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. 5, Issue. 2, February 2016, pg.39 – 45

A Hybrid Security Model for Distributed Cloud Management

Ankita Singh

Student, M.Tech (CSE), Deenbandhu Chhotu Ram University of Science and Technology, Murthal

Dr. Parvinder Singh

Associate Prof., M.Tech (CSE), Deenbandhu Chhotu Ram University of Science and Technology, Murthal

Abstract— Cloud system is gaining the importance in public environment. But security is always a critical challenge while sharing the valuable information. In this work, a high level integrated security model is presented for managing large data on cloud system. In this work, a RSA integrated SHA method is presented to provide the secure file management in distributed cloud. The proposed authentication and cryptographic model has provided the security for public and private cloud system. The work ensures the communication level, user level and file level security. The efficiency results show that the model has improved the security and the reliability in the system.

Keywords: SHA, Public Cloud, File System, Authentication, Communication

I. INTRODUCTION

Cloud system provides the platform to share the services and the products among distributed users. The global clients of cloud systems are dependent to the domain, platform and the services. These services are provided by multiple cloud service systems and service providers. Most of these services are available in public environment with authentication checks. While providing the services, some of the checks and the rules are decided to avail the services to particular client or the client. The services are dedicatedly provided based on the service level analysis, requirement level analysis and the security constraint level analysis. The basic model of cloud service distribution policy is shown in figure 1. The model defined here is generic to the service or the domain type. It is applied in each public cloud system for sharing of services and the products.

