March - April 2020
ISSN: 0193-4120 Page No. 11335 - 11338

Real Time Sensitive Data Sharing System for Hiding and Monitoring Information using Cloud Computing

[1]P. Sasank, [2]Logu. K

[1]UG Scholar, [2]Associate Professor,
[1,2]Saveetha School of Engineering, SIMATS, Thandalam, Chennai
[1]sasankpamidi99@gmail.com, [2]klogu786@gmail.com

Article Info
Volume 83
Page Number: 11335 - 11338
Publication Issue:
March - April 2020

Abstract

Cloud computing is one of emerging technology in this digital world. In cloud computing large amount of information are stored through internet. The major benefit of the cloud computing is it decreasing the cost of maintaining our own server system. Here the data are stored on the cloud server not in our own local system. Using this concept of cloud computing the users can store and share the data with others from remote location itself. Cloud server also contains large amount of sensitive data like electronic health details. The sensitive type of data cannot be demonstrated to other third party users when the content is shared. So, the security is one of the important concerns in this situation. In this proposed model data integrity concept is applied to give the assurance of secured data. Encryption concept is provides the security of entire file. So, the other third party users unable to open this particular file. To avoid this problem the proposed system is used. In this proposed model remote information integrity approach is used to hide the sensitive information. Finally the proposed scheme performance is compared with existing techniques.

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 15 April 2020*

Keywords: *Cloud Computing, Sensitive Data, Encryption, Integrity, Electronic Healthcare, Sanitizer.*

I. Introduction

In every business organizations and institutions contains huge amount of data. Storing the entire data into the local system is very difficult. For that reasons most of the business organizations store their information to the cloud storage. Sometimes the data stored on the cloud also going to deleted or corrupted due to human mistakes or software viruses. To verify the data on the cloud various schemes are already available. In these schemes the data owner initially prepares the signature of the data blocks before store the data into the cloud server. The data blocks are integrated with the signatures and stored on the cloud server. This stored data accessed by others using various applications like Google Drive, iCloud etc. Cloud server also contains large amount of sensitive data.

The healthcare organizations also store their data on the cloud. The healthcare organizations are stored the patients details such as name of the patient, contact number and unique number of the patients. If the details are stored directly into the cloud server the researchers use and share their data for their research activities. Data integrity has given from remotely to the sensitive information on the cloud server. To avoid this specified problem is to decrypt the whole fileusing generated signatures by the users. But in this method, the entire information is going too encrypted. The researchers are not able to use the sensitive data for their research work. Many times the sensitive data is need for analysis infectious like problems. Data distribution with sensitive information encryption from remotely is very useful.

This type of problems was not solved in existing research works. Here fig 1 illustrate about HER.

March - April 2020
ISSN: 0193-4120 Page No. 11335 - 11338

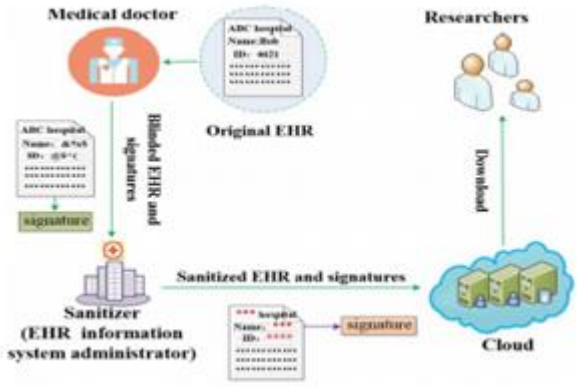

Figure 1: Example for HER

In this EHR example the data can be categorized into two types. The first type of the data is personal information like name of the patient and patient registration number. Another type of the data is healthcare organization sensitive data such as hospital name. Actually the sensitive information are marked as * symbol and upload to the cloud server for the purpose of research. Here sanitizer is called as the administrator of the entire organization data. The important individual personal data not share to sanitizer. To protect the patients data the doctor blind the information before transfer the data to the sanitizer. Whenever the medical practitioner needs the data from EHR they issue the result to the sanitizer. The sanitizer sends the blind data to the practitioner. The doctor recovers to the original form. By using this process the sensitive data will be hided from others.

This article can be divided as follows. Section 2 describes about existing techniques used to save the sensitive data. Section 3 discussed about the proposed method and process flow of our system. Section 4 explains about this proposed system result. Section 5 concludes the proposed system.

II. Literature Survey

Hovav Shacham et al., shared their view of data security. They said that data storage center only provides the security of stored data. Providing security was the challenging task of the storage area. In this article the authors gave the initial proof of the security concept. In this scheme BLS concept was used to secure the data. PRF concept was used for security user's verification [2].

