International Journal of Future Generation Communication and Networking
Vol. 13, No. 3s, (2020), pp. 827–831

A Survey on Multi-disciplinary Cloud Storage (M-Crypt)

S.S. Telsang[#1], Shraddha Kumbharkar[#2], Nikita Panhale[#3], Shreyas Sonawane[#4], Gauri Budhe[#5]

[#1]*Information Technology Department, Savitribai Phule Pune University, Pune.*

[1] supriyastelsang@gmail.com
[2] kumbharkarshraddha@gmail.com
[3] tejshreyas.sonawane@gmail.com
[4] nikitapanhale18@gmail.com
[5] gauri.budhe7@gmail.com

Abstract

Cloud computing is the long-dreamed vision of computing as a utility. Besides all the benefits of the cloud computing security of the stored data need to be considered while storing sensitive data on the cloud. Cloud users cannot rely only on the cloud service provider for the security of their sensitive data stored on the cloud. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of the cloud server. With the continuous and exponential increase in the number of users and the size of their data, it is difficult to maintain the integrity of data on the cloud. Many efforts are being made to design a secure system using encryption techniques. This paper gives a survey of different techniques used by the researchers to solve the data security issues over the cloud in addition to the abstract view of the proposed system that we are going to implement the increase the security level of the outsourced data.

Keywords— Cloud Computing, Data Security, Multi-Disciplinary Cloud, Cloud Storage, Data Encryption, Cloud Service Provider, Data Decryption, Data Splitting, Cloud Node.

I. INTRODUCTION

Cryptography is the technique for securing the secrecy of the data. Many different methods have been developed to encrypt and decrypt data in order to maintain the secrecy of the message. Sometimes it is not enough to just maintain the secrecy of a message, it is also necessary to keep the existence of the message secret. With the fast expansion of network bandwidth, the volume of user's data is growing geometrically. The user's requirement cannot be satisfied with the capacity of the local machine anymore. Therefore, people try to find new methods to store their data. Pursuing a more powerful storage capacity, a growing number of users select cloud storage. Information outsourcing and sharing have become ubiquitous in our life as cloud computing assures to elastically store and process a large amount of data. The data stored on the cloud mostly comprises secret and sensitive data. Figure 1 shows the cloud data storage system.

ISSN: 2233-7857 IJFGCN

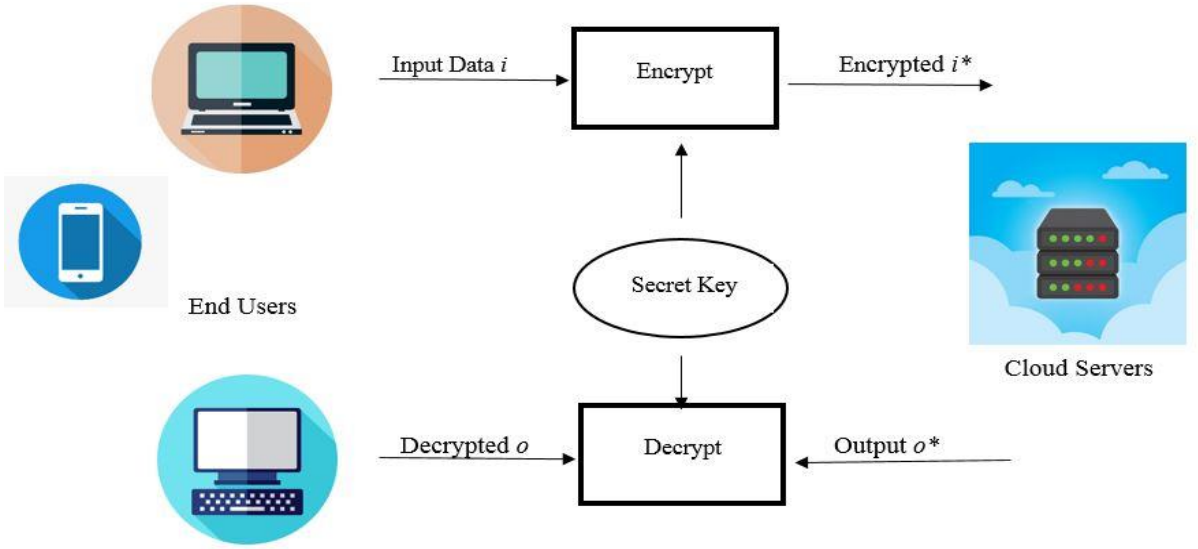

Figure 1: Existing Cloud data Storage [1]

But there are certain privacy issues in traditional systems when outsourcing data on to the cloud as Cloud Server Provider (CSP) will take place of the user to manage the data. In consequence, the user does not control the physical storage of their data, which results in the separation of ownership and management of data. The CSP can easily access and search the data stored in the cloud. In the meantime, the attackers can also attack the CSP server to get the user's data. The above two cases both make users fell into the danger of information leakage and data loss.

