issue can be in the form of attacks or the incomplete transaction. The session level security is defined to handle these kinds of problems in cloud system.

A) Cloud Service Architecture

Cloud system is an organized architecture that is defined in several means. One of such effective representation is the service level based architecture. This architecture is defined with three main service layers or the model called IaaS, Paas and SaaS. The IaaS (Infrastructure-as-a-Service) is described as the machine on demand service that avail

the physical resources or the hardware in the form of remote service to the customer. PaaS (Platform-as-a-service) is defined as the complete application environment by using which the developers can interacted with development software in a shared remote server system. SaaS (Software-as-a-Service) gives the concept of public cloud where an end user can interact to the system in an integrated environment and multiple vendors are available to provide the requested services[7][8].

In this paper, the security aspects related to the cloud service model are explained. These aspects include the issues and the relative solutions. In this section, the exploration to the cloud system and its security concerns is defined. This section also explained the cloud service model. In section II, the Cloud Architecture is defined. In section III, the work cloud service security models are explained along with issues and the solutions. In section IV, the conclusion of the paper work is described.

II. EXISTING WORK

Security is always one of the most common and open research area, because of this lot of work is already done in the area of security system in cloud environment. In this section, some of the work done by the earlier researchers is discussed.

V. D. Cunsolo performed a work to achieve the information security in distributed system. To resolve the security problem in network based distributed system, author suggested a light weighted cryptographic approach. The objective of work was to provide a secure asymmetric approach to provide secure communication of data as well as file system. Author proposed a secure distributed file system with asymmetric or symmetric structure. Author defined the secure interfacing with cloud and grid based systems[4]. Christian Schridde provided a secure cloud infrastructure based work to provide the security over the cloud system. Author presented a secure infrastructure to provide service over the cloud environment. The work includes the identity based cryptographic model based on public key system. Author provided the cloud based data transmission under the trust analysis. Author also provided the comparative analysis between the approaches[5]. Yingjie Xia defined a ECC model over the cloud system to improve the security on cloud system. Author defined a hybrid ECC system for cloud data. It provided a platform to provide secure file communication, backup system and the resource sharing on distributed cloud. Author provided different security levels for different kind of cloud and avail different secure services with confidential protocol and privacy. Author combined the hash key based cryptography and enhance it using ECC to provide secure user control system[6].

Ching-Nung Yang[1] has defined a work on data security and integrity in cloud environment to perform reliable service distribution in cloud networks. Author defined a data or storage oriented secure service distribution mechanism so that the service distribution benefit will be taken by the cloud users. Author defined a work on key based authentication for cloud security analysis. Author used a combined secure approach for information sharing using ECC and Diffie Hellman approach. Author used the symmetric bivariate polynomial information sharing system for cloud environment. Author defined a trusted third party system where multi-server system is extended to get fit to the environment. Author defined a multi server system so that effective secure servive provider is established. Author proposed an effective secure service mechanism in cloud environment. Yingjie Xia [6] defined a virtualization process for the military cloud. Author defined the secure communication using cryptography for the military based system. Author provided the secure sharing over the cloud environment under the hardware based data communication with cryptographic security. Author defined an approach called infrastructure virtualization to achieve the secure communication over cloud. Author also performed a secure verification of the system in cloud environment. Author defined the secure kernel system to achieve the systematic secure transmission in cloud system. Jonathan A.P. Yanping Xiao [7]presented a secure middleware in cloud environment. Author defined a survey on this middle ware technology under different platforms such as AppScale, Altocumulus, Cloudify etc. Author also presented the analytical study over the cloud to achieve the secure integration and provide a security standard for the future technology research..

Vasyl Ustimenko [9] presented a key based secure and scalable cloud environment for the application based security. Author provided a trustful cloud environment to provide the secure communication based on secure key management scheme. Author provide provided the secure application mechanism to achieve the coordination between the owner and multiple users.

