ISSN: 2278-4632
Vol-10 Issue-5 No. 5 May 2020

IMPLEMENATION OF SSGK PROTOCOL FOR SECURELY SHARE DATA IN CLOUD STORAGE

N.Keerthana
Department of Computer Science Engineering, Narayana Engineering College, Gudur.
keerthana.narayana99@gmail.com

Y.Vinay Kumar
Asso.Professor, Department of Computer Science and Engineering, Narayana Engineering College Gudur
vinay@narayanagroup.com

Ch.D.Sunil Kumar
Asso.Professor Department of Computer Science Engineering, Narayana Engineering College, Gudur.
cassunil@gmail.com

U.Prasanna
Department of Computer Science Engineering, Narayana Engineering College, Gudur.
prasannauppu1998@gmail.com

P.Chandana Sireesha
Department of Computer Science Engineering, Narayana Engineering College, Gudur.
sireeshasireesha0419@gmail.com

Abstract–

A cloud-based big data sharing system utilizes a storage facility from a cloud service provider to share data with legitimate users. In contrast to traditional solutions, cloud provider stores the shared data in the large data centers outside the trust domain of the data owner, which may trigger the problem of data confidentiality. This paper proposes a secret sharing group key management protocol (SSGK) to protect the communication process and shared data from unauthorized access. Different from the prior works, a group key is used to encrypt the shared data and a secret sharing scheme is used to distribute the group key in SSGK. The extensive security and performance analyses indicate that our protocol highly minimizes the security and privacy risks of sharing data in cloud storage and saves about 12% of storage space.

Keywords-*Encryption,Ciphertext, Cloud Storage, Data Security, Group Keys*

I. INTRODUCTION

The emerging technologies about big data such as Cloud Computing, Business Intelligence, Data Mining, Industrial Information Integration Engineering (IIIE) and Internet-of-Thing have opened a new era for future Enterprise Systems(ES). Cloud computing is a new computing model, in which all resource on Internet form a cloud resource pool and can be allocated to different applications and services dynamically. Compared with traditional distribute system, a considerable amount of investment saved and it brings exceptional elasticity, scalability and efficiency for task execution. By utilizing Cloud Computing services, the numerous enterprise investments in building and maintaining a supercomputing or grid computing environment for smart applications can be effectively reduced. Despite these advantages, security requirements dramaticallyrisewhenstoringpersonalidentifiableoncloudenvironment. This raise regulatory compliance issues since migrate the sensitive data from federate domain to distribute domain. To take the benefit enabled by big data technologies, security and privacy issues must be addressed firstly.

Because shared data on the cloud is outside the control domain of legitimate participants, making the shared data usable upon the demand of the legitimate users should be solved. Additionally, increasing number of parties, devices and applications involved in the cloud leads to the explosive growth of numbers of access points, which makes it more difficult to take proper access control. Lastly, shared data on the cloud are vulnerable to lost or incorrectly modified by the cloud provider or network attackers. Protecting shared data from unauthorized deletion, medications' and fabrication is a difficult task. Conventionally, there are two

ISSN: 2278-4632
Vol-10 Issue-5 No. 5 May 2020

separate method stop remote the security of sharing system. One is access control; in which only authorized user recorded in the access control table has the access privilege of the shared data.

A cryptographic system is said to be secure if the ciphertext does not contain adequate details to find out the matching plaintext. There are many cryptographic systems that use complex operations involving substitutions and permutations to produce resistant ciphertext, even if the level of the security of these cryptosystems are good, there should be tradeoff between security level and operational cost and the ever increasing virtual infrastructure and mobile, cloud computing technologies creating much more complexities and demanding cost effective and secure cryptographic algorithms[6]. The security level is measured in terms of various statistical tests and cost is measured based on the type of the operations used that transforms the plaintext to ciphertext. The cryptographic system algorithm will not be kept secret.

II. BACKGROUND WORK

Many solutions have been proposed to solve the privacy risks of cloud-based storage. Rao proposed a secure sharing schemes of personal health records in cloud computing based on ciphertextpolicy attributed-based (CP-ABE) signencryption. It focuses on restricting unauthorized users on access to the confidential data. Liu et al. proposed an access control policy basedonCP-ABEforpersonalrecordsincloudcomputingas well. Only one fully trusted central authority in the system is responsible for key management and key generation. Huang et al.introduced a novel public key encryption with authorized equality warrants on all of its ciphertext or a specified ciphertext. To strengthen the securing requirement, Wu et al. proposedan efficient andsecureidentity-based encryption scheme with equality test in cloud computing. Xu et al. proposed a CP-ABE using bilinear pairing to provide users with searching capability on ciphertext and fine-grained access control. He et al. proposedascheme named ACPC aimed at providing secure, efficient and fine-grained data access control in P2P storage cloud. Recently, Xue et al. proposed a new framework, named RAAC, to eliminate the single-point performance bottleneck of the exiting CP-ABE based access control schemes for public cloud storage[7]. While these schemes use identity privacy by using attribute-based techniques which fail to protect user attribute privacy.

