International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

Providing Privacy in Healthcare Cloud for Medical Data using Fog Computing and Cryptography

Miss. Pachore Poonam A[1], Prof. S.D. Jondhale[2]

[1]Miss. Pachore Poonam A, Dept. of Computer Engineering, PREC, Loni, Maharashtra, India.
[2]Prof. S. D. Jondhale, Dept. of Computer Engineering, PREC, Loni, Maharashtra, India

---

Abstract - *Today internet is getting faster and cheaper to use with the introduction of 4G network. Thus due to this external storage sources such as cloud is used by many on daily basis. There emerged various cloud providers both in private and public cloud computing scenarios. Thus with the fast and massive growth of data that is being stored on the cloud gave development opportunities to make the cloud more secure and reliable. The major sector among all that was heath related services which started using cloud to satisfy their daily needs.*

So in this paper we are going to concentrate on securing health services using cloud and ways to make it safe and secure to use. However, in current storage scenario, health care data is totally stored in cloud servers. Thus, users who upload their data on cloud lose their right of control of the data on cloud and face privacy leakage risk. The other privacy protection schemes and technologies are usually based on encryption technology, but these kinds of methods cannot effectively resist attack that are originated from the inside of cloud server by a cloud provider whose services are handled by a third party source. So we thought of implementing a novel approach which will spilt data and store on cloud and local servers simultaneously. This technique will be explained as Split and Combine (SaC). To upload data, the data will be split in to two where the first will be saved on the cloud and the other will be saved on the local server. To request data, we will again combine the data from the cloud and the local server. We are intending to use Google Drive as the Cloud. In this project, the main focus has been given to secure healthcare private data in the cloud using a local server computing facility and AES algorithm.

***Key Words*: Cloud, Healthcare, Security, Local Server, Spreadsheet, AES, SaC**.

1. INTRODUCTION

Today computer technology is become an integral part of our day to day life. Cloud computing is the hot topic today that is being used by many. Thus cloud computing is used in large amount of applications from social networks to health care and many more. Thus as the use of cloud increased it gave rise to misuse of user data by an attacker. Thus security challenges arose from it as most of the application data is handled by third party cloud handlers. With the introduction of 3G and 4G networks the internet got faster thus increasing the amount of data that is being sent on the cloud. Thus to track this amount of data from attackers got a very challenging task. Thus the privacy of data on the cloud providers was unpredictable. There were many cyber-attacks

2. REVIEW OF LITERATURE

This topic of previous studies describes the fundamentals of various techniques and technologies used to protect data that is stored on the cloud. It helps in understanding and evaluating various ideas put forward by various technical papers published by various publishers.

Ashish Singh et al.[1] authors explains the idea of about the basic features of the cloud computing, security issues, threats and their solutions that can be achieved by using various techniques used to overcome them. It also explains some key topics related to cloud such as cloud architecture framework, service and deployment model, cloud technologies, cloud security concepts, threats, and attacks that come with cloud computing. It also concentrates a lot of open research issues related to the cloud security that can be improved upon. The Main Limitation of this paper is that it concentrates on saving data as whole on the cloud only.

Tian Wang et al.[2] authors explains the idea of taking full advantage of cloud storage and protect the privacy of data from leakage together. In this paper they explain a technique named, Hash-Solomon code algorithm is designed to divide data into different parts to store data at various steps. Then, a small part of data is saved in local machine and fog server in order to protect the privacy of a whole data. It has high accuracy to store data. The Limitation of the paper is that it concentrates on only splitting data and not the security of the split data which is achieved by the concept in our paper.

S. Seema et al. [3] authors explain the idea of using multi keyword search approach for finding data on the cloud. The approach presented in this paper is known as secure multi-keyword ranked search over encrypted cloud data. This approach in the paper supports some of the functions like uploading and deletion of les which can be done by multiusers. Here RSA algorithm is used. The proposed technique in this paper makes use of a structure known as tree-based indexing to develop search competence and also provides adaptable uploading and deletion of les. The

Limitation of the paper is that it concentrates on RSA algorithm and not on SaC technique which is more efficient then it.

Sherman S.M. Chow, et al.[4] authors explain the idea of public auditing of the data that is stored on the cloud. It introduces a third party auditor (TPA) to check the integrity of outsourced data and be worry free and be tension free. Thus the work proposed in this paper increases a secure cloud storage system supporting privacy-preserving public auditing for easy cloud use. It also extends TPA to perform audits for multiple users simultaneously and efficiently without any extra cost and efforts. This proposed schemes are provably secure and highly efficient for various cloud providers. The Limitation of the paper is that it concentrates on public auditing and not on SaC technique which is more efficient then it.