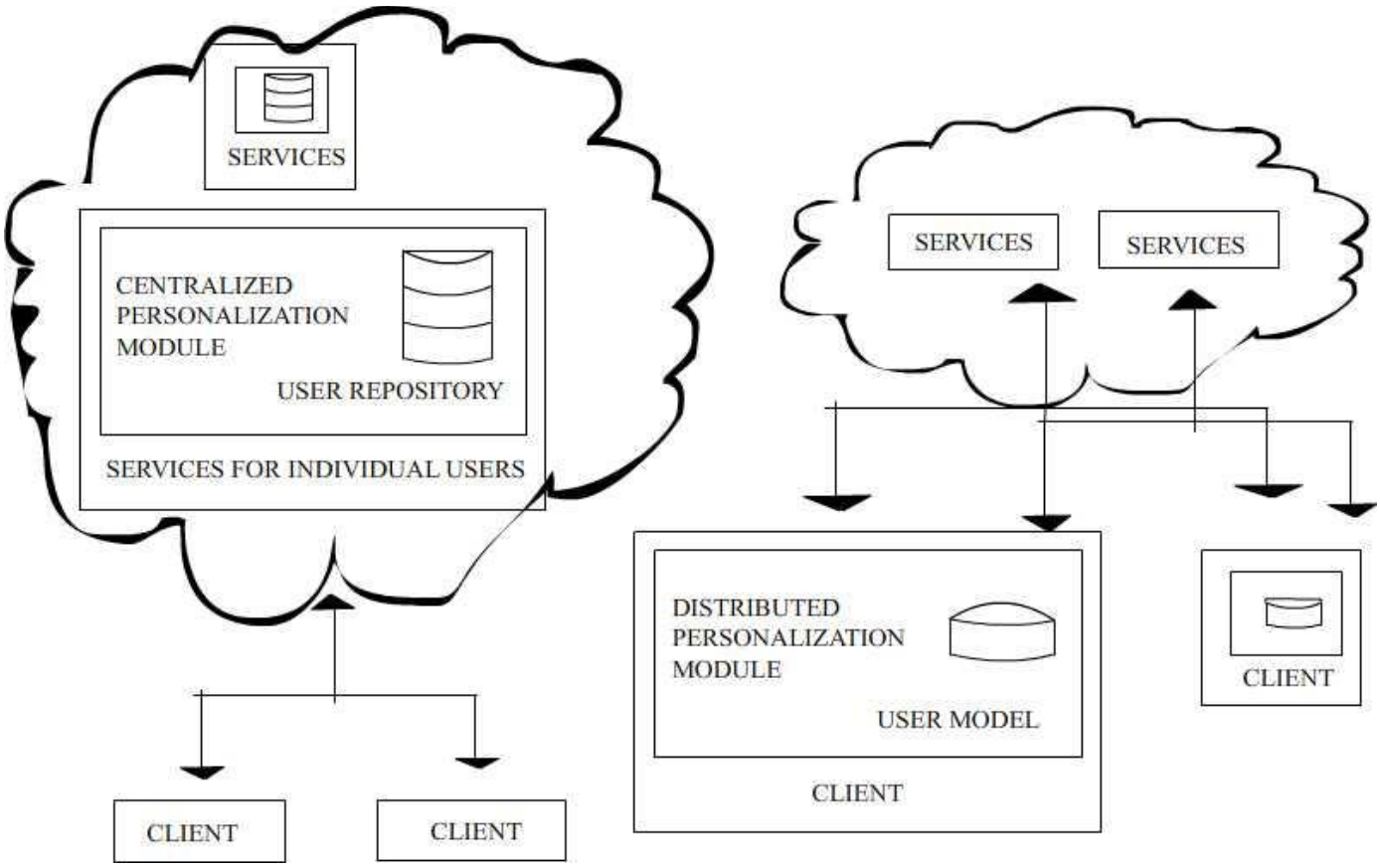

Figure 1 : Public Cloud Model

The model here shows the integration of these services along with the availability with the client after performing the user check. The authentication is the first level verification applied with authorization check to avail the right services to right user. The figure is showing the user level modeling in the cloud environment. This kind of check is required to achieve the integrity, security and the reliability while performing the communication in open environment. In more dedicated security systems, the authentication check is applied relative to the information type or the domain type. The content and the history level analysis are also the key aspects to improving the security in cloud environment.

In this paper, a hybrid security model is presented for public cloud environment. The work is here defined dedicatedly for the cloud security improvement while managing the larger files. The work model has combined the RSA and SHA methods to improve the reliability and security. In this section, the cloud system is described relative to the user perspective. In section II, the work defined by earlier researchers is discussed. In section III, the proposed research methodology is described. In section IV, the analytical results obtained from the work are presented. In section V, the conclusion of the work is presented.

II. RELATED WORK

Cloud System is one of the major research area for which the contribution of lot of researchers is present. Some of the work provided by earlier researchers is presented in this section. Author[1] provided a work on the cloud service allocation and the risk assessment in the distributed cloud. Author provided the provided the computing capabilities analysis along with the security issue observations so that the cloud service system will be handled effectively. Author provided the handling of the system with risk level observation so that the security aspects will be improved. Author provided the observations at the risk level so that the dedicated points can be found the resource level updation can be done. The method includes the service level and the server level assessment over the cloud system to improve the system security upto high extents. Author provided the

resource management under security aspects so that the risk reduction will be achieved. Author[2] provided a work on improved security system with specification of communication and user level security with specification of file aspects and the authentication aspects. Author provided the featured analysis along with the secure information derivation so that the quantized aspect analysis can be achieved for cloud system. Author provided a work on security metric based assessment to provide the service level agreement between the cloud system and the user. Author achieved the web service driven estimation to achieve the aspects and the relative derivation so that the integrity modeling and the reliability driven aspects can be achieved from the cloud system. Author incorporated the security arrangement along with the service modeling. Author[3] provided a work on secure service level for cloud system to improve the secure and integrity. Author provided the transaction level observation while performing the service agreement. Author provided the assessment based on the framework observation along with QoS level assurance. Author provided the service communication analysis with architectural improvement with security measures. Author identified the risk assessment so that the information tracking will be done more effectively.