Boyang Wang et al., says that the data available on the cloud is not secure. Third party members are easily access and share the data. To provide more security on cloud data the owners can generate signatures. The actual data with there is stored on the cloud server. Each and every block of the data can sign by various users. Here already signed users are exited from the group, the particular block is signed by other user. This task is very difficult because cloud contains large amount of data.

In this paper the authors used a new concept for audit for the shared data on the cloud. Here proxy signatures are used to resign the block instead existing user. This technique is also used in batch auditing also. In batch auditing multiple tasks are audited simultaneously. The final result shows that this proposed method increase improve the effectiveness of user resigning [3].

Yannan Li et al., explained about the importance of security in cloud server. Various auditing protocols are used to verify and ensure the honesty of the outsourced information. The important problem of an existing system was key management. In this paper the authors introduced new auditing concept based on fizzy identity for key management. Here new protocols were constructed using biometrics concept with fuzzy logic. They proved that this new concept provide more security than other models. Finally this protocol was executed in real time scenario. [4].

G., Susilo et al., proposed new protocol offers the property of error-tolerance, namely, it binds with private key to one identity which can be used to verify the correctness of a response generated with another identity, if and only if both identities are sufficiently close. We prove the security of our protocol based on the computational Diffie-Hellman assumption and the discrete logarithm assumption in the selective-ID security model. Finally, we develop a prototype implementation of the protocol which demonstrates the practicality of the proposal [4]

Huaqun Wang discussed about the importance of the cloud computing concepts. Cloud computing provides flexible, forceful infrastructure of healthcare, business organizations and educational institutions. Using public data the owners move the data into the cloud not they are able to control over the data. Here cloud security was the biggest challenge. Sometimes clients are not able to access the data remotely. In this paper the authors describe about proxy provable data possession. Here the authors implement and execute this proposed model. Finally they done security analysis and shows the output of proposed system provides better security compared with other schemes [5].

Jian Shen et al., said that due to the development of communication technology all the organizations are going to use the computers for their storage and processing task. But storing large amount of data in the single system is very difficult. Cloud computing infrastructure provides more storage area of any type of organizations. Cloud security was challenging task in this current scenario. Many research people were developing security protocols for cloud server. In this research article the author

March - April 2020
ISSN: 0193-4120 Page No. 11335 - 11338

proposed a new protocol for cloud server. This new protocol using blockless checking and provides the facility for batch auditing. This new protocol consists of doubly linked table and use location array for storing the location. Finally the security analysis was conducted. Based upon the security analysis this new protocol executed efficiently compared with other protocols [6].

Ch Sai Pavan et al. explained the importance of cloud computing in various organizations. Cloud computing is developing technology used to store large amount of data from various organizations and individual users. But the data owners have fear about the security of their data. Many protocols were already used to provide the security of the cloud data. In this article the authors proposed a new security protocol. This protocol is executed based on doubly link table and array of location. This new protocol implemented and executed with real time data. The final result shows the efficiency of the proposed protocol compared with existing protocols [7].

P. Kanimozhi says that cloud concept is mainly used to store large amount of data from various institutions and organizations. But the data owners have a fear about the security of the stored data. Here the authors used a set of security policies and architecture used to check the security level of storage area of the cloud. Multi users also verified by using this implemented technique and auditing also performed. The major benefit of this proposed technique was reducing the memory usage than existing techniques [8].

III. Proposed Method

This proposed system is mainly used to provide the secure way of storing sensitive data in cloud computing environment. The following fig 2 represents our proposed model for integrity auditing.

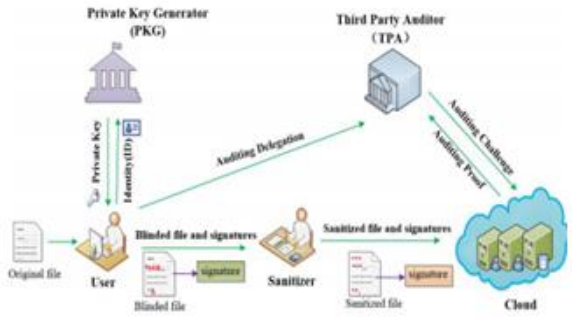

Figure 2: The Proposed Auditing model

This proposed system consists of various modules like User, Sanitizer, PKG and TPA. The user is the part of the organization. They have large amount of file to be transferred in the cloud storage. The sanitizer integrates with the data to the sensitive type of information. The responsibility of the PKG is generating private key based upon user ID. TPA is used to verify the integrity of data on the cloud storage instead of users. The main goal of this proposed model is to provide the correct private key data to the user. This private key is used to pass the verification information to the client. The private key is generated by using key generation algorithms. In this system the data owner pass the blinded file with the proper signature to the sanitizer. The sanitizer verifies the signatures with the blinded file data and transferred to the cloud storage. This all verification process is managed by using third party auditors. The auditing proof will be transfer the cloud by third party auditors. The sensitive information is not sending to the sanitizer. If the user accesses the data from cloud storage they are not able to find the sensitive information.