Chang-Ji WANG[11] provided the attributed oriented encryption analysis with constant size with cipher text. Author provided a new cryptographic algorithm to provide the fine grained data sharing with decentralized access control system. Author defined the secure key policy system with cipher text and to achieve the attribute and private key association over the system. Author provided the trustful cloud storage over the cloud system under the KP-ABE scheme. Author defined an application level secure system to embed the security under the cloud storage environment. Author defined the monotonic structural access over the cloud system and also provided the secure key exchange mechanism using Diffie Hellman algorithm. Dexian Chang[10] defined a trust analysis on cloud environment. Author defined the trusted relationship over the cloud environment under the flexibility and scalability parameters. Author defined the cloud virtualization under the different user domains. Author defined a trusted service domain for multiple user domains to achieve the cloud virtualization platform. Author also provided the inter domain communication and migration facility to provide the reliable communication over the system.

M.Venkatesh[8] defined a work over the secure data storage in cloud system with public auditability. Author uses the internet feature and software support to improve the communication capability in the cloud system. Author defined the secure remote communication to utilize the cloud resources. Author used the RSA based secure storage system with public auditing to improve the cloud system. The public key cryptography is here implemented to improve the security support along with reduction of the computation time on cloud system. Obtained results show that the work has improved the security over the existing method.

III. CLOUD ENVIRONMENT

Cloud is a substitute to Cloud environment but it also gives the extension to the traditional cloud architecture. This extension is in terms of service and new features included to cloud structure. These services and features are included in the cloud environment in terms of API so that the new integrated cloud storage and synchronization application can be designed. Cloud provides a free service to the storage and fee based architecture so that effective and secure storage of data, photos and other media information can be stored. The cloud environment is defined with big data centers of Cloud servers. Apple provide such cloud architecture so that Application free environment will be generated[13][14].

Cloud is fully integrated with mobile devices including the iPhone, iPod, iPad etc. Different platform environment support the Cloud architecture. The Apple TV and computer based operating system so that the use of parts of Cloud, photos and music. This cloud system is defined with SaaS model along with integrated IaaS model[15]. The architecture of Cloud system is shown in figure 2.

Once the Cloud is activated, the user can choose the settings respective to the supported applications. These settings are data oriented to identify Cloud is storing the data or not. There are number of separate setting page so that the relative options will be selected and identified. Cloud defined the work on internet connection. Author defined the connection based on differnt version of the document. Cloud is specially designed for apple applications. It also controlled by Microsoft Windows and the control panel so that the mails, nodes and photo features will be transmitted effectively[16].

