Improving privacy and security of data using Secured Distributable Cloud Storage (SDCS)

Padmanaban K[1], Lakshmi.B[2], Keerthana R[3], Hemavaasanthi E[4]
Asst. Professor (SS) [1], III Year B.E. CSE[2 3 4]
Department of Computer Science and Engineering,
Rajalakshmi Engineering College, Chennai.
padmanaban.k@rajalakshmi.edu.in[1], lakshmi.b.2014.cse@rajalakshmi.edu.in[2],
keerthana.r2.2014.cse@rajalakshmi.edu.in[3], hemavaasanthi.e.2014.cse@rajalakshmi.edu.in[4]

***Abstract*:** Cloud Computing is a recent BUZZWORD in the IT world. Behind this fancy poetic phrase there lies a true picture of the future of computing for both in technical perspective and social perspective. There are three issues that we are going to consider in cloud computing. First is Security Issue, security loss says about how the data is being used by the server providers. They try to business your data that you have stored in their servers. To overcome this Issue, we use the concept of Distributed Storage System**.** Second one is Data Loss, the problem of the ever increasing threat of Malware and Ransomware to cloud storage has led to the option of storing a copy the user data on Proxy Server**.** Third is, issues on Hacking, it is illegal access of data. Hackers are the crackers who hack the data during transmission of data either for social good purpose or for personal purpose. Cryptographic Data splitting with dynamic approach is used for securing information.

Keywords *– Secured Distributable Cloud Storage, Security, Data Integrity, Cryptography, Dynamic Splitting of Data, 3DES*

*****

1. PROBLEM ANALYSIS

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process the data in third party data centers. Some of the problems arises due to this. The various issues in cloud computing are as follows:

Security issue - There are number of security concerns associated with cloud computing. These issues fall into two broad categories namely

- Security issues faced by cloud providers
- Security issues faced by their customers

The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their applications and use string passwords and authentication measures. When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insiders attacks. According to a recent cloud security alliance report, insider attacks are the sixth biggest threat in cloud computing. Therefore, cloud service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, cloud service providers often store more than one customers' data on the same server. As the result, there is a chance that one users' private data can be viewed by other users. To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

Data loss - Cloud service providers find themselves in a struggle balancing responsibility for maintaining data integrity with delivery cost effective solution to their customers, all the while protecting their own data assets and bottom line. Basic types of data loss includes include DATA DESTRUCTION, DATA CORRUPTION AND UNAUTHORISED DATA ACCESS. The reason for these types of loss is varied and include infrastructure malfunctions, software errors and security breaches.

There exist many types of data within a cloud environment. These data types can be classified into general categories or data domains. The importance of these domains, to the constituents of the cloud environment gives rise to the concept of data loss domains or, who is effected most and how much impact is there if the data is lost. The three major data domains are as follows

- PNCE(Provider Non-Customer Effective)
- PCE(Provider Customer Effective)
- CUST(Customer)

PNCE: The data loss domains contains information that belongs to the cloud service provider and has no effect on the customer. This information if lost or damaged will have a significant impact on the provider and their ability to conduct business.

PCE: The domain represents that data which is owned by the provider and significant to the provider for business reasons. Both provider and customer will be impacted in the case of loss and responsibility. Basically the data is shared but primarily falls on the provider.

CUST:The customer owns this data and it is responsible for its protection unless otherwise arranged with the provider. A

customer may choose to have a cloud service provider replicate, back up or protect customer owned data based on an agreement with the provider. these services generally take the form of a financial and service level agreement between the parties.

Hacking - Hacking is someone who SEEKS and EXPLOITS weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment or to evaluate those weaknesses to assist in removing them.White hat is the name given to ethical computer hackers, who utilize hacking in a helpful way. White hats are becoming a necessary part of the information security field whereas the Black Hats hacker who VIOLATES THE COMPUTER SECURITY for a little reason. Blackhats are called as computer criminals.

2. RELATED WORKS

2.1 **Data Security and Privacy Protection Issues in Cloud Computing:** It is well-known that cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn't move them to cloud. The market size the cloud computing shared is still far behind the one expected. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. This paper provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work about data security and privacy protection issues in cloud.

2.2 Data security in cloud computing: This paper discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to it concerning security. The paper will go in to details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. Availability of data in the cloud is beneficial for many applications but it poses risks by exposing data to applications which might already have security loopholes in them. Similarly, use of virtualization for cloud computing might risk data when a guest OS is run over a hypervisor without knowing the reliability of the guest OS which might have a security loophole in it. The paper will also provide an insight on data security aspects for Data-in-Transit and Data-at-Rest. The study is based on all the levels of SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).