Author[4] provided a comparative analysis to generate the risk observations and to evaluation the service aspects under the environmental constraints so that the effective communication will be performed. Author provided the work to reduce the risk and threats to improve the security and reliability. Author improved the security updation in cloud and grid environment at infrastructure level and at service level. Author also achieved the comparative observation on various associated aspects. Author provided the derivation in the cloud system and environment to gain the specific communication with high security measures so that the reliability and integrity of system will be improved. Author[5] provided a work on security solution so that the reliable communication derivation and security issue. Author provided the effective issues and measures so that the information tracking will be done more reliability. Author provided the analysis on security methods. Author[6] provided a work on derivation on assessment on cloud system along with the specification of the associated framework..Author discussed the system under different security issues and presented the test under different vectors such as scalability, efficiency and cost etc. Author defined the system as a management framework approach under 5 key points called user requirement analysis, service analysis, risk analysis, third party review and the desktop assessment. Author provided the system review under the trust and reliability models. Jijun Zhang[7]presented another work on risk analysis .Author performed the parametric analysis under the security risk. Author defined a security analysis and indicator system that performs the assessment under different security vectors under forward assessment approach. Maneesha Sharma[8]performed a work, "Cloud Computing: Different Approach & Security Challenge". Author provides a study on different security aspects and relative challenges. Author defined the cloud security as the main factor while selecting the cloud server or the services. Different cloud service issues are integrated to the system so that the effective tracking is done. Sheng Jen Jian[9] author defined a cloud based decision support system under the risk analysis under heart disease assessment. Author presented a fuzzy expert system. Author defined the analysis under ANOVA vector. Author defined a risk factor based cloud analysis under the system tune-up mechanism. Author defined the system for public environment under different impact factors. Sneha Prabha Chandran[10] performed a work on the risk analysis in cloud system environment. Author defined different risk factors along with relative issues and the integration. Author provided the risk assessment and measure so that the risk relative to the data integrity is reduced and resolved upto an extent. Author provided an analysis on different risk measure so that the security decision can be taken at earlier stage.

III. RESEARCH METHODOLGY

In this present work, a Cryptographic based security model is defined to provide secure file management on cloud server. The work is here defined in two main stages. In first stage, the hadoop based file system manager is defined with associated operations. These operations includes, file uploading, downloading and forwarding. In second stage of this model, the security is integrated with each process stage of cloud server. The first level security is achieved using authentication. It means only the private users or the authenticated users can communicate with cloud server.