IV. Results And Discussions

In this proposed system is used to attain information sharing with hide sensitive data in remote auditing for secured cloud environment. By using this system the sensitive information hides from the public and the remaining information displayed to the user. Here sanitizer module is used to sanitize the information blocks matched to the specified sensitive data of the file on the cloud server. Initially data owner integrates data blocks with sensitive data of the initial file and produce the equivalent signature, and transfer the data to the sanitizer.

The sanitizer linked these data blocks into the common format and the blocks equals to the companies' sensitive data. This system also converts the signature to the valid data for the file on sanitizer. This system is used to notice remote integrity of data auditing. And also this system shared the data in the cloud server. The following fig 3 represents the process of integrity auditing.

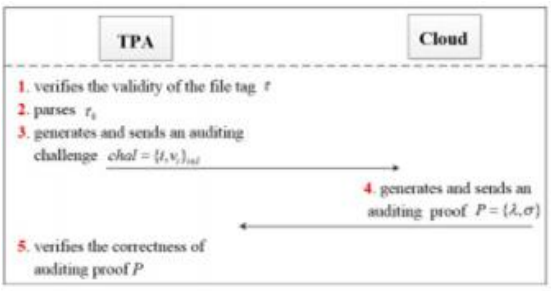

Figure 3: Process of Integrity Auditing

The performance of the proposed system is compared with other related existing systems. The following table 1 describes the performance of our proposed model compared with other techniques by considering various functionalities.

Table 1: Functionality Comparison with Existing Schemes

Schemes	Public verifiability	Certificate management simplification	Data sharing	Sensitive information hiding
Shacham et al. [2]	Yes	No	No	No
Wang et al. [3]	Yes	No	Yes	No
Li et al. [4]	Yes	Yes	No	No
Wang et al. [5]	No	No	No	No
Shen et al [6]	Yes	No	No	No
Ours	Yes	Yes	Yes	Yes

V. Conclusion

The cloud storage provides large amount of space to store the user's data. Using cloud storage the user can able to upload various types of data. The data may be in text form, images, audio, video etc. But security is the major concern of the cloud computing technique. To improve the security level of sensitive data the proposed system is used. This system satisfies various cloud computing security properties. The major properties are correctness of the private key, correctness of data owner generated signature and its equivalent blinded file and the correctness of auditing. Here we constructed an actual data integrity based on identity with responsive data hiding in cloud environment. This system is mainly used to store the sensitive information which is more secured in the cloud server. Finally the performance of the proposed systemcompared with other related existing security schemes. Based on performance analysis, this proposed system is more secure compared with other schemes.

References

[1] Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J. (2019), " Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage", IEEE Transactions on Information Forensics and Security, Vol. 14, No. 2,pp. 331–346.

[2] Hovav Shacham & Brent Waters, Compact Proofs of Retrievability, pp 1-38.

[3] Wang, B., Li, B., & Li, H. (2015)., "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE Transactions on Services Computing, Vol 8, No. 1, pp., 92–106.

[4] Li, Y., Yu, Y., Min, G., Susilo, W., Ni, J., & Choo, K.-K. R. (2017), "Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage System", . IEEE Transactions on Dependable and Secure Computing, pp.1–12

[5] Wang, H. (2013), "Proxy Provable Data Possession in Public Clouds. IEEE Transactions on Services Computing,", Vol 6, No. 4,pp 1-9.

[6] Shen, J., Shen, J., Chen, X., Huang, X., & Susilo, W. (2017)., "An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data",. IEEE Transactions on Information Forensics and Security, Vol 12, No 10,pp. 2402–2415.

[7] Ch Sai Pavan & P Sudheer Kumar(2018), "Novel Dynamic Structure to Implement Public Auditing Protocol on Cloud Data", International Journal of Advanced Research in Computer And Communication Engineering, Vol. 7, No. 3, ISSN: 2278-1021.

[8] P. Kanimozhi(2018), "An Efficient Public Auditing Mechanism With Improved Security For Multiple Cloud Storage Systems", International Journal Of Pure And Applied Mathematics, Vol. 118 No. 15, Issn: 1311-8080 pp. 265-270.

[9] R. Tamilarasi & S. Nirmala Sugirtha Rajini (2016), "Efficient And Secure Way Of Keeping Patient Healthcare Records And Access Control Strategies For Data Stored In Clouds: A Survey", Asian Journal Of Microbiology, Biotechnology & Environmental Sciences, Vol 18, No. 4, pp. 939-940.

[10] S. Nirmala Sugirtha Rajini & E. Mercy Beulah(2016)," Cloud Based Architecture For Healthcare System", Asian Journal Of Microbiology, Biotechnology & Environmental Sciences, Vol. 18, No,4, pp. 1017-1018