2.3 Ensuring data storage security in Cloud Computing: Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

3. PROPOSED SYSTEM MODEL

In this proposed model, ***security*** is mainly focused on the issues related to the data security and privacy aspects in cloud computing. This multi cloud model which is based on partitioning of application system into distinct clouds instead of using single cloud service such as in Amazon cloud service. Due to the enormous growth in transaction volume and size of business application databases. This is particularly true for many successful online service providers, Software as a Service (SaaS) companies, and social networking Web sites. User data will be converted into structured binary data entirely depending on the type of file being encoded and these data will be divided into parts, or shards. Each of these shards will be hosted in multiple servers.

Cloud backup assures that user data is recoverable and protected. With industry-leading encryption and security practices, cloud-based data backup is highly secure in order to maintain ***data integrity***. The servers operate in a group. It relies on a centralized shared disk facility, typically a Storage Area Network (SAN). Each node in the cluster runs a single instance of the database server. Cryptographic data

splitting with dynamic approach is used for ***securing information***. This approach prevents the unauthorized data retrieval by ***hackers*** and intruders.

3.1 System Design

While data stored in cloud server, the dependable data storage is used, whereas data will be stored in more than one server. User can upload their data files into cloud servers. All data blocks never stored in same server. That should be resided in different server's location. The proposed model will encrypt the data blocks using encryption key. Master server should aware of where that particular data block is to be present in which server. When storing each file, user level authentication to be done. Then that will be password protected. So that others cannot access that files. But actual authorized user can view and download their file without any risk.

4. EXPERIMENTAL RESULTS

The proposed framework is implemented and tested on simulation of simple cloud setup with the help of .NET framework. Iinitially the basic network model for the cloud data storage is developed. There are three different network entities that can be identified as follows:

4.1 User: an entity, who has data to be stored in the cloud and relies on the cloud for data storage and computation.

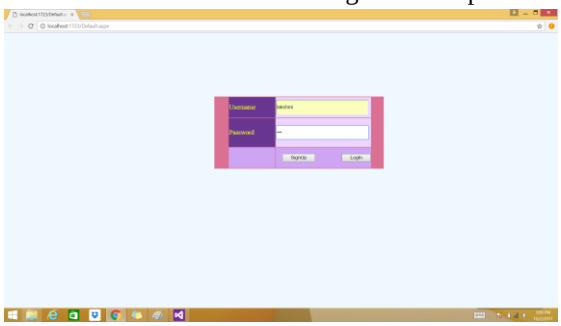

Figure 1 – User Authentication

4.2 Secured Distributable Cloud Server(SDCS): an entity, which is managed by cloud service provider to provide data storage service and has significant storage space and computation resources.

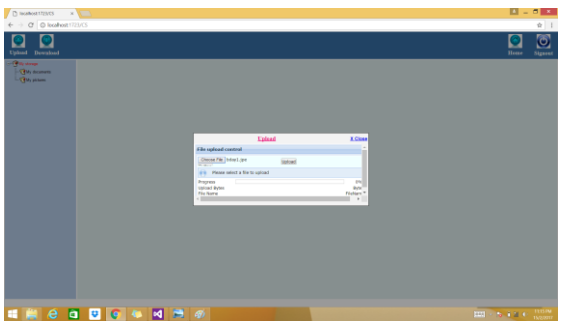

Figure 2 – File or Data uploaded to Cloud Storage

4.3 Service Provider: an entity, which has skills and abilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

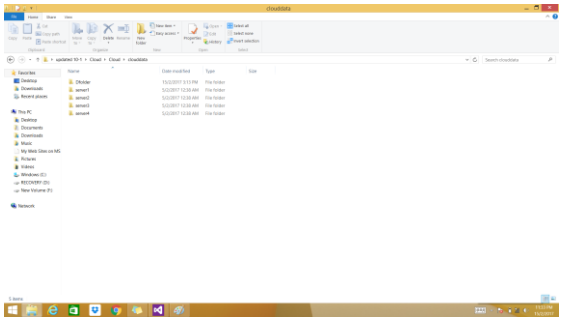

Figure 3 – Secured Distributable Cloud Server (SDCS)

When storing each file, user level authentication to be done. Then that will be password protected. So that others cannot access that files. But actual authorized user can view and download their file without any burden.

