ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

Reliable Multilayer Architecture for Privacy Preserving In Cloud

[1] J K Periasamy,[2]Aathira H N, [3]Akshya P, [4] Vaishnavi R,[5] Sethu Raman K
[1][2][3][4] Department of Computer Science and Engineering, Sri Sairam Engineering College Chennai, India
[5] Automation test engineer, Private IT Sector

***Abstract* – Cloud has become an intelligent storage to the users due to its irresistible features in optimizing cooperation, regular backing up of private files and huge space for less money. Most vulnerable factor in the cloud is security breach and privacy of files. The proposed framework can take the control of data management and security over the cloud. Secured file storage algorithm based on encryptions/decryptions are used to avoid the man in middle attack. Framework is designed with three layered approach on storing the data, which adopts bucket concept algorithms to split the files as chunks and store it in the cloud, fog and local system directory. Based on the computational intelligence, this algorithm could compute the distributed proportions.**

Keywords- Data management, hash algorithm, fog server, reverse hash algorithm, computational intelligence.

1. INTRODUCTION

The geometric growth of unstructured data and their wide ease of use have made Cloud computing to play an inevitable role in this digital environment. With local machine as a only storage medium it is inefficient to meet the user needs. Moreover frequent changes in user's working environment have urged the need for proving seamless access to the global users. The
emerging trend is to replenish Cloud as a convincing medium for utility storage and wide access. Besides the key advantage of cost saving, cloud storage can facilitate information sharing and task collaborating, promote portability and universal accessibility of data ,as well as provide easy and convenient solution to many other problems[1]. With the cluster of application, network technology and distributed file system technology, cloud storage makes a large number of different storage devices to work together coordinately [2][3]. The loopholes in using cloud as a component are man in cloud attack, hijacking of accounts, insider threat, insecure API's , denial of service attack, data loss and many other security concerns. The major issue in this cloud environment is the security breach and privacy of the data being stored. The user feeds the data directly to the cloud service provider. The service provider takes over the role of user and thus isolating the user from having knowledge about physical implementation of user's data. When the intruder hacks the cloud service provider (CSP), the user and CSP loses access of control over the data being stored.

2. RELATEDWORKS

With the development in network infrastructure and the increased bandwidth, enhanced various application services through internet. Cloud computing arises as an emerging technology which solely depends on internet as a medium to transfer data between the end users and the cloud storage. Providing security to the data stored in cloud plays a vital role in the discovery of new security standards and enables development of cloud computing technology. In order to resolve privacy issues, the common techniques for providing data security are through encryption, enabling secure channel for data transmission and providing user authentication. These above methodologies are based on various cryptographic algorithms, the most efficient client based encryption technique for cloud computing is Efficient-RSA, an asymmetric key algorithm which provides resistance against attacks such as mathematical, brute force and timing attack [4]. Additionally this encryption makes the searching process in cloud difficult. Usually multi-keyword or single key-word search are used for extracting the correct data, to improve efficiency uni-gram based keyword transmission is done [5]. Another alternative to keyword search is based on the idea of conceptual graphs which uses two different schemes such as PRSCG and PRSCG-TF for different scenarios [6]. In a traditional system, the user data is uploaded to Cloud Service provider (CSP) and this CSP is responsible for encrypting the plain text on behalf of the user and store them in cloud. If this CSP is distrustful, the user may lose his

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

privacy of data. A Customer Relationship Management (CRM) is proposed which utilizes three systems, including an encryption and decryption system, storage system and CRM application system [7]. The above mentioned techniques explain various methodologies for securing the data stored in cloud. Based on the inferred method, a three layer privacy preserving scheme is proposed which stores the encrypted user data in three varied locations.

3. EXISTING SYSTEM

In the traditional system the original data gets split up and their redundant copies of data are stored in a single cloud server or multiple cloud server. The cloud data may include sensitive information such as passwords files, security records, financial information,encryption-decryption keys and so on. This authorized information must be stored in such a way that no outsider should crack it. Cloud storage is opted in a situation where there is need for large storage capacity.After all, no enterprises can let their core data be handled by others easily since it is a matter of life and death [8]. In the existing system the user uploads the data to the cloud server which encrypts the original data using any of the standard encryption algorithm techniques. When this encryption pattern is decoded, trespasser could take over the control of the data in cloud and the user loses control over his/her own data. When confidential information gets disclosed many security issues arises which may also result in masquerader attack or modification of message content.