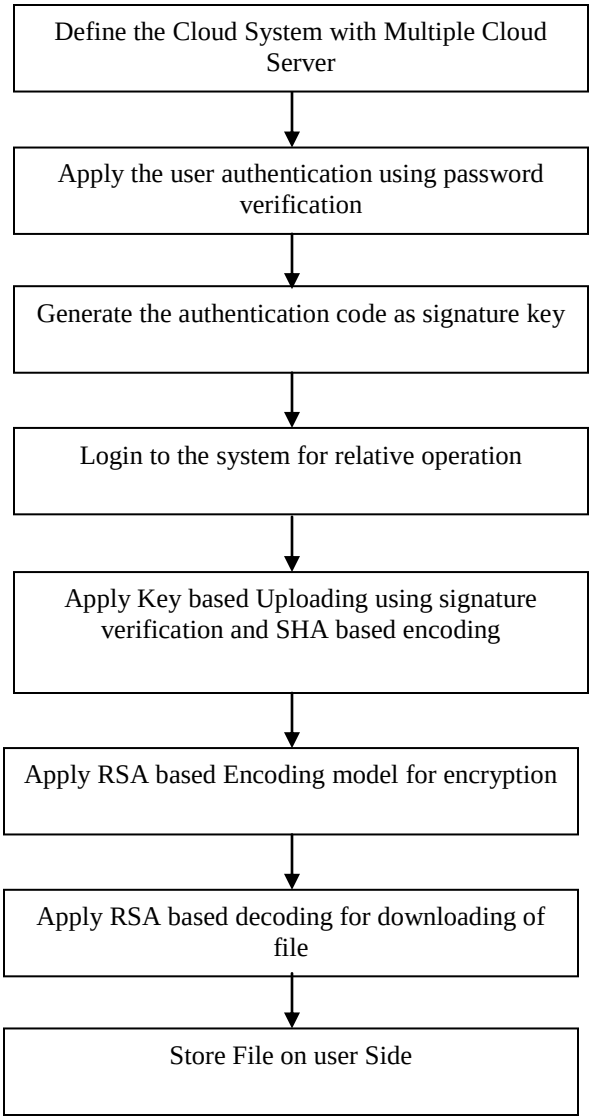

Figure 2 : Proposed Model

Once the authentication is proved, the user can upload and download the file. In this stage, the data management on hadoop based cloud server is done using Cryptographic technique. This technique is based on the user signature based cryptography. This cryptography is applied using hybrid RSA and SHA algorithm. Instead of whole information code, the signature is here used to provide the secure data management. In final stage, the communication over the cloud server is also secured. The model is described in figure 2

The presented work is here defined to provide the information security and secure data or file management on cloud server. The real time files are uploaded on cloud server and same information is downloaded. But to provide the relative file management operations some of the associated information is also maintained on cloud server. The algorithmic specification is shown in table 1.

Table 1 : Algorithm

Algorithm(CloudServer,Client)
/*CloudServer is providing the distributed generalized cloud service for file managent. Client is the user who want to avail the defined cloud services*/
{
1. Initialize the Cloud Server in association with relative services for file uploading, downloading and forwarding.
2. If(CheckAuthetnication(Client,CloudServer)=Fail)

[As a new client enter to the system, the verification on cloud server, if authentication fail, no file level communication will be performed]
{
3. Register(Client, CloudServer)

[If Client is new, then registeration of client can be done]
}
4. Upload File for Secure Information Storage over the Cloud Server
5. KeyPair=GenerateKey(Client,File)

[Generate the Key Pair to upload the file over the cloud server]
6. MsgBlocks=Split(File, BlockSize)

[To perform the Cryptography Divide the Message is smaller blocks]
7. For i=1 to MsgBlocks.Length

[Process all the Message Blocks]
{
8. Seq=GenerateSeqTransition(MsgBlocks)

[Perform the Block Sequence Transition over the message blocks]
9. Define Hexa Blocks to perform the hash mapping over the data codes
10. Generate Aggregative Haxa Blocks
11. Perform EncryptedMessage=Mod($Text^{PrivateKey}$,N)

[Apply The Key based Encoding]
Return EntryptedMessage
}

IV. RESULTS

The analysis of this presented work is defined respective to the time taken for encryption and decryption. The work is applied for multiple files. The comparative analysis is defined using proposed Cryptographic technique and RSA based encryption model. The comparative analysis of the simulation time is here defined for different files. The simulation time based comparison is defined in this section. The comparative observations are taken against the RSA based security and the comparative observations are taken against the time taken in encryption and decryption process.

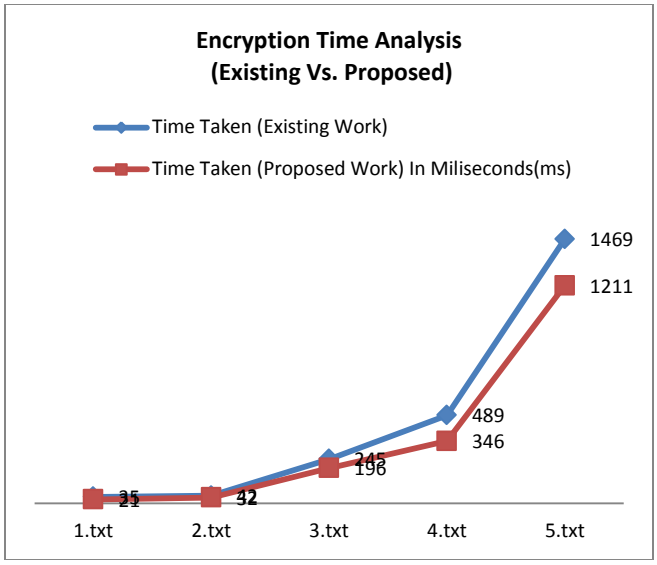

Figure 3 : Encryption Time Analysis (Existing Vs. Proposed)