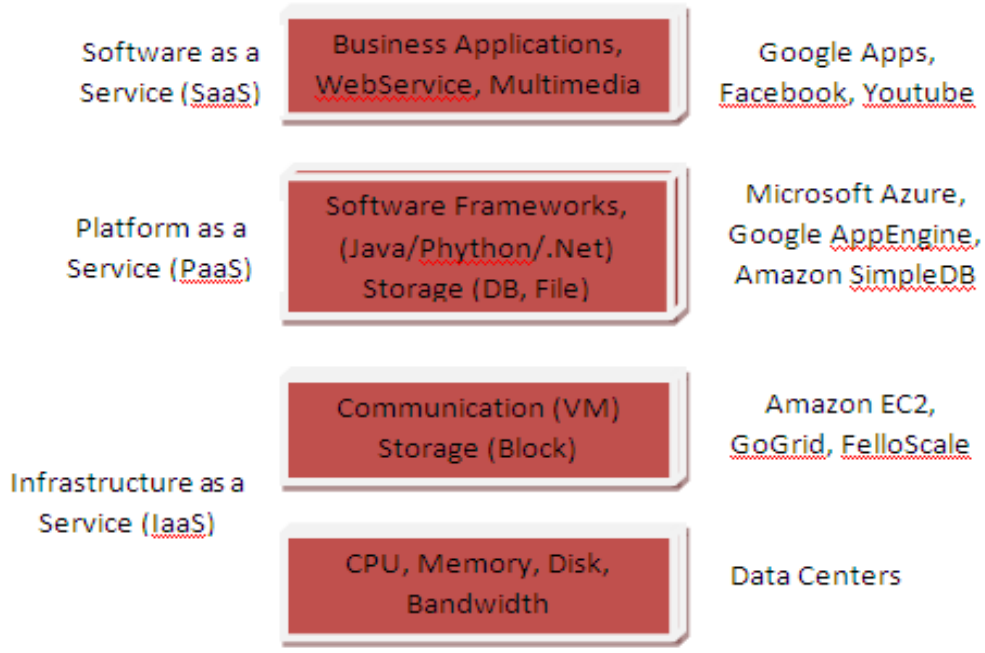

Figure 2 : Cloud Architecture

IV. PROPOSED MODEL

Today instead of maintaining the data on individual system, whole data and information is generally placed on some centralized system with distributed environment. Such distributed system can have multiple service providers as well as multiple users. This kind of environment is provided by Cloud environment. A Cloud is the distributed system for new era that provides the shared and distributed infrastructure, services and the products. It provides a model based environment adapted by most of the web clients to avoid the individual installation of software, security etc. As the Cloud system is open publicly using internet, it is having the main challenge in the form of security.

The presented work is about to provide the secure communication with data Cloud for the public and private access over the system. In most of the existing approaches a generalized cryptographic approach is implemented to achieve the security over the Cloud system. In this work a user perspective security scheme is been presented. According to this approach, to a secure tunnel based transmission is provided for the frequent communicating authenticated users. For such users, one time authentication will be performed using RSA algorithm. Once the session is established, SSL layer is activated to provide the secure transmission over the Cloud. The second level of security is provided for the authenticated Cloud users that avail the Cloud services rarely. For such users, each time authentication is performed using RSA approach but no tunnel will be defined. At the final stage, for the free uses, a RSA based authentication will be performed and allow the public area for the access.

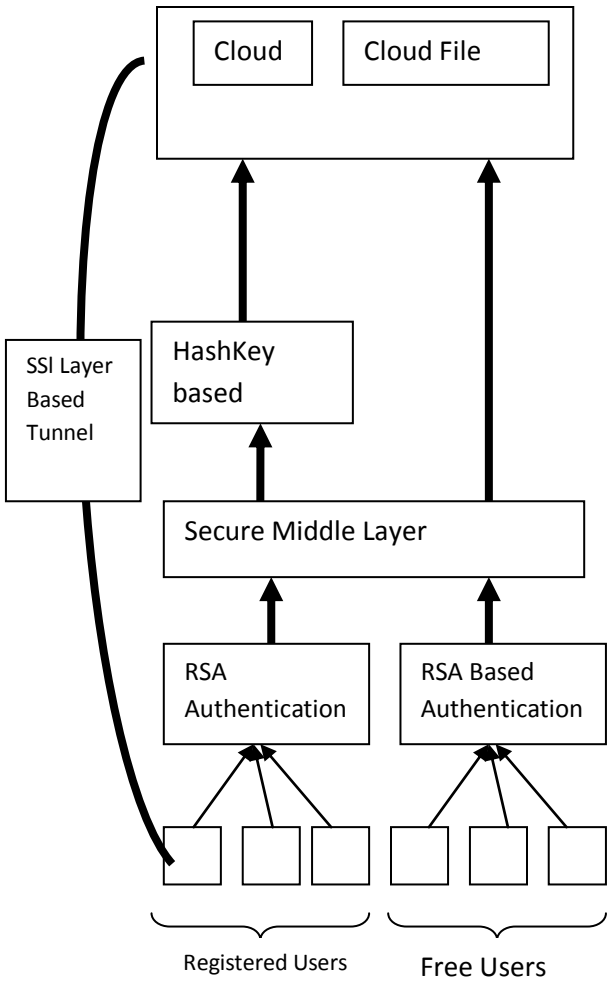

Figure 3 : Proposed Model

As shown in the figure, the Cloud server is having the raw data or the file as the available data resources. System can have single or multiple Cloud system. This Cloud server is the top layer that will provide the resources to all users publicly. The users that will perform the data request can be registered user or the free visiting users. The security is here mainly incorporated for the registered users. To provide the security over the system, security is here implemented on the middle layer called the security layer. The work of this security layer is divided in three parts.