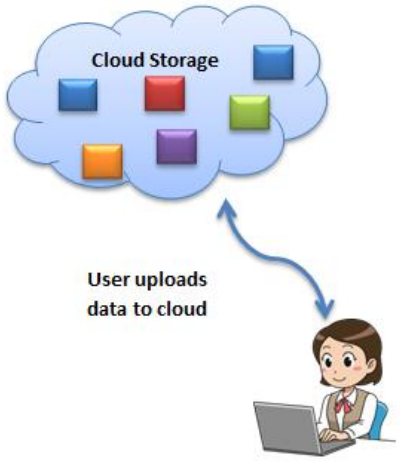

Figure 1

Figure 1 represents the traditional method of storing data sets in redundant fashion and providing authorized access. In recent three layered framework hash-solomon code algorithm is designed to divide data into different parts and store them in respective locations [9]. The major disadvantage that persists in recently proposed system is the security drain of the data stored in local system directory. When there is no backup option and if the data in the local system is lost, the original data content can't be rebuilt.

4. PROPOSED SYSTEM

The degree of security is the basic and the most predominant metric that evaluates the quality of cloud. It is imperative to make out a strong security fence over the data. Some suggested methodologies generate an unique User Service Dependent Identity(USID) with privacy check by establishing mapping among the existing user identity(ID)and pool of User ID's to enhance the privacy of sensitive user information[10].In our proposed system ,the data uploaded by the user is encrypted using standard hashing techniques such as Secure Hash Algorithm(SHA) / Message Digest 5(MD5). The hashed output is then reverse hashed using any of the hashing algorithm in order to attain a greater level of security. The encrypted cipher text is then segmented into three chunks by adopting bucket concept algorithm such as reed-solomon code or simply string slicing. The fragmented data is then stored in varied locations like cloud server, fog server which is an extended version of cloud computing and the local machine. On retrieving the stored data, initially the user must be validated against access rights. Once the user is authorized for access the fragmented data are integrated into a single component. The extracted data is decrypted and the original plain text is made available to the user. The physical implementation of the above process is completely hidden from the user and thus attaining higher level of data abstraction.

5. SYSTEM MODEL

i. Encryption of user data:

The massive growth of data and the proportional growth of finding loopholes in the storage structure is driving the technology towards the usage of incorporating the most secured format of data storage and access. Most commonly known and effective method of providing security is encryption/decryption methodology. In some design before uploading the data into the cloud, a 256-bit symmetric key with rotation is being used for encryption and for retrieving the original data a shared secret key is used[11]. In our system the trend being used is

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

cryptographic hash function for encryption and decryption. SHA-160 is implemented to perform encryption of plain text where the input is translated to 160bit output which is in hexadecimal format. The reverse hash algorithm is then applied to the output of the previous hashing algorithm. MD5 is used to perform reverse hashing which is one way cryptographic function to generate 128bit message digest. Our system performs hashing-reverse hashing sequentially to ensure a higher level of security.

ii.Data
segmentation and storage: Existing framework of uploading the entire document as redundant copies in a single or multiple cloud suffers from a serious degradation in terms of security. So the proposed system takes the advantage of fragmenting the original data into three chunks of varied proportions. Neural network concept is used as a splitting approach in domain such as machine learning [12]. Reed-solomon code is used for data segmentation in case of variable length chunks or simply string slicing can be applied in case of equivalent sized blocks. The sliced data are stored in three major servers. A part of data is being stored in cloud server, another part is uploaded to the fog server and the rest is stored in the users local machine. This split and store approach safeguards the data from unauthorized user. Even if the data from any of the storage medium is hacked, the information available is insufficient for the intruder to make progress.

iii. Decryption
To retrieve the original data, the encrypted segments should be treated with anefficient decryption algorithm. Advanced Encryption Standard (AES) algorithm is applied separately on each of the three parts.Divide and conquer strategy is adopted to merge the segments into an individual content and the whole is decrypted using any standard decryption algorithm such as AES. The original information is now made available to the end user in response to the access request.

The proposed framework is an efficient Cloud storage technique where the information fed by the user gets encrypted then followed by fragmentation into discrete parts. The encrypted contents are then stored in distinct locations such as cloud, fog and the local machine.