R. Kowsik et al. [5] authors explain the idea for securing data in the cloud using offensive decoy technology for data security. In this paper abnormal data activity is found using a thread . The unauthorized access is detected using challenge questions set during registration. When unauthorized access is detected disinformation attack is launched by returning large amounts of decoy in formation to the attacker to misguide him. It protects the misuse of data by the attacker. The Limitation of the paper is that it concentrates on offensive decoy technology and not on SaC technique which is more efficient then it.

3. PROPOSED METHODOLOGY

In the proposed system we consider of dropping the traditional approach of storing the data as a whole using SaC technique. Furthermore, data security is the most important part in cloud storage security and it includes three aspects: data privacy, data integrity and data availability at a given time a user intends to use them. Thus to add extra security for the SaC we are going to use encryption and decryption techniques with it. We are proposing to use Google Drive and Google Spreadsheet for demonstration of out technique.

3.1 Architecture

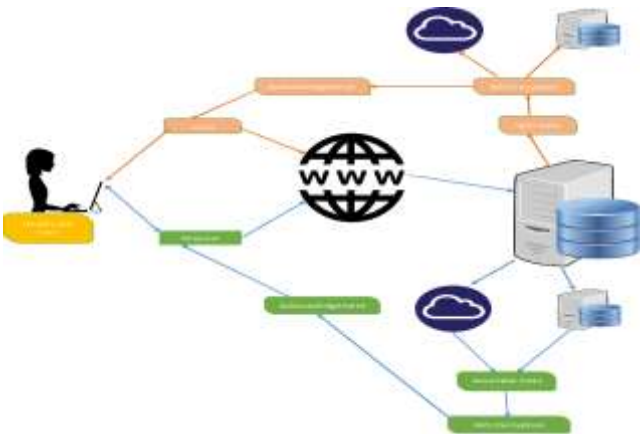

Fig -1: Proposed System Architecture

Fig 1 shows the proposed system architecture which will be explained in brief as follows:

1) Healthcare User: This entity may be anyone from the health sector such as doctor, patient, Staff etc. This will be a mobile application with various users.

2) Send Data: Here data is sent for uploading which is received on the local server for further processing. The data will be received using internet and cloud.

3) Split Data: Here data is split on local server for uploading. The Split data calculation will depend on the formula applied to number of fields in the table that is to be uploaded.

4) Encryption: Here the split data is encrypted using AES Algorithm. The AES algorithm increases the security of the data.

5) Upload: Here the 80 percent split data is uploaded to cloud and the remaining is kept on the local server. The local server database may be oracle etc. and the cloud server database will be Google Spreadsheet.

6) Request Data: Here data is requested by user for downloading which is received on the local server for further processing. The Request is first received by the local server.

7) Download data: Here data is downloaded from the cloud and local server.

8) Combine Data: Here the split data is combined together with help of formula to split and combine technique.

9) Decryption: Here the combined data is decrypted and shown to the user. The user can view the data on the mobile

3.2 Algorithm

AES is a short form of Rijndael block cipher . It was developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES was first adopted by the U.S. government for security and is now used worldwide. It is the advanced version of the Data Encryption Standard (DES), which was published in 1977. The AES algorithm is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data using AES. AES is included in the ISO/IEC 18033-3 standard for security features.

AES is the rst (and only) publicly accessible cipher approved by the National Security Agency(NSA) for top

secret information when used in an NSA approved cryptographic module (see Security of AES, below).

4. RESULT ANALYSIS AND DISCUSSION

4.1 Results for communication with cloud

1) Upload and View Data: In the screenshot a communication with the cloud is made and the data can be uploaded and downloaded using the application.

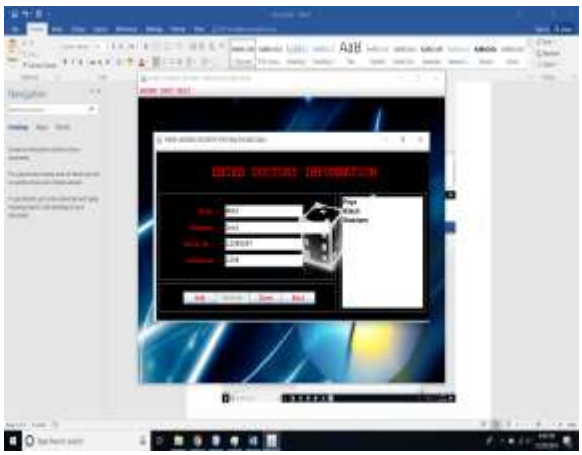

Fig-2 : Result to Upload and View Data

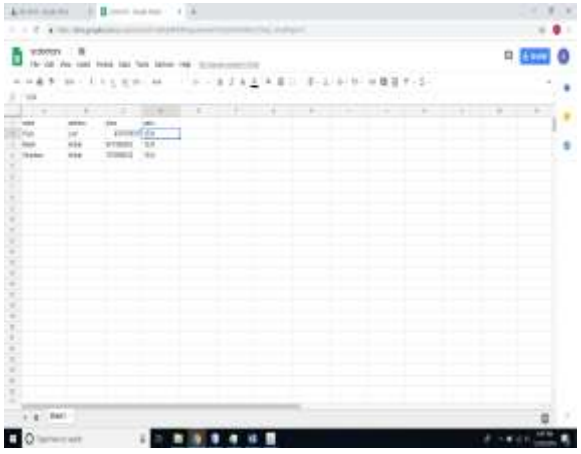

Fig-3: Result to Show Data on Cloud

2) Data on the Cloud: In the screenshot the data that is to be uploaded and downloaded is stored on the Google Drive Spreadsheet.