The concept of Multi-disciplinary Cloud Storage can overcome this security issues. In such a system we can use double encryption. User firstly encrypt the data at server side and the data is stored in distributed form i.e. one part of data on cloud node and another chunk of data on another node. At the cloud node again, encryption is performed and data gets stored after encryption sends it to the cloud for storage. At the cloud end data again decrypted can store the data by encryption it. The problem of hacking can only be prevented by making the use of double encryption and data distributed storage.

II. TYPES CLOUD SERVICES

Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (Saas). These are called the cloud computing stack, since they form on top of one another. Knowing what they are and how they are diverse makes it easier to achieve your business goals.

Infrastructure-as-a-service (IaaS) [1], [6]

The most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you go basis.

ISSN: 2233-7857 IJFGCN

Platform as a service (PaaS) [1], [6]

Platform-as-a-service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development.

Software-as-a-service (SaaS) [1], [6]

Software-as-a-service (SaaS) is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC.

III. LITERATURE SURVEY

[4] proposes to use multiple mobile sinks to help with data uploading from WSNs to Cloud. An efficient algorithm is intended to schedule the multiple mobile sinks, with several provable properties. We conduct extensive simulations to evaluate the performance of the proposed algorithm. The results show that our algorithm can upload the data from WSNs to Cloud within the limited latency and minimize energy consumption as well.
[2] gives two schemes for different application scenarios i.e. the distributed file system or the operating system. The given virtual machine monitor, conventional attacks and attacks from cloud administrators. In one scheme, every chunk of user's file is protected, so the privacy of every chunk is guaranteed. Secondly, the complete file is protected, and the privacy of the whole file is guaranteed not all chunks. The visual projection of the SSL secure connection and secure virtual machine are evaluated. In consideration of the privacy of the user's data, the overhead can be tolerated.
[8] use two mechanisms i.e. data encryption and file splitting. When a user uploads a file, it is encrypted using AES encryption algorithm. Then encrypted file is divided into equal parts according to the number of clouds and stored on the cloud.
[9] uses the hashing function & key management to provide the security and authentication to target data. Here the splitting of the file in different portions is done then encode and store it on different cloud. Meta data necessary for decrypting and moving a file will be stored in metadata management server. File can club with another file.
[3] proposed a novel approach namely Secure-Split-Merge (SSM) for the security of data. The proposed SSM scheme uses a unique mechanism of performing splitting of data using AES 128 bit encryption key. The chunks of encrypted splits are being maintained on various rack servers of different types of cloud zones. The comparative analysis shows that the proposed system gives effective outcomes as compared to various existing and traditional security standards.

[6]proposed a model to protect data in cloud computing. In this model the algorithm of the Rives Shamir- Adleman (RSA) is applied to the private data. Furthermore, the protocol of Challenge-Handshake -Authentication-Protocol (CHAP) is used to improve the security of the authentication as well. The results show this model is secure and practical.

ISSN: 2233-7857 IJFGCN

[1]focused mainly on client-side security. Even if some intruder (Unauthorized user) gets access to the data accidentally or intentionally, he will not be able to decrypt it. Also, it is proposed that encryption must be done by the user to provide better security. Henceforth, security is provided using Rijndael Algorithm along with EAP-CHAP.

[7] discussed the mechanism of privacy-preserving public auditing and used the independent entity TPA (third-party auditor) and the purpose was to modify data or to improve integrity and audit the data. This paper used encryption techniques AES and SHA to compare and evaluate performance or to maintain privacy and secure data.

[5] discussed the concept cryptosystem that was used for cloud data sharing. This paper shows the cryptographic techniques that were used to efficiently store secure data in cloud storage and used those schemes that were more flexible. The purpose of this paper was to compress the keys, using the cryptosystem concept.

IV. PROPOSED SOLUTION

The main aim of the proposed system is to provide robust security to personal data by splitting into two chunks and using double encryption. System can store data securely by splitting into the chunk and stored on different cloud nodes with encryption. Figure 2 shows eh architecture of the proposed system.