A) Authentication

The authentication is here provided at two levels. For the free users, the authentication is provided using RSA cryptography approach where as for the registered users, the authentication will be achieved using hash key based RSA algorithm. As the user will enter to the system, the authentication check will be performed using the cryptographic approach. A free user is a visiting user that can visit the public pages of the Cloud but cannot perform any data oriented operation over the Cloud. But the registered user is allowed to perform the data downloading on Cloud.

B) Secure Session

If the authenticated register user wants to download some data from the Cloud server, the session key will be generated. This key will be activated for the specific period. As the session will be established, the next work is perform the secure data transfer on client end from the server. To perform this secure transmission SSL enabled secure tunnel will be generated between the client and the server with specific bandwidth. The communication will be performed using this tunnel. As the communication will end, the session key will be deactivated.

C) Secure Data Management

Data over the cloud will be managed in the cryptographic form. To perform the data encryption over the cloud the RSA based cryptography approach will be implemented.

V. CONCLUSION

In this paper, an exploration to the Cloud service model and the integrated security aspects is defined. In this work, a three stage security model is suggested that combines the authentication, secure data management and secure data transmission over the system.

REFERENCES

[1] Minqi Zhou, Rong Zhang, Wei Xie and Weining Qian, Aoying Zhou, Security and Privacy in Cloud Computing: A Survey. Sixth International Conference on Semantics, Knowledge and Grids., 2010.

[2] Jianfeng Yang and Zhibin Chen, Cloud Computing Research and Security Issues. 2010

[3] Louis J. Freeh, Keynote talk at International Cryptography Institute, Sept. 1995. Available through http://www.fbi.gov/crypto.htm .

[4] V. D. Cunsolo, Achieving Information Security in Network Computing Systems, Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009

[5] Christian Schridde, An Identity-Based Security Infrastructure for Cloud Environments, 2010.

[6] Yingjie Xia, Hierarchy-Aware ECC Model for Cloud, 2nd International Conference on Industrial and Information Systems, 2010

[7] Yanping Xiao, An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing, 2010

[8] M.Venkatesh, Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing, 2012

[9] Vasyl Ustimenko, On some mathematical aspects of data protection in cloud computing, 2012

[10] Dexian Chang, TSD: A Flexible Root of Trust for the Cloud, 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012

[11] Chang-Ji WANG, A Key-policy Attribute-based Encryption Scheme with Constant Size Ciphertext, Eighth International Conference on Computational Intelligence and Security, 2012

[12] Sahil Madaan, Implementation of Identity Based Distributed Cloud Storage Encryption Scheme using PHP and C Languages on Linux Platform, 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012

[13] Tamal Kanti Chakraborty, Enhanced Public Auditability & Secure Data Storage in Cloud Computing, 2012

[14] Apache Cloud nextgen mapreduce (yarn) http://Cloud.apache.org/docs/ current/Cloud-yarn/Cloud-yarn-site/YARN.html.

[15] AN INTRODUCTION TO THE CLOUD DISTRIBUTED FILE SYSTEM HTTP://WWW.IBM.COM/DEVELOPERWORKS/LIBRARY/WA-INTROHDFS

[16] Selic, B. (2004) Fault tolerance techniques for distributed systems. IBM.http://www.ibm.com/ developerworks/rational/library/114.htm

[17] Jared Evans CSCI B534 Survey Paper. "Fault Tolerance in Cloud for Work Migration" http://salsahpc.indiana.edu/b534projects/sites/default/files/public/0_Fault%20Tolerance%20in%20 Cloud%20for %20Work%20Migration_Evans ,%20Jared %20Matthew.pdf