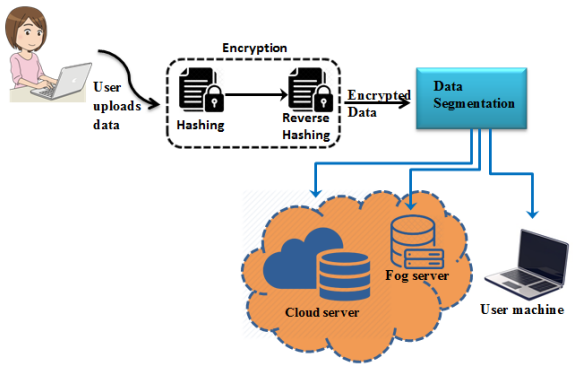

Figure 2 is the system architecture for the proposed framework. The user uploads the data through the application developed to serve this purpose. The data encryption and segmentation followed by storage occurs at the backend. To retrieve the uploaded content, decryption algorithm is processed so that the original content is accessible by the end user.

A. USER REGISTRATION
Upon opening the website, the user has to register /login using email id and password. The registered credentials should be remembered for future usage. Once the login is done, the user can upload the files into the cloud.

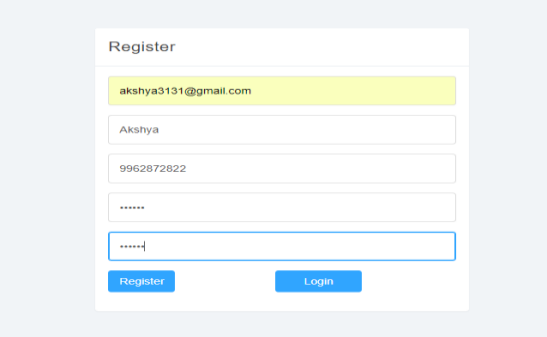

Figure 3

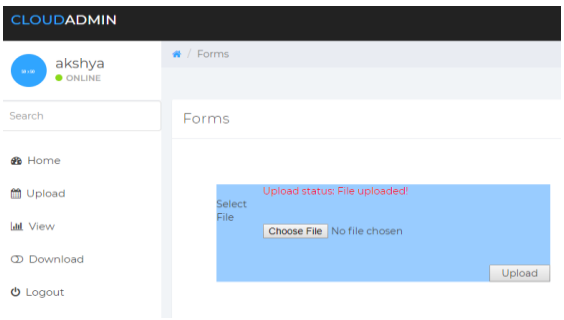

Figure 4

Figure 3 and 4 are the registration and upload screens.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

B. DATA ENCRYPTION AND FRAGMENTATION

The user data is encrypted by adopting hashing technique like SHA-256. Reverse hashing is then applied using MD5.The secured context is then splitted up using string slicing or Reed Solomon algorithm.

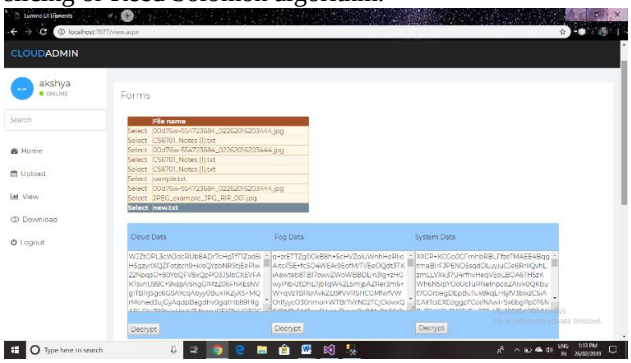

Figure 5

The above screenshot figures out the encryted and fragmented data.

C. DATA DECRYPTION

For making the data available to the user AES decryption methodology is implemented.To retrieve the uploaded data the user is initially authorised and when he/she clicks the decrypt button in view menu ,the each part gets decrypted .The distinct parts are merged together to form an individual part and it is decrypted again to gain the original datathat is being uploaded earlier .The below figures picture outs the live screens in the website being developed.

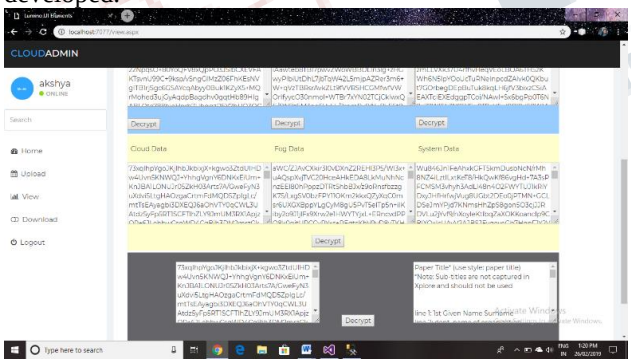

Figure 6

To download the uploaded files the user must click the dowload menu . After selecting the particular file to be downloaded, the requested file gets dowloaded.The below Figure 7 shows the screenshot when the end user downlods the uploaded file.