III. PROPOSED METHOD

Here, we define the application scenario of our protocol and security requirements.

A. Cloud Storage for Big Data

The architecture of cloud based big data is illustrated in Figure.1. It consists of three parts: source data, cloud center and services. Between source data and cloud center layer, unstructured or semi-structured source data is structured. They include processing methods such as data collection, data mining and data aggregation. The processed source data is stored on cloud in relational or NoSQL databases[8].

A cryptographic system is said to be secure if the ciphertext does not contain adequate details to find out the matching plaintext. The security level is measured in terms of various statistical tests and cost is measured based on the type of the operations used that transforms plaintext to ciphertext. In order to make a cipher more difficult to break, one could use various keys in cryptosystem. This would help to cover any perceptible patterns in the ciphertext. In fact, one can produce unbreakable ciphertext by supplying randomly generated key on each bit of data that is mathematically infeasible to break[5]. Since different random bits or keys would not lead to any repeating patterns. We are with a particular emphasis on novel technique to secure user data, we have designed a secure and cost effective new cryptosystem called Rbits (Random bits) cipher. In different directions we identify that Rbits having highest immunity to crack and presenting various analysis tests in support from this viewpoint and the analyzed results are reported.

B. An Example of Healthcare Information System

Cloud storage provides not just low cost, but high scalability and availability. It may be a natural solution to some of problems in storing and analysing the increasing patients' medical records. For health care providers ,only based on the aggregation of all patients 'medical records, could proper diagnosis be made. Reference proposed a cloud based platform for healthcare[2]. Cloud storage provides a commonplace for storing medical records which overcome the delay of transferring medical records between different healthcare providers and make diagnostic process more efficient. The e-healthcare cloud provides many advantages in collaboration and data sharing among health care providers. Nevertheless, in consider of the highly privacy of medical data it comes with significant risks of medical records. Firstly, medical records are shared on the public channel where

ISSN: 2278-4632
Vol-10 Issue-5 No. 5 May 2020

many attackers on the channel to eavesdrop the medical records. Additionally, due to the increasing number of parties, devices and applications involved in cloud, unauthorized parties or cloud providers may have the ability to access shared medical records. Last but not the least, some authorized parties may work together to get some unauthorized medical records illegally.

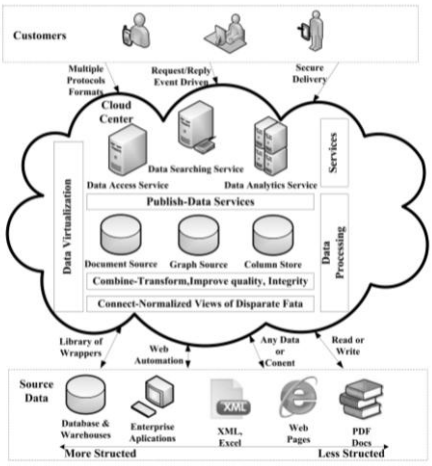


Fig.1: Cloud storage architecture for big data

The detailed process of SSGK is shown as Figure.2:

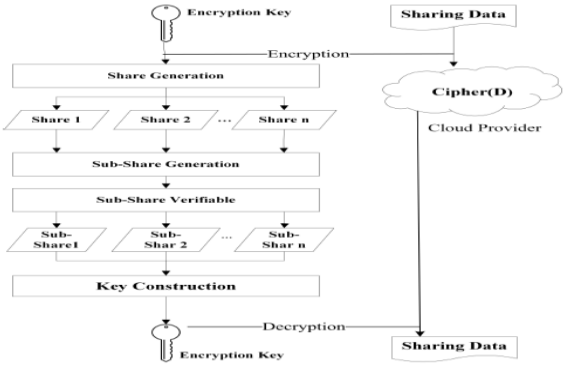
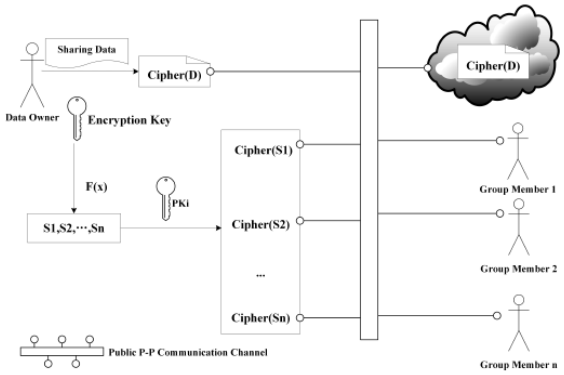


Fig. 2: Data sharing model of the proposed SSGK protocol.

The data owner O creates the secret key and encrypts the data using symmetric encryption algorithm AES. Then secret sharing scheme is used byOto distribute the secret key[9]. As the public channel is available for communications between every pair of participants, an asymmetric encryption algorithm RSA is used to protect the key sub-shares from known by unauthorized users. The distribution protocol is summarized as followed steps and shown as Figure.3.



ISSN: 2278-4632
Vol-10 Issue-5 No. 5 May 2020

Fig. 3: Data sharing model of the proposed SSGK protocol.

IV. RESULTS

The implementation of our proposed system can be shown in figures.

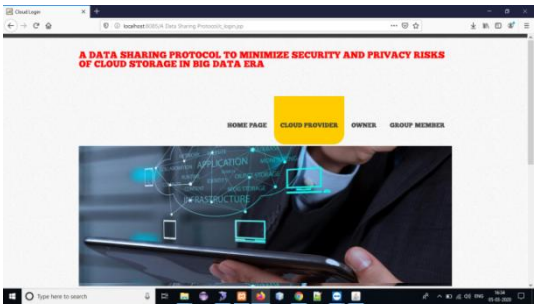


Fig. 4: Home Page

As shown in the above fig.4it is the home page of the project where we have the cloud provider, owner and group member menus respectively.

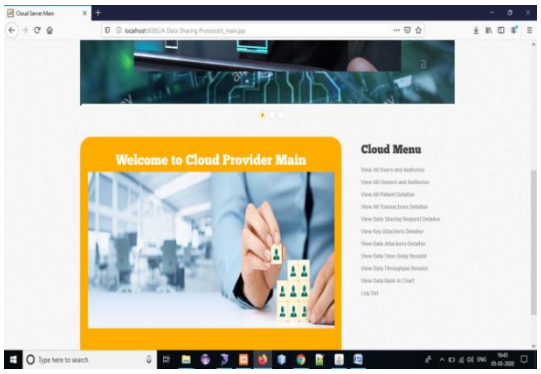


Fig. 5: Cloud Home

The fig. 5 shows the cloud provider home and major functionalities of cloud provider like gives the authority for the verified owners.

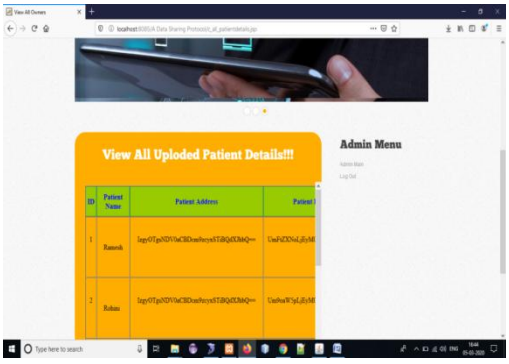


Fig. 6: View Patient Details

ISSN: 2278-4632
Vol-10 Issue-5 No. 5 May 2020

The fig. 6 shows the Patient Details to the request candidate group members which are comes under the category of it.

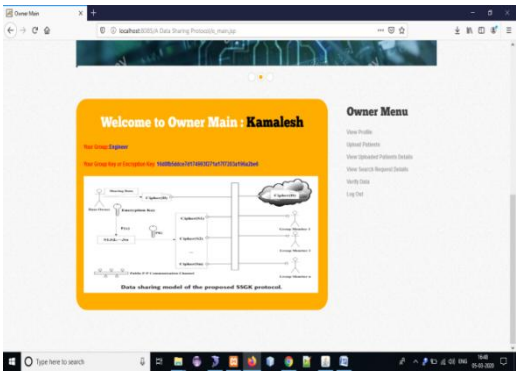


Fig. 7: Owner Home

The fig.7 shows the owner home page it will shows the name of the creation of the group and then all the additional details also is to be filled.

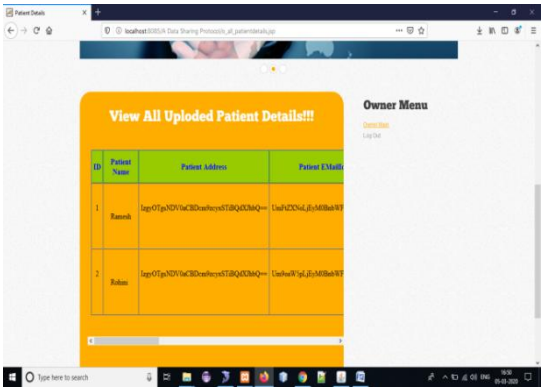


Fig. 8: View Uploaded Patient Details

The fig.8 shows the uploaded patient details of the respectively their individual group owners of their respective patient details.

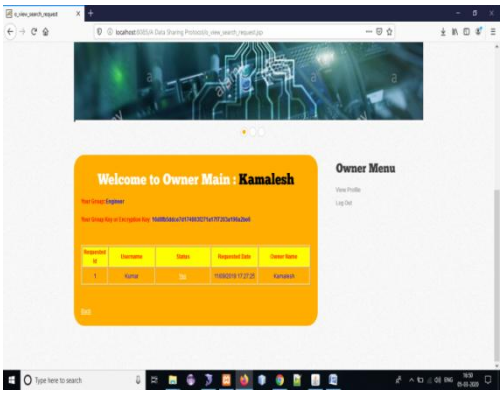


Fig. 9: View File Access Requests

ISSN: 2278-4632
Vol-10 Issue-5 No. 5 May 2020

The fig.9 shows that view file access requests from the respective group participates to send the request to the owner of the candidates.

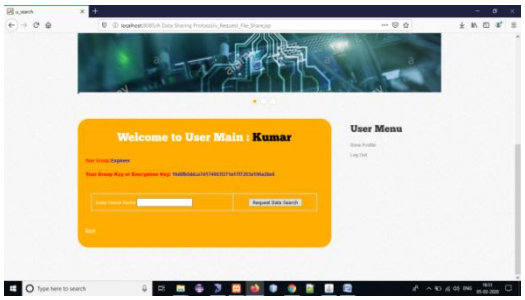


Fig. 10: Search File Details

The fig.10 shows the search the file details .It means that the owner provided data is to be searched their group members with the correct name so the data is to be seen after the acceptance of the owner.

V. CONCLUSION

In this paper, we propose a novel group key management protocol for the data sharing in the cloud storage. In SSGK, we uses RSA and verified secret sharing to make the data owner achieve ne-grained control over the outsourced data without relying on any third party. In addition, we give detailed analysis of possible attacks and corresponding defences, which demonstrates that GKMP is secure under weaker assumptions. Moreover we demonstrate that our protocol exhibits less storage and computing complexity.

The problem of forward and backward security in group key management may require some additions to our protocol. An efficient dynamic mechanism of group members remains as future work.

REFERENCES

[1]D.Wu, G. Zhang, and J. Lu, ``A fuzzy preference tree-based recommender system for personalized business-to-business E-services," IEEE Trans. Fuzzy Syst., vol. 23, no. 1, pp. 29-43, Feb. 2015.

[2] Si Han ; Ke Han ; Shouyi Zhang, " A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era" , IEEE Access, Vol. 7, PP-60290 – 60298.

[3] P. Zhao, W. Yu, S. Yang, X. Yang, and J. Lin, ``On minimizing energy cost in Internet-scale systems with dynamic data," IEEE Access, vol. 5, pp. 2006820082, 2017.

[4] P Penchalaiah, M Vijay Kumar *etl*, **"***A Research Threshold Efficient Hybrid Encryption Schema for Secure File System***",** International Journal of Recent Technology and Engineering (IJRTE),ISSN: 2277-3878, **(SCOPUS)** Volume-8, Issue-2S3, Page 888 –891,July 2019

[5] Penchalaiah P, Ramesh Reddy K, "Random Multiple Key Streams for Encryption with Added CBC Mode of Operation*", Perspectives in Science (ISSN: 2213-0209), (**ELSEVIER**,* **UGC Journal no-62532**), Volume 8, pp.57-62, April 2016.

[6] Penchalaiah P, Ramesh Reddy K, "Secure and Cost Effective Cryptosystem Design Based on Random Multiple Key Streams", *Journal of Information Security Research,(* ISSN: 0976-4143) *DIRF Publisher*, Volume 7, Number 1, pp. 29-40, March 2016.

[7] S. Jin-Shu, C. Dan, W. Xiao-Feng, and S. Yi-Pin, ``Attributed-based encryption schemes," J. Softw., vol. 22, no. 6, pp. 12991315, 2011.

[8] X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, "Data mining with big data," IEEE Trans. Knowl. Data Eng., vol. 26, no. 1, pp. 97-107, Jan. 2014.

[9] Z. Pervez, A. M. Khattak, S. Lee, and Y.-K. Lee, ``SAPDS: Self-healing attribute-based privacy aware data sharing in cloud," J. Supercomputer. vol. 62, no. 1, pp. 431460, Oct. 2012.