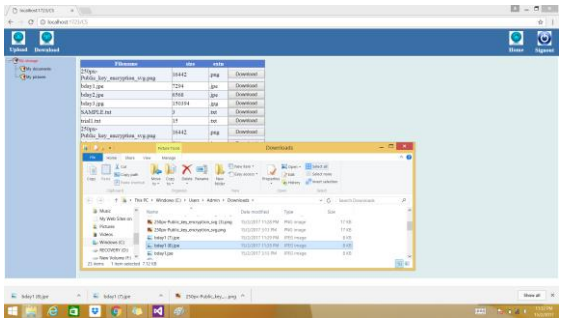

Figure 4 – User download their file from Cloud Storage

5. CONCLUSION

In this paper, storing the data in un-trusted cloud server in a secure manner here in this application. When storing each file, user level authentication to be done. So that others cannot access that files. But actual authorized user can view and download their file without any risk. User or data owner will register his details and upload his data or the important information that all the data files and the information will be send to the master server. While data stored in cloud server, the dependable data storage is used, whereas data will be stored in more than one server. All data blocks never stored in same server. That should be resided in different server's location. The proposed model will encrypt the data blocks using encryption key. Master server should aware of where that particular data block is to be present in which server.

6. REFERENCES:

[1] W. Stallings “Cryptography and network security principles and practice,” Fourth edition, Prentice hall, 2007.

[2] Thomas Loruenser; Daniel Slamanig; Thomas Langer; Henrich C. Pohls " PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services" 2016 11th International Conference on Availability, Reliability and Security (ARES).

[3] Hai-ting Cui " Research on the model of big data serve security in cloud environment" 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI).

[4] Jianghong Wei; Wenfen Liu; Xuexian Hu "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption" IEEE Transactions on Cloud Computing Year: 2016, Volume: PP, Issue: 99.

[5] Z. Fu, X. Cao, J. Wang and X. Sun, "Secure Storage of Data in Cloud Computing," 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, 2014, pp. 783-786.

[6] Yang Tang Patrick P. C. Lee John C. S. Lui and Radia Perlman. FADE: Secure overlay cloud storage with Access Control and Assured Deletion. In IEEE Computer Society vol. 9 no. 6 pp. 903-916 2012.

[7] G. Zhao C. Rong and Jin Li et al. Trusted Dara Sharing over Untrusted Cloud Storage Providers. In Proc. of the 2nd IEEE International Conference on Cloud Computing Technology and Science. pp. 97-103 2010.

[8] Z. Pervez A M. Khattak S. Lee et al. SAPDS: self-healing attributebased privacy aware data sharing in cloud. The Journal of Supercomputing vol. 62 no. 1 pp. 431-460 2012.

[9] H. Y. Lin C. Y. Yang M. Y. Hsieh. Secure Map Reduce Data Transmission Mechanism in Cloud Computing Using Threshold Secret Sharing Scheme. In Software Engineering and Knowledge Engineering: Theory and Practice. Springer Berlin Heidelberg pp.761-769 2012 .

[10] O. Verma R. Agarwal D. Dafouti S. Tyagi "Peformance analysis of data encryption algorithms" Electronics Computer Technology (ICECT) 2011 3rd International Conference on pp. 399-403 2011.

[11] J. Black and P. Rogaway. 2002. Ciphers with arbitrary finite domains. Topics in Cryptology-CT-RSA '02 LNCS vol. 2271 Springer pp. 114-130 2002.

[12] Mihir Bellare Phillip Rogaway Terence Spies. 2010. "The FFX Mode of Operation for Format-Preserving Encryption" Draft 1. 1 February 20 2010.

[13] Lin Zi ; Shi Wenxiao ; Wang Li "A study and analysis on a high intensity public data encryption algorithm" Intelligent Control and Automation 2000. Proceedings of the 3rd World Congress on Pub Year: 2000 Page(s): 2492-2494 vol. 4.

[14] Hamalainen P. ; Hannikainen M. ; Hamalainen T. ; Saarinen J. "Configurable hardware implementation of triple-DES encryption algorithm for wireless local area network" Acoustics Speech and Signal Processing 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on Publication Year: 2001 Page(s): 1221-1224 vol. 2.

[15] Chin Mun Wee, P. R. Sutton and N. W. Bergmann, "An FPGA network architecture for accelerating 3DES - CBC," International Conference on Field Programmable Logic and Applications, *2005.*, 2005, pp. 654-657.