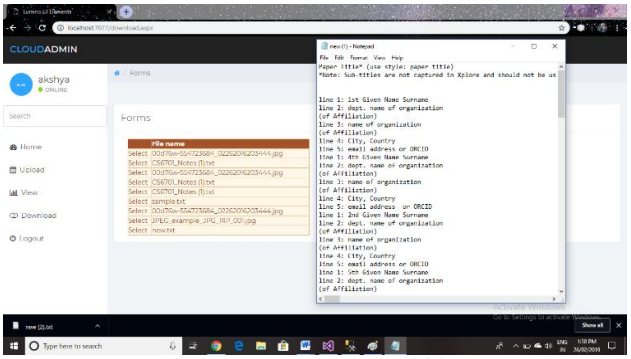

Figure 7

6. FUTURE SCOPE

Our system frames an application to store sensitive data in cloud and thus the security and privacy of information is achieved. Future studies are promoted towards developing a system that provides storage of large volume of data with high performance ratio and more secured framework.Deep learning methodology can be incorporated to split and store the user data into random proportions.

7. CONCLUSION

In the technological world,the volume and the type of data being used is varying dramatically. The need for storage and management of geomentrically growing data has made the world to move towards the trend of cloud usage.But the serious unsolved issue that prevails even today is security of cloud data. Thus, the proposed system ensures the security factors such as confidentiality, integrity andprivacy in terms of split and store approach.This concept screens the cloud data from being exploited by the hackers because even if a part of data is cracked the complete information is still unknown.The act of applying hashing and reverse hashing using a well known encryption techniques like SHA-256 and MD5 sheilds the input data by framing a complex encryption pattern.While retrieving the data in future,AES alogorithm serves the purpose of decryption and thus making the information transparent to the user. The proposed system uses the most secured algorithms for encryption and decryption and thus attaining a higher level of security.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

REFERENCES

1. Chun-Ting Huang_, Lei Huangy, ZhongyuanQinz, Hang Yuan_, LanZhoux, Vijay Varadharajanx and C.-C. Jay Kuo"Survey on Securing Data Storage in the Cloud" Article inAPSIPA Transactions on Signal and Information Processing • January 2014
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. 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.
4. FatemiMoghaddam F.; Karimi,O., &Alrashdan,M.T. " A comparative study of applying real-time encryption in cloud computing environments. 2013 IEEE 2nd international conference on cloud networking.
5. Fu, Z., Wu, X., Guan, C., Sun, X., & Ren, K. (2016). " Toward Efficient Multi-Keyword Fuzzy Search Over Encrypted Outsourced Data With Accuracy Improvement". IEEE Transactions on Information Forensics and Security, 11(12), 2706–2716.
6. Fu, Z., Huang, F., Ren, K., Weng, J., & Wang, C. (2017)." Privacy-Preserving Smart Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data" IEEE Transactions on Information Forensics and Security, 12(8), 1874–1884.
7. Jing-Jang Hwang, Hung-Kai Chuang, Yi-Chang Hsu, &Chien-Hsing Wu. (2011). "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Servic". 2011 International Conference on Information Science and Applications.
8. Du meng "Data security in cloud computing" 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka.
9. Tian Wang , Jiyuan Zhou, Xinlei Chen , Guojun Wang , Anfeng Liu , and Yang Liu" A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing" IEEE transactions on emerging topics in computational intelligence,vol. 2, NO.1, February 2018.
10. Syed MujibRahaman,Mohammad Farhatullah" A model for Preserving cloud computing Privacy"2012 International Conference on Data Science & Engineering (ICDSE).
11. Prakash, G. L., Prateek, M., & Singh, I. "Data encryption and decryption algorithms using key rotations for data security in cloud system". 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014).
12. Z. Reitermanov´a, Charles University, Faculty of Mathematics and Physics, Prague, Czech Republic. "WDS'10 Proceedings of Contributed Papers", Part I, 31–36, 2010.