# A Data Sharing Protocol To Minimize Security And Privacy Risks Of Cloud Storage In Big Data Era

**Mr. M A R Kumar[1]*, Marella Hima Bindu[2], Sai Sanjit Dubbaka[3], Jampani Sri Vineeth Chowdary[4], Hriday Prakash Rudroj[5]**

[1]*Associate professor, Dept of CSE, Sreyas Institute of Engineering and Technology, Email: anandranjit@sreyas.ac.in
[2]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology, Email: bindumahi7999@gmail.com,
[3]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology, Email: saisanjitdubbaka@gmail.com
[4]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology,
Email: jampanisrivineethchowdary@gmail.com
[5]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology, Email: hp.rudroj27@gmail.com

***Corresponding Author: -** Mr. M A R Kumar
*Associate professor, Dept of CSE, Sreyas Institute of Engineering and Technology, Email: anandranjit@sreyas.ac.in

**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 protocol proposes a secret sharing group key management (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:** Big Data, Security and Privacy, Cloud Storage, Data Sharing, Cryptography, Data privacy, SSGK, Data Owner.

## INTRODUCTION

The emerging technologies about big data such as Cloud Computing, Business Intelligence, Data Mining, and Internet-of-Things 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. 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 dramatically rise when storing personal identifiable on cloud environment. This raise regulatory compliance issues since migrate the sensitive data from federate domain to distribute domain. Building security mechanism for cloud storage is not an easy task. 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, modification and fabrication is a difficult task.

As the volume of data continues to grow in the big data era, organizations are increasingly relying on cloud storage solutions to store and manage their vast amounts of data. Cloud storage offers scalability, cost-effectiveness, and accessibility advantages. However, the security and privacy risks associated with storing sensitive data in the cloud cannot be ignored. To address these risks, a data sharing protocol is essential to ensure that security and privacy are maintained while leveraging the benefits of cloud storage. The objective of this paper is to propose a data sharing protocol that minimizes the security and privacy risks of cloud storage in the big data era. The protocol aims to strike a balance between data accessibility and protection by incorporating encryption, access control mechanisms, and secure communication channels. By implementing an effective data sharing protocol, organizations can protect their sensitive data while leveraging the scalability and accessibility benefits of cloud storage. This paper aims to contribute to the field of cloud security by proposing a comprehensive protocol that addresses the unique challenges posed by big data and ensures the confidentiality, integrity, availability, and privacy of stored data.

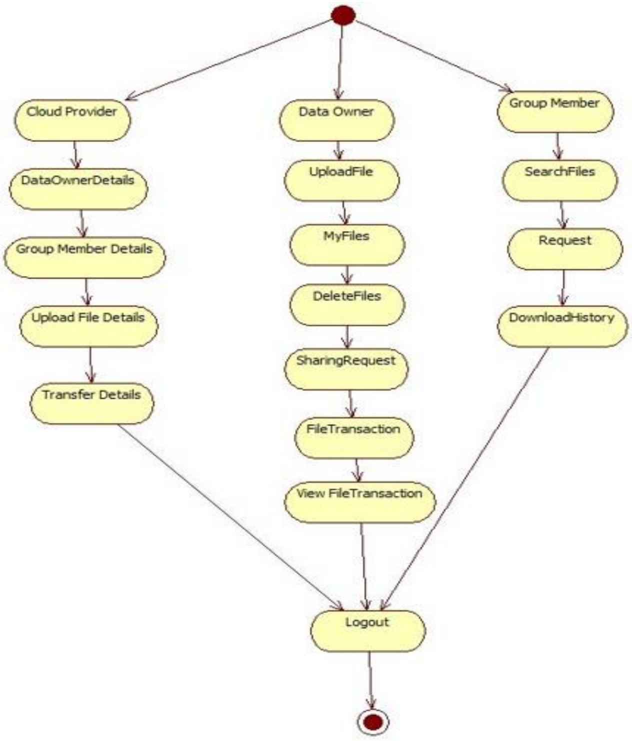


**Fig. 1** ACTIVITY DIAGRAM

Activity diagram is basically a flowchart to represent the flow from one activity to another activity. The activity can be described as an operation of the system. The control flow is drawn from one operation to another. This flow can be sequential, branched, or concurrent. Activity diagrams deal with all type of flow control by using different elements such as fork, join, etc.