Here figure 3 is showing the encryption time analysis applied over the input files. The results shows that the encryption time in proposed work model is always lesser then existing approach.

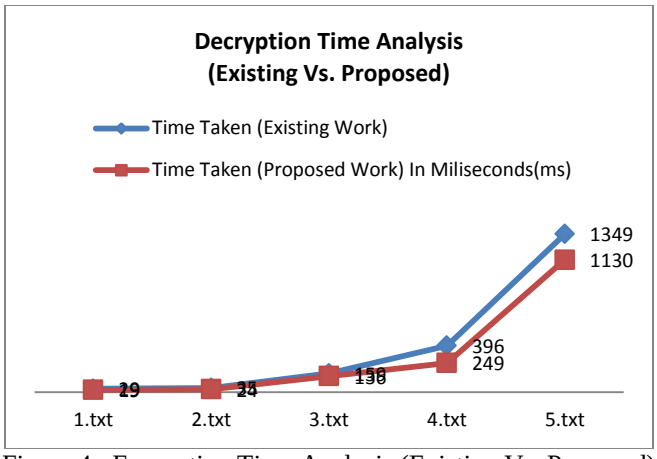

Figure 4 : Encryption Time Analysis (Existing Vs. Proposed)

Here figure 4 is showing the encryption time analysis applied over the input files. The results shows that the encryption time in proposed work model is always lesser then existing approach.

V. CONCLUSION

In this paper, a hybrid security model is presented for public cloud system. The proposed security model combined the features of RSA and SHA method. The RSA where used for signature map, the SHA for applying the cryptography. The comparative results shows that the model has improved the efficiency and the security in cloud system.

REFERENCES

[1] Liu, S. (2013). VMRaS: A Novel Virtual Machine Risk Assessment Scheme in the Cloud. IEEE 10th International Conference on Services Computing 978-0-7695-5026-8/13 © 2013 IEEE .

[2] Shetty, S. R. (2013). Security Risk Assessment of Cloud Carrier. IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing , 442-449.

[3] Hammadi, A. M. (2012). A Framework for SLA Assurance in Cloud Computing. 26th International Conference on Advanced Information Networking and Applications Workshops.

[4] Lim, C. (2012). RISK ANALYSIS AND COMPARATIVE STUDY OF THE DIFFERENT CLOUD COMPUTING PROVIDERS IN INDONESIA. International Conference on Cloud Computing and Social Networking , 1-5.

[5] Sanchez, D. M. (2012). Comparison between security solutions in Cloud and Grid Computing. International journal of Advanced Research in Computer Engineering and Technology .

[6] Xie, F. (2012). A RISK MANAGEMENT FRAMEWORK FOR CLOUD COMPUTING. IEEE CCIS2012 978-1-4673-1857-0/12 .

[7] Zhang, J. (2012). A Research on The Indicator System of Cloud Computing Security Risk Assessment. IEEE .

[8] Sharma, M. (2012). Cloud Computing: Different Approach & Security Challenge. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307

[9] JIAN, S. J. (2012). A CLOUD DECISION SUPPORT SYSTEM FOR THE RISK ASSESSMENT OF CORONARY HEART DISEASE. Proceedings of the 2012 International Conference on Machine Learning and Cybernetics

[10] Chandran, S. P. (2012). Cloud Computing: Analysing the risks involved in cloud computing environments. Proceedings of Conference of Computer Science , 1-5.

