International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 01-06 www.ijaem.net ISSN: 2395-5252

Group Key Management Protocol for File Sharing on Cloud Storage

[1]Mallikarjuna Reddy, [2]Mr S Balamurugan, [3]Dr N Naveen Kumar

[1] PG Research Scholar, [2] Assistant Professor, [3] Associate Professor
[1,2,3] Department of Computer Applications
Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India.

Date of Submission: 25-08-2022 Date of Acceptance: 05-09-2022

ABSTRACT
The large-scale sharing desires of the many enterprises promote the event of cloud storage. whereas the cloud computing stores the shared files outside the trust domain of the owner, the strain and issues for file security is arising. during this paper, a Group Key Management Protocol for file sharing on cloud storage (GKMP) is2 planned. faced with network attacks from public channel, a gaggle key generation theme supported mixed coding technology is planned. And a verification theme is employed to forestall shared files from being attacked by the collusion attack of cloud providers and cluster members. Security and performance analyses indicate that the planned protocol is each secure and economical for knowledge sharing in cloud computing. [1]

Keywords- Asymmetric Key Cryptography, Data Security, Cloud Storage, File Sharing, Group Key, Distribution of Key.

I. INTRODUCTION

Cloud storage systems are the supply of attraction for the web users thus on have easy accessibility anyplace and anytime. several on-line service suppliers have thrived to serve the individual users, industrialists additionally because the business folks to own their knowledge on cloud with reliableness and security. faced with today's innovative blow-up of cloud technologies, reconstruction services in terms of cloud became a lot of standards. in an exceedingly shared-tenancy cloud computing surroundings, knowledge from totally different purchasers which may which might be hosted on separate virtual machines may reside on one physical machine. Faced with today's innovative blow-up of cloud technologies, reconstruction services in terms of cloud became a lot of standards. in an exceedingly shared-tenancy cloud computing surroundings, knowledge from totally different purchasers which may which might be hosted on separate virtual machines may reside on one physical machine. beneath this paradigm, the information storage and management area unit beneath full management of the cloud supplier, thus knowledge homeowners' area unit left vulnerable and need to only think about the cloud supplier to safeguard their knowledge.

Recent news shows that Google provided the law enforcement agency all the documents of its users when receiving a look warrant, however the users haven't been tuned in to the search till they're in remission. as a result of cloud supplier has the complete access to the information, the privacy of knowledge of information may well be desecrated if users' data is intercepted or changed by the cloud supplier. there's a series of cryptologic schemes beneath such circumstance that a third-party auditor is ready to visualize the provision of files whereas nothing regarding the file leaks. Likewise, cloud users most likely won't hold the belief that the cloud server is doing an honest job in terms of confidentiality. The cloud users area unit intended to encipher their files with their own keys before uploading them to the cloud server. The remaining challenge is a way to share and manage the cryptologic keys among valid users while not the participant of the cloud supplier.[1]

II. LITERATURE REVIEW

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system, the above consideration is taken into account for developing the proposed system.

III. ARCHITECTURE AND WORKDONE

The flow for the project is given below Fig1..1

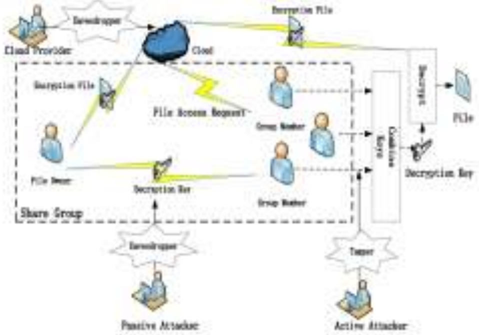

Fig1.1 Architecture of proposed system

EXISTING METHOD:

Compared to CFS and NASD, CFS is tailored towards single-user workstations and relied on user-supplied passwords for data encryption. NASD proposes a distributed system comprising intelligent disks and users supplied keys as proofs of authorization. While these schemes use identity privacy by using attribute-based techniques which fail to protect user attribute privacy. The drawbacks of existing classification and security techniques are:

- Does not prevent outside attacks.
- Not secure.
- Cannot prevent the shared files.