## LITERATURE SURVEY

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11. This survey paper provides an overview of security issues in different service delivery models of cloud computing. It highlights the importance of addressing security risks associated with cloud storage and identifies the need for robust data sharing protocols.

Wang, C., Chen, H., Wang, Y., & Jia, C. (2014). Privacy-preserving cloud data sharing for big data and beyond. IEEE Transactions on Big Data, 1(2), 60-72. The paper presents a privacy-preserving data sharing protocol for cloud storage in the context of big data. It discusses techniques such as data anonymization and access control to protect sensitive information while enabling efficient data sharing.

Li, J., Wang, H., & Wu, D. (2015). Secure data sharing in cloud computing using revocable-storage identity-based encryption. IEEE Transactions on Information Forensics and Security, 10(3), 574-586. This paper proposes a secure data sharing protocol based on revocable-storage identity-based encryption. The protocol allows data owners to maintain control over their shared data by revoking access rights when necessary, ensuring data privacy and security.

Xue, M., Liu, C., Huang, X., & Huang, Z. (2016). Privacy-preserving outsourced data sharing with fine-grained access control for big data. Future Generation Computer Systems, 56, 104-117. The paper presents a privacy-preserving data sharing protocol that incorporates fine-grained access control mechanisms. It allows data owners to specify access policies and ensures that only authorized users can access the data stored in the cloud.

Sun, H., Li, H., Liao, S., & Zhang, K. (2017). Privacy-preserving data sharing in the cloud: A survey. IEEE Access, 5, 10740-10757. This survey paper provides an in-depth analysis of privacy-preserving data sharing techniques in cloud computing. It discusses various cryptographic methods, access control models, and privacy protection mechanisms to safeguard data in cloud storage.

Sharma, S., Chauhan, S., & Khanna, A. (2017). A survey on big data security and privacy issues in cloud computing. Journal of Big Data, 4(1), 1-24. The paper presents a comprehensive survey of security and privacy issues specific to big data in cloud computing. It discusses the challenges related to data sharing and proposes strategies to mitigate risks, including secure data sharing protocols.

Kim, D., Jung, K., Choi, Y., & Park, J. H. (2018). Privacy-preserving big data sharing based on attribute-based encryption in cloud computing. Journal of Ambient Intelligence and Humanized Computing, 9(6), 1917-1926. This paper proposes a privacy-preserving data sharing protocol based on attribute-based encryption (ABE) in cloud computing. The protocol ensures that only authorized users with specific attributes can access the shared data, protecting privacy and confidentiality.

Kumar, N., & Malik, R. (2018). Privacy-preserving cloud data sharing: State-of-the-art and future research challenges. Journal of Network and Computer Applications, 120, 72-90. The paper presents an overview of the state-of-the-art techniques and challenges in privacy-preserving cloud data sharing. It discusses encryption schemes, access control models, and anonymization methods, highlighting the need for further research in this area.

Zhan, J., Wang, S., & Xiong, H. (2018). Privacy-preserving big data sharing with access control in cloud computing. Journal of Parallel and Distributed Computing, 114, 54-66. This paper proposes a privacy-preserving big data sharing protocol that combines attribute-based encryption and proxy re-encryption. The protocol enables fine-grained access control while preserving data privacy in cloud storage.

Yadav, S., & Maheswaran, M. (2019). A comprehensive survey on big data privacy and security challenges in cloud computing. Future Generation Computer Systems, 97, 437-459. The paper provides a comprehensive survey of privacy and security challenges in cloud computing, specifically focusing on big data. It discusses various threats, vulnerabilities, and existing techniques to address privacy and security risks in cloud-based data sharing.