4.2 Discussion for communication with cloud

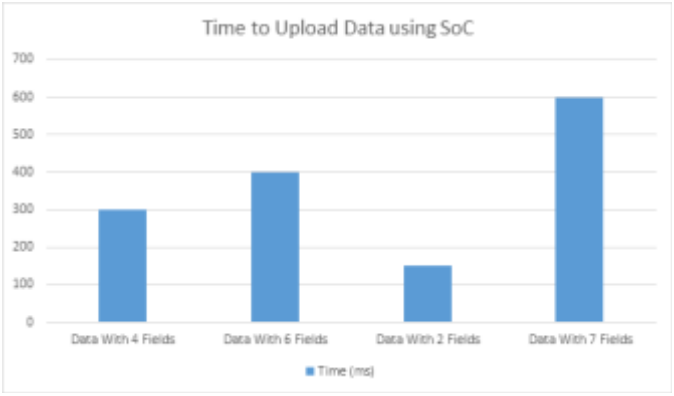

Fig-4: Time to Upload Data

1) Upload: In the above bar chart time to upload data using SaC is shown which is milliseconds (ms).

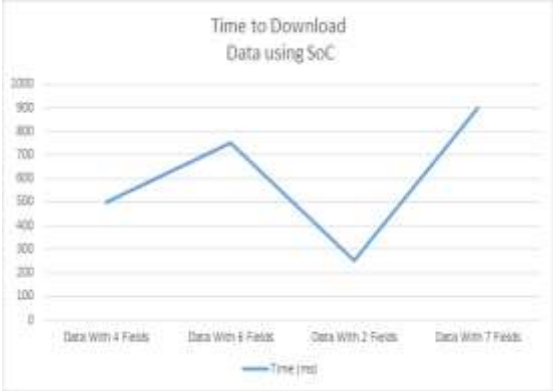

Fig-5: Time to Download Data

2) Download: In the above line chart time to download data using SaC is shown which is milliseconds (ms).

5. CONCLUSION

This Project explain a novel approach with various techniques to improve the security of a Health care data using cloud and Split and Combine (SaC) technique. At first data is split and uploaded successfully. Then the data is downloaded and Combined together. To enhance the security, the data after split id encrypted using AES algorithm and decrypted after combining the data. The current system is very good in increasing the security of data on the cloud as the data is partially stored on the cloud. The drawback of the system is that the local server should always be on to combine the data together.

REFERENCES

[1] Cloud security issues and challenges: A survey by Ashish Singh and Kakali Chatterjee in Journal of Network and Computer Application Volume 79, 1 February 2017, Pages 88-115

[2] A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing on Cloud Computing by Tian Wang , Jiyuan Zhou, Xinlei Chen , Guojun Wang , Anfeng Liu and Yang Liu in IEEE Transactions on Emerging Topics in Computational Intelligence (Volume: 2 , Issue: 1 , Feb. 2018)

[3] Centralized multi-user and dynamic multi-keywords search scheme over encrypted cloud data by S. Seema ; Y. Harshitha ; P. Apoorva in 2017 International Conference on Communication and Signal Processing (ICCSP)

[4] Privacy-Preserving Public Auditing for Secure Cloud Storage by Cong Wang ; Sherman S.M. Chow ; Qian Wang ; Kui Ren ; Wenjing Lou in IEEE Transactions on Computers (Volume: 62 , Issue: 2 , Feb. 2013)

[5] "Mitigating Insider Data Theft Attacks in the Cloud on Cloud Computing by R. Kowsik ; L. Vignesh in 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM)

[6] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," Pervasive Mobile Computing., vol. 41, pp. 219–230, 2017.

[7] Z. Fu, F. Huang, K. Ren, J.Weng, and C.Wang, "Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.

[8] J. Hou, C. Piao, and T. Fan, "Privacy preservation cloud storage architecture research," J. Hebei Acad. Sci., vol. 30, no. 2, pp. 45–48, 2013. 12

[9] Q. Hou, Y. Wu, W. Zheng, and G. Yang, "A method on protection of user data privacy in cloud storage platform," J. Comput. Res. Develop., vol. 48, no. 7, pp. 1146–1154, 2011.

[10] P. Barham et al., "Xen and the art of virtualization," ACM SIGOPS Oper. Syst. Rev., vol. 37, no. 5, pp. 164–177, 2003.