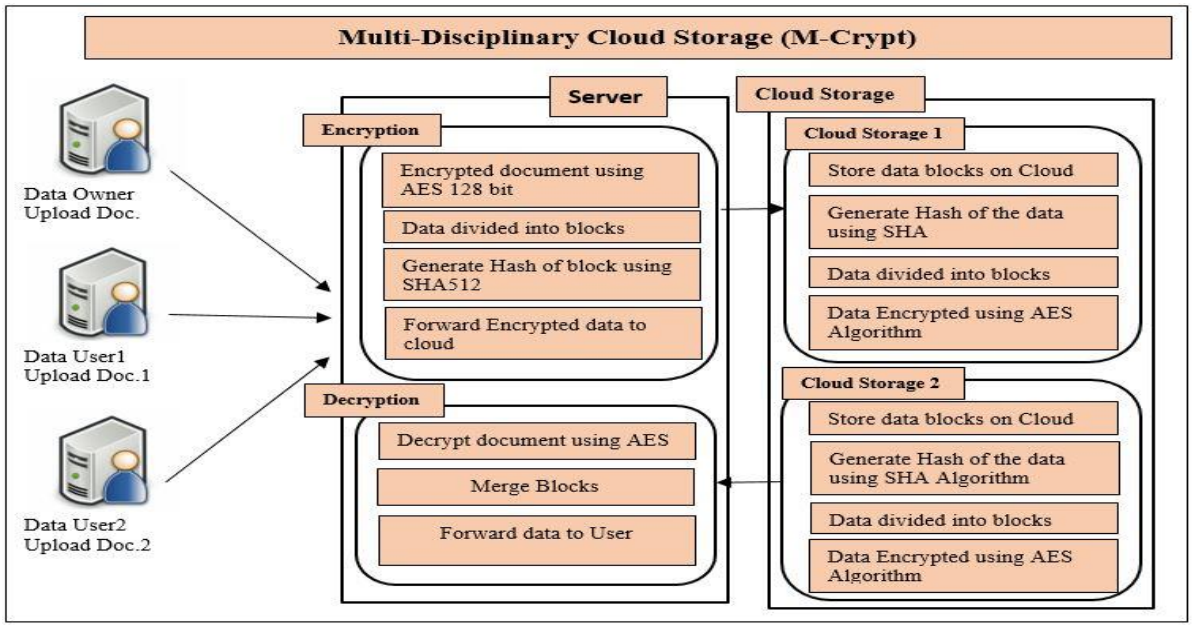

Figure 2: System Architecture

In proposed system we are making use of semi trusted cloud service provider, while user will upload the file and file will be uploaded on the server, here the server performs the encryption of the uploaded file and then divide the file into blocks and hash of the data will be computed. And one share of the data will be stores on the cloud storage 1 and the remaining half share data will be forwarded to the cloud storage 2. The cloud we again going to perform encryption of the data to make it more secure and the data will be divided into the blocks and stored on the cloud with the computing the hash of the data. It maintains the privacy of the stores data due to double encryption of the data and also the file is stored on two different locations so if CSP tries to access the file then he cannot get the whole data.

ISSN: 2233-7857 IJFGCN

V. CONCLUSION

The system offers double security i.e. by using double encryption than the existing system. By analysing the security, we can substantiate that our planned proposal is probably protected by encrypting the file twice i.e. one at the time. Data owner first will encrypt the file and then the data is again encrypted on cloud so that it could be more secure. Here we used an AES 128 bit for the encryption of the file. This double encryption would help the users to secure any kind of important data on any level so as the data could be reused in future, whenever in need, maintaining its authenticity.

REFERENCES

[1] SanjoliSingla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 2, Issue 7, July2013.

[2] H. Li, W. Sun, F. Li, and B. Wang, \Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397{1409, 2014.

[3] BurhanUl Islam Khan,AsifaBaba,RashidahOlanrewaju, SajaadAhmed,"SSM: Secure-Split-Merge data distribution in cloud infrastructure", 2015 IEEE Conference on Open Systems (ICOS).

[4] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, \Efficient data collection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130{143.

[5] B. M. Kore; ArchanaJadhav, Prof. V. V. Pottigar, (2016) "A Literature Survey on Secure Data Sharing in Cloud Storage with KeyAggregateCryptosystem," International Journal of Computer Science and Information Technologies, Vol. 7, No.3, pp.1511-1513.

[6] Asst. Lec. GhassanSabeehMahmood "Data Security Protection in Cloud Computing by using Encryption", Kirkuk University Journal /Scientific Studies (KUJSS) Volume 12, Issue 4, September 2017.

[7] MohanedZkaria Salem; Sahar F. Sabbeh and Tarek EL-Shishtawy, (2017) "An Efficient Privacy Preserving Public Auditing Mechanism for Secure Cloud Storage", International Journal of Applied Engineering Research, Vol. 12, No.6, pp. 1093-1101.

[8] Jolly Dutta 1, Kanika Gupta 2, Abhishek Chaudhary3, Avinash kumar Sharma, "Providing Security by Encryption and Splitting Technique over Cloud Storage", International Journal of Engineering and Techniques - Volume 4 Issue 2, Mar – Apr 2018.

[9] RishabhMudgal&Mrs.KirtiBhatia,"ENHANCING DATA SECURITY USING ENCRYPTION AND SPLITTING TECHNIQUE OVER MULTI-CLOUD ENVIRONMENT", INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY,August 2018.

[10] Tannu,Dr.Karambir ,"Enhancing Data Security in cloud using Encryption Techniques", Indian Journal of Computer Science and Engineering (IJCSE).

ISSN: 2233-7857 IJFGCN