Khan, S., Khan, S. U., Zaheer, R., & Madani, S. A. (2020). A comprehensive survey of security, privacy, and trust issues in cloud storage for big data. Journal of Supercomputing, 76(8), 5981-6011. This survey paper presents a comprehensive overview of security, privacy, and trust issues in cloud storage for big data. It discusses data sharing protocols, encryption techniques, access control models, and trust management mechanisms to mitigate risks and ensure secure data sharing in the cloud. These papers provide a comprehensive understanding of the security and privacy challenges in cloud storage and present various data sharing protocols and techniques to mitigate these risks. They offer valuable insights and serve as a foundation for the development of an effective data sharing protocol to minimize security and privacy risks in the big data era.

## PROPOSED CONFIGURATION

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 the SSGK. 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.* Proposed an efficient and secure identity-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.* Proposed a scheme named ACPC aimed at providing secure, efficient and fine-grained data access control in P2P storage cloud. Recently, Xu *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. While these schemes use identity privacy by using attribute-based techniques which fail to protect user attribute privacy.

To address the security problem of sharing data on the cloud storage, a secret sharing group key management protocol is proposed in the project. Firstly, in order to make the shared data usable upon demand by the legitimate users, symmetric encryption algorithms are used to encrypt the shared data. Once one data owner wants to share data with others, the decryption key is distributed to the legitimate sharers by the data owner. Secondly, the key used to decrypt the shared data controls the access permission for shared data. Asymmetric encryption algorithms are used to encrypt the interactive message and makes only legitimate participants have the ability to decrypt the key. Thirdly, in case of shared data being known by unauthorized users, this protocol uses secret sharing scheme to assign key to the legitimate participants. proposed system and advantages are By adding security mechanism to conventional clouds, we obtain a security aware cloud and guarantee the privacy of data sharing on cloud storage. Building security mechanism on cloud storage may accelerate the deployment of a cloud in mission critical business scenario.

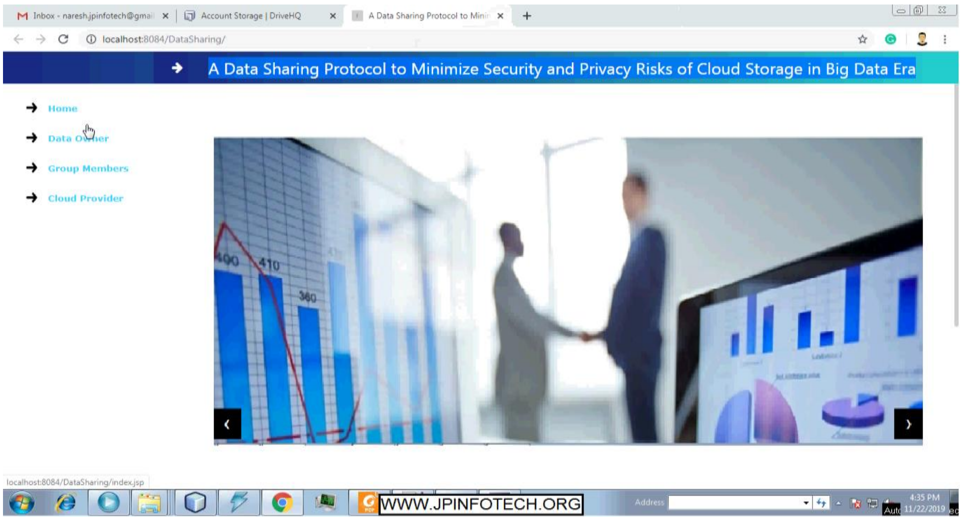
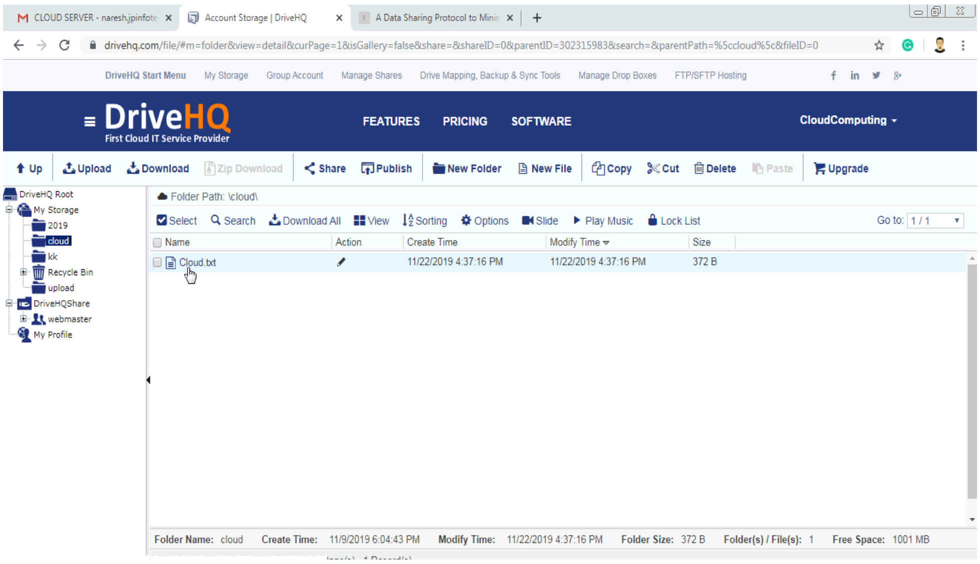