PROPOSED METHOD:

In proposed scheme, the verification scheme is used to prevent shared files from being attacked by the collusion attack of cloud providers and group members. Security and performance analyses indicate that the proposed protocol is both secure and efficient for data sharing in cloud computing. Faced with network attacks from public channel, a group key generation scheme based on mixed encryption technology is proposed. The advantages are:

- Verification of protocols can be done
- Trustable

APPLICATIONS:

Health Care: Breaking a downward trend over the past two years, a Ponemon study found that both the organizational cost of data breach and the cost per lost or stolen record have increased. On average, the cost of a data breach for an organization represented in the study increased from $5.4 million to $5.9 million. The cost per record increased from $188 to $201.

- Malicious or criminal attacks result in the highest per capita data breach cost.
- Consistent with prior reports, data loss or exfiltration resulting from a malicious or criminal attack yielded the highest cost at an average of $246 per compromised record. In contrast, both system glitches and employee mistakes resulted in a much lower average per capita cost at $171 and $160, respectively.
- The results show that a probability of a material data breach over the next two years involving a minimum of 10,000 records is nearly 19 percent.

To resolve this issue, the healthcare organization brought up the challenge of data residing at the end-point and deployed a proactive mobility control and monitoring solution. Leveraging Cisco technologies, firewall management, data loss prevention engines, and better file sharing controls, data at the end-point was basically eliminated. It was replaced with secure access to central data repositories wrapped with greater controls.

Organizations: Cloud file-sharing is the process of sharing data and files over the internet between multiple users. Some IT managers choose to go for flexible and convenient options of file-sharing that would be cost-effective plus time-efficient and this cloud solution just fits in rightly. Given the remote access feature of cloud, users can access their data from any device or location. Nowadays, technology has become the core requirement and efficient business tool. Businesses keep growing and as it outspreads its boundaries to different areas, it necessitates secure platform for file exchange and storage. With the ever-increasing amount of data, there's a need to store it somewhere safe as organizations largely deals with sensitive information. Here is how cloud-based file sharing can benefits organizations.

There are several issues such as Data Security, Network related issues, Scalability, CIA and Privacy.

Data Security: Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.

When properly implemented, robust data security strategies will protect an organization's information assets against cybercriminal activities, but they also guard against insider threats and human error, which remains among the leading causes of data breaches today. Data security involves deploying tools and technologies that enhance the organization's visibility into where its critical data resides and how it is used. Ideally, these tools should be able to apply protections like encryption, data masking, and redaction of sensitive files, and should automate reporting to streamline audits and adhering to regulatory requirements. Data security uses tools and technologies that enhance visibility of a company's data and how it is being used. These tools can protect data through processes like data masking, encryption, and redaction of sensitive information. The process also helps organizations streamline their auditing procedures and comply with increasingly stringent data protection regulations. A robust data security management and strategy process enables an organization to protect its information against cyberattacks. It also helps them minimize the risk of human error and insider threats, which continue to be the cause of many data breaches.

Network related issues: Cloud storage security has improved significantly over the past few years, but that doesn't mean administrators can rest easy. Cloud storage security issues are still common, exposing enterprise data to unauthorized parties. This could potentially lead to angry customers, furious business partners, costly lawsuits and other headaches. Below are the cloud storage security risks, and tips on how to avoid them. Misconfiguration, Insufficient Data Governance, Poor Access Controls, Inadequate Security Controls and Sketchy regulatory compliance.

Scalability: Scalability becomes crucial in this environment, ensuring that security strategies and services continue to close any gaps while at the same time, not impact productivity by introducing bottlenecks to the operation lifecycles. The process for developing a cyber security strategy for a healthy security posture should include the following aspects:

- Infrastructure
- Procedures
- Cyber Security Strategies

CIA:

Confidentiality: When doing business with clients and prospects, it is common to collect and store their personal information. Names, email addresses and phone numbers are a few examples of personal information. This is sensitive data that your company is responsible for protecting and securing. Relying and trusting your cloud or CRM provider is not enough. Your business needs to enforce extra security measures to ensure that your clients and prospects' privacy is safeguarded. Protecting confidentiality can start from defining and controlling access levels of information internally and externally. For example, those who work in the IT department that typically don't interact with clients and prospects, should not have access to client information. If someone does not need a type of information to perform their work, then they should not have access to that information. When data accessibility is limited, you significantly lower the chances of having information being leaked accidentally or intentionally.

Examples of confidentiality risks include data breaches caused by criminals, insiders inappropriately accessing and/or sharing information, accidental distribution of sensitive information to too wide of an audience.

Integrity: Integrity means that data or information in your system is maintained so that it is not modified or deleted by unauthorized parties. This is an important element of data hygiene, reliability and accuracy. To reserve data integrity, the easiest methods are backing up your data, using access controls, monitoring your audit trail and encrypting your data.

Examples of attacks on integrity include email fraud attacks (which compromise the integrity of communications), financial fraud and embezzlement through modification of financial records, even attacks like Stuxnet that impacted the integrity of industrial control systems data flows to cause physical damage.

Availability: The final component of the CIA Triad is availability. It means that systems and data are available to individuals when they need it under any circumstances, including power outages or natural disasters. Without availability, even if you have met the other two requirements of the CIA Triad, your business can be negatively impacted. To ensure availability, your organization can use redundant networks, servers and applications. These can be programmed to become available when the primary system is broken down. Besides having backups, the design of IT architecture plays a key role as well. For instance, if high availability is a component of your IT systems, then you could maintain a certain level of operational performance for an extended period of time even in unexpected circumstances.

IV. RESULT & DISCUSSION

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of tests. Each test type addresses a specific testing requirement.

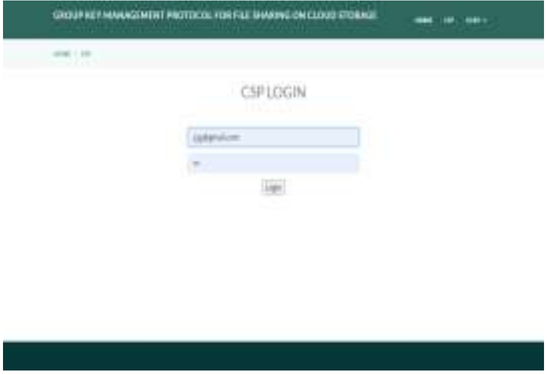
GROUP KEY MANAGEMENT PROTOCOL FOR FILE SHARING ON CLOUD STORAGE
CSP LOGIN
Login

Fig: 4.1 Input Login Screen for the CSP

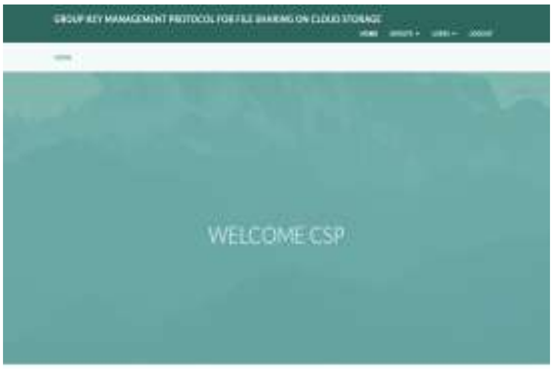
GROUP KEY MANAGEMENT PROTOCOL FOR FILE SHARING ON CLOUD STORAGE
WELCOME CSP

Fig: 4.2 After CSP Login, Screen for the user

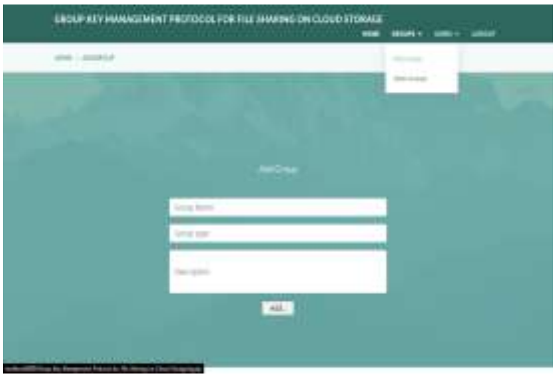
GROUP KEY MANAGEMENT PROTOCOL FOR FILE SHARING ON CLOUD STORAGE
Add Group
ADD

Fig: 4.3 Add Group Screen for CSP

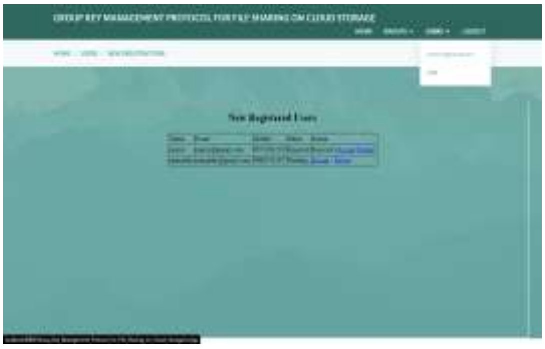
GROUP KEY MANAGEMENT PROTOCOL FOR FILE SHARING ON CLOUD STORAGE
New Registered Users

Fig: 4.4 New Registered Users Screen

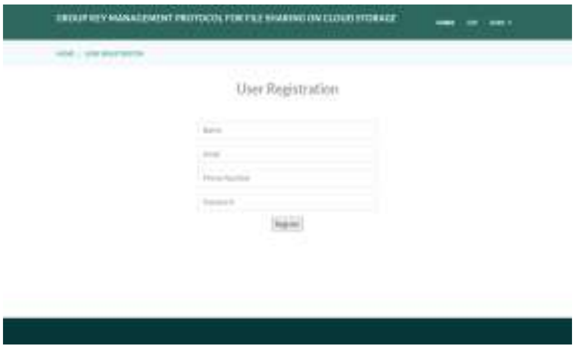
GROUP KEY MANAGEMENT PROTOCOL FOR FILE SHARING ON CLOUD STORAGE
User Registration
Register

Fig: 4.5 User Registration Screen

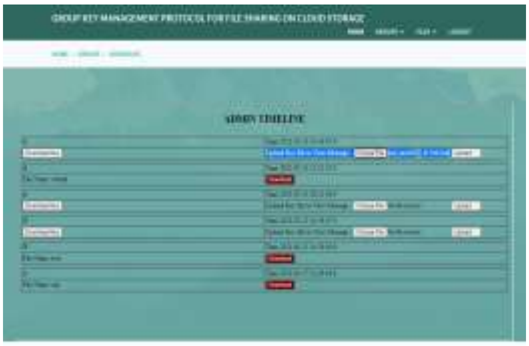
GROUP KEY MANAGEMENT PROTOCOL FOR FILE SHARING ON CLOUD STORAGE
ADMIN TIMELINE

Fig: 4.6 Admin Timeline Screen

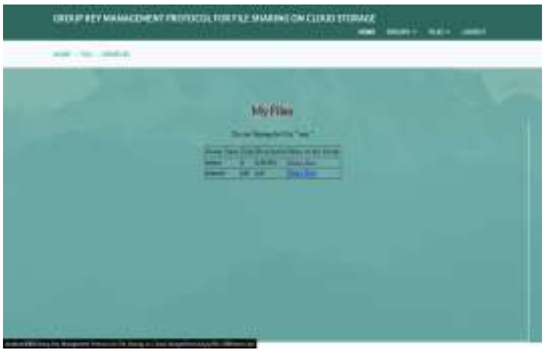
GROUP KEY MANAGEMENT PROTOCOL FOR FILE SHARING ON CLOUD STORAGE
My Files

Fig: 4.7 My Files Screen for User

Group Members: Group Members (GM) are a pool of registered users that will be store their private data into the cloud server and share them using others in the group. Both Group Admin and group member can login using their login details. When a successful login, Group Admin make active newly added members of the cloud by generating keys for each member and sends it to the consistent group members. It can also check the group details and group key. After successful login, Group Members signature is verified. After successful verification, the group member can upload, download and can modify the files. Group Admin must be encrypting data files before uploading to the cloud. Group member encrypt with group key and Group Admin response and shared the public key. After that GM will be decrypt with Public and private key.