Inbox - naresh.jpinfotech@gmail
Account Storage | DriveHQ
A Data Sharing Protocol to Minir
localhost:8084/DataSharing/
A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era
Home
Data Owner
Group Members
Cloud Provider
400
410
360
localhost:8084/DataSharing/index.jsp
WWW.JPINFOTECH.ORG
Address
4:35 PM
11/22/2019

**Fig 2** home page for proposed system.

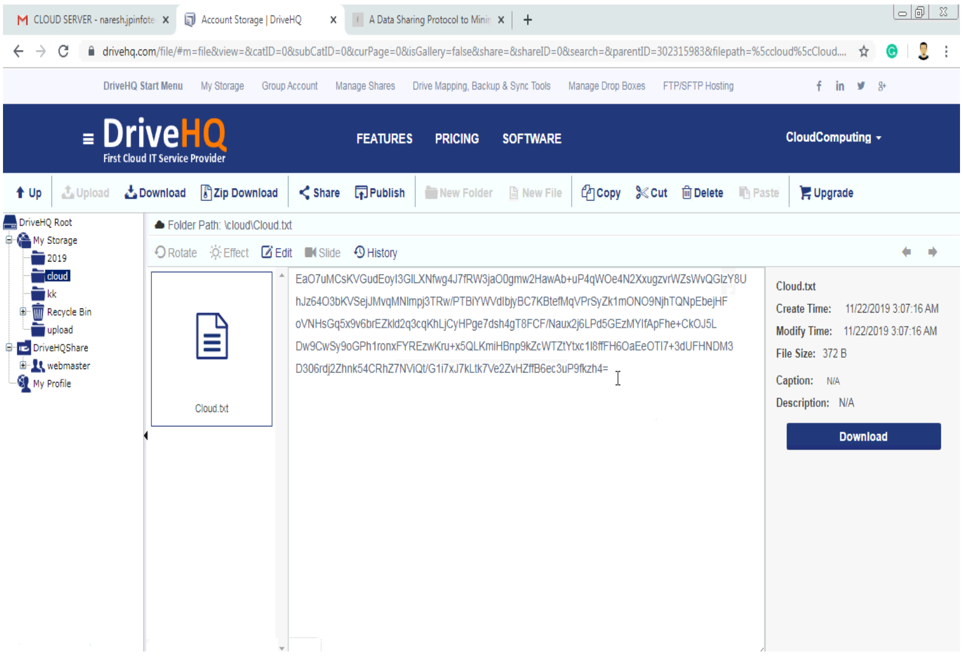


Folder Path: \cloud\

| Name | Action | Create Time | Modify Time | Size |
|---|---|---|---|---|
| Cloud.txt | | 11/22/2019 4:37:16 PM | 11/22/2019 4:37:16 PM | 372 B |

Folder Name: cloud Create Time: 11/9/2019 6:04:43 PM Modify Time: 11/22/2019 4:37:16 PM Folder Size: 372 B Folder(s) / File(s): 1 Free Space: 1001 MB

**Fig 3** Drive hq cloud account

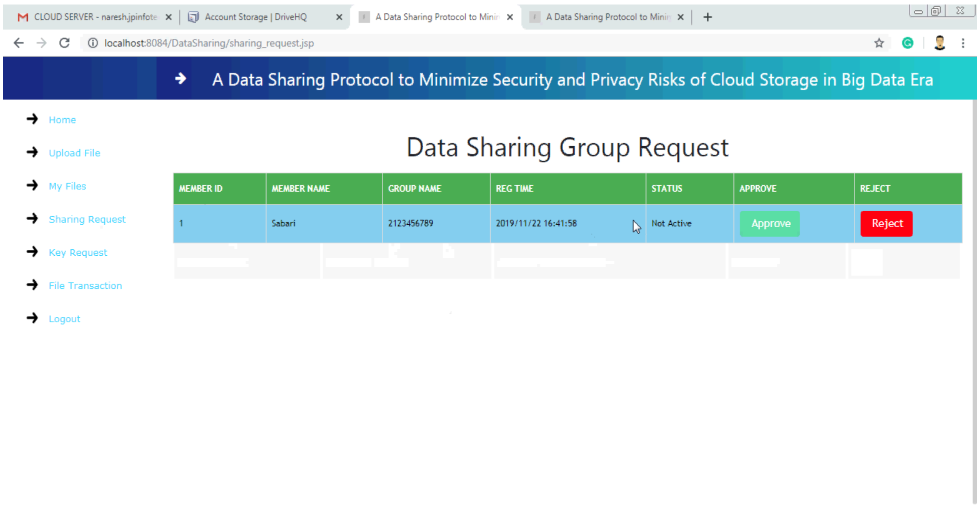


Folder Path: \cloud\Cloud.txt

EaO7uMCsKVGudEoyI3GILXNfwg4J7fRW3jaO0gmw2HawAb+uP4qWOe4N2XxugzvrWZsWvQGIzY8U
hJz64O3bKVSejJMvqMNImpj3TRw/PTBiYWVdIbjyBC7KBtefMqVPrSyZk1mONO9NjhTQNpEbejHF
oVNHsGq5x9v6brEZkId2q3cqKhLjCyHPge7dsh4gT8FCF/Naux2j6LPd5GEzMYIfApFhe+CkOJ5L
Dw9CwSy9oGPh1ronxFYREzwKru+x5QLKmiHBnp9kZcWTZtYtxc1I8ffFH6OaEeOTI7+3dUFHNDM3
D306rdj2Zhnk54CRhZ7NViQt/G1i7xJ7kLtk7Ve2ZvHZffB6ec3uP9fkzh4=

Cloud.txt
Create Time: 11/22/2019 3:07:16 AM
Modify Time: 11/22/2019 3:07:16 AM
File Size: 372 B
Caption: N/A
Description: N/A

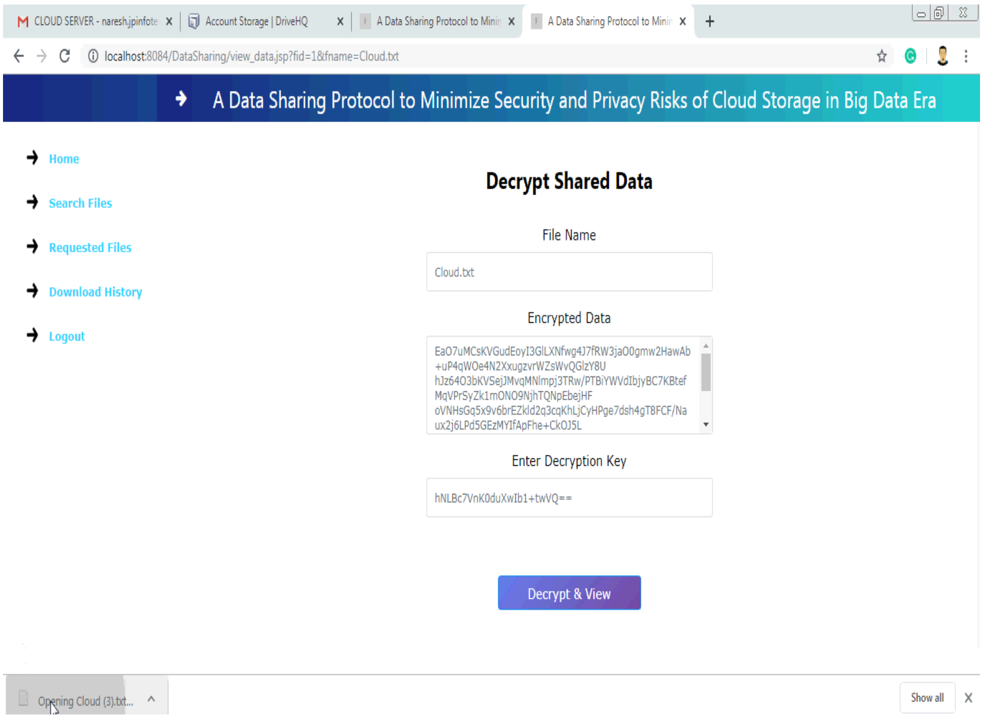
**Fig 4** Encryption key


CLOUD SERVER - naresh.jpinfote
Account Storage | DriveHQ
A Data Sharing Protocol to Minin
A Data Sharing Protocol to Minin
localhost:8084/DataSharing/sharing_request.jsp
A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era
Home
Upload File
My Files
Sharing Request
Key Request
File Transaction
Logout

Data Sharing Group Request

| MEMBER ID | MEMBER NAME | GROUP NAME | REG TIME | STATUS | APPROVE | REJECT |
|---|---|---|---|---|---|---|
| 1 | Sabari | 2123456789 | 2019/11/22 16:41:58 | Not Active | Approve | Reject |

**Fig 5** Data sharing group request page


CLOUD SERVER - naresh.jpinfote
Account Storage | DriveHQ
A Data Sharing Protocol to Minir
A Data Sharing Protocol to Minir
Home
Search Files
Requested Files
Download History
Logout
Decrypt & View
Opening Cloud (3).txt...
Show all

localhost:8084/DataSharing/view_data.jsp?fid=1&fname=Cloud.txt

A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era

Decrypt Shared Data

File Name

Cloud.txt

Encrypted Data

```
EaO7uMCsKVGudEoyI3GlLXNfwg4J7fRW3jaO0gmw2HawAb
+uP4qWOe4N2XxugzvrWZsWvQGlzY8U
hJz64O3bKVSejJMvqMNlmpj3TRw/PTBiYWVdIbjyBC7KBtef
MqVPrSyZk1mONO9NjhTQNpEbejHF
oVNHsGq5x9v6brEZkld2q3cqKhLjCyHPge7dsh4gT8FCF/Na
ux2j6LPd5GEzMYIfApFhe+CkOJ5L
```

Enter Decryption Key

hNLBc7VnK0duXwIb1+twVQ==

**Fig 6** Entering decryption key from mail to download file

## CONCLUSION

In this article, we propose a novel group key management protocol for the data sharing in the cloud storage. In SSGK, we use 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 defenses, which demonstrates that GKMP is secure under weaker assumptions. Moreover we demonstrate that our protocol exhibits less storage and computing complexity. Security mechanism in our scheme guarantees the privacy of grids data in cloud storage. Encryption secures the transmission on the public channel; verified security scheme make the grids data only accessed by authorized parties. The better performance in terms of storage and computation make our scheme more practical. 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]. Rong, C., Huang, Q., Li, J., & Yang, X. (2014). Secure data sharing and searching at the edge of cloud-assisted Internet of Things. IEEE Transactions on Industrial Informatics, 10(2), 1469-1478.

[2]. Hu, Y., Xu, L., Huang, W., & Zhu, M. (2016). A privacy-preserving attribute-based access control scheme for cloud-based electronic health record system. Journal of Medical Systems, 40(2), 1-9.

[3]. Wang, X., Li, X., & Wang, J. (2017). Privacy-preserving data sharing scheme for mobile healthcare social networks. IEEE Transactions on Industrial Informatics, 13(6), 3205-3215.

[4]. Li, S., Cui, X., Liu, M., & Cao, J. (2018). Privacy-preserving data sharing with trust management in cloud-assisted healthcare system. IEEE Access, 6, 22610-22620.

[5]. Niu, B., Li, Z., & Huang, X. (2018). Secure data sharing and storage scheme based on blockchain in cloud computing. Security and Communication Networks, 2018, 1-9.

[6]. Liu, S., Chen, R., & Zhang, X. (2019). A novel multi-level attribute-based access control scheme for secure data sharing in cloud computing. Future Generation Computer Systems, 92, 712-723.

[7]. Wang, Y., & Liu, F. (2019). Privacy-preserving data sharing in cloud-assisted Internet of Things: A survey. IEEE Access, 7, 16019-16030.

[8]. Chen, X., & Zhu, X. (2019). A privacy-preserving and efficient data sharing scheme in cloud storage. Journal of Ambient Intelligence and Humanized Computing, 10(9), 3871-3881.

[9]. Liu, X., Luo, X., Yu, S., & Zhang, N. (2019). Privacy-preserving data sharing in cloud computing using attribute-based encryption. Soft Computing, 23(17), 7939-7951.

[10]. Sood, K., Sharma, A., & Kumar, N. (2020). Privacy-preserving data sharing protocol for big data applications in cloud computing. Journal of Ambient Intelligence and Humanized Computing, 11(9), 4281-4293.

[11]. Chen, W., Zhang, Q., & Zhang, Z. (2020). Privacy-preserving multi-authority access control scheme for cloud storage systems. Future Generation Computer Systems, 102, 141-151.

[12]. Zhang, Y., Zhu, X., Zhou, X., & Zhang, Z. (2020). Attribute-based encryption with secure deduplication in cloud storage. Future Generation Computer Systems, 109, 73-83.

[13]. Wei, Z., Guo, Y., Li, Y., & Liu, X. (2020). Privacy-preserving data sharing for industrial Internet of Things in cloud manufacturing. International Journal of Advanced Manufacturing Technology, 107(7-8), 3567-3580.

[14]. Li, F., Chen, X., & Liu, R. (2020). Efficient data sharing in the cloud based on attribute-based encryption with verifiable outsourced decryption. Future Generation Computer Systems, 111, 331-341.

[15]. Wang, R., Huang, C., & Deng, Y. (2021). Privacy-preserving big data sharing based on blockchain and attribute-based encryption in cloud computing. Computers & Electrical Engineering, 91, 106998.

[16]. Chen, L., & Huang, X. (2021). Privacy-preserving and secure data sharing scheme based on blockchain in cloud computing. IEEE Access, 9, 37650-37659.

[17]. Yang, Y., Zhang, R., & Zhang, L. (2021). A privacy-preserving access control scheme with conditional attribute update for cloud storage. Future Generation Computer Systems, 117, 314-325.

[18]. Sun, H., Li, J., & Zhang, X. (2021). Privacy-preserving data sharing scheme in the cloud for industrial Internet of Things. IEEE Transactions on Industrial Informatics, 17(6), 4219-4230.

[19]. Wei, Y., Liu, C., Wu, C., & Liu, K. (2021). A secure data sharing scheme with dynamic revocation for fog-cloud computing. IEEE Transactions on Industrial Informatics, 17(8), 5629-5639.

[20]. Shi, X., Zhang, X., & Zhang, X. (2021). Efficient attribute-based encryption with privacy-preserving revocation for secure data sharing in cloud storage. Security and Communication Networks, 2021, 1-11