Key Generation and Encryption: Initially, data owner has to register in trusted third-party system for keeping the files in cloud environment. Data owners create the login credentials for uploading files and those credentials are also used to upload the user lists and their permissions. After receiving a particular file (F) from the data owner, the TTP generates keys by using asymmetric key encryption. Asymmetric key generation is not discussed in this paper and it is assumed that any standard asymmetric key generation algorithm (APKI) is utilized for this purpose.

Decryption of File: The data owner provides user list/access permission list (UAPL), user specific security questions and answers, number of file access permission to the TTP server. The data owner invites all the users given in the access control list with the link to the TTP and half or part of owner's public key for self-registration. When a user wants to access the uploaded file in the cloud, the user initially registers with the TTP. Once user registration is completed, the user gets login credentials from the TTP. After successful authentication between TTP and requesting user, the user request any particular file through File Identification (F_{ID}) along with the part of the public key provided to it by the data owner. TTP validates the user access permission for that particular requested file. The TTP regenerates the public key by combining its own half or part of the public key and the received half or part of the public key from the user. In the meanwhile, the TTP downloads the requested file in the encrypted form from the cloud data storage. The downloaded file is then decrypted using the regenerated public key.

Encryption and Decryption Process: Encryption and Decryption in cryptography mechanism are the vital elements for establishing security in cloud computing environment. The encryption and decryption process are performed in PKI through RSA, ElGamal and Paillier algorithms. The comparison of the PKI algorithms in terms of time consumption during the process of encryption and decryption when 10 KB file is used highlights that RSA performs better as shown in Figure 5. However, the RSA algorithm degrades in its performance during the encryption of large files in the order of hundreds of MB size. But ElGamal and Paillier are proved for its usage in encrypting large size files. The comparison of both ElGamal and Paillier exhibits their performance equally when the proposed methodology of key management is utilized.

USER:

- **Registration:** User registers with their details.
- **Login:** After CSP accepted user registration user can login with their email id and password.
- **Groups:** View User joined group and view file in groups. raise a request for file accessing.
- **Files:** In this user can upload files and view files and download files and share file into their joined group.

CSP (CLOUD SERVICE PROVIDER):

- **Login:** Login with valid email id and password.
- **Add groups:** CSP can add groups, In the group adding form contains group name, max limit of members.
- **User joining requests:** In this new user registration list. Here CSP can accept new user into group.

V. CONCLUSION

In this paper, we propose a novel group key management protocol for file sharing on cloud storage. Public key is used by GKMP to guarantee the group key distribute fairly and resist attack from compromised vehicles or the cloud provider. We give detailed analysis of possible security attacks and corresponding defence, which demonstrates that GKMP is secure under weaker assumptions. Moreover, the storage overhead and the computation and communication cost reduced. Our scheme efficient and effective data sharing in cloud application.

FUTURE SCOPE

In future we can implement to add security authentication schemes for data sharing and also implement to data auditing schemes.

REFERENCES

[1]. Po-Wen. C, Chin L," Audit-Free Cloud Storage via Deniable Attribute Based

Encryption", IEEE Transactions on Cloud Computing, vol.6, no.2, pp. 414-427, 2018.

[2]. J. Zhou et al., "Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation", Comput. J., vol. 60, no. 8, pp. 1210-1222, Aug. 2017.

[3]. J. Wu, Y. Li, T. Wang, et al. CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing, IEEE Access, vol.7, pp.160482-160497, 2019.

[4]. Hu.X, Jianfei.S, "Comments on Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing", IEEE Transactions on Dependable and Secure Computing., vol. 14, no.4, pp. 461-462, Aug.2017.

[5]. J. Shao, R. Lu, X. Lin, "Fine-grained data sharing in cloud computing for mobile devices", Proc. IEEE Conf. Comput. Commun. (INFOCOM), pp. 2677-2685, Apr./May 2015.

[6]. R. Ahuja S. K. Mohanty K. Sakurai "A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing" Comput. Elect. Eng. vol. 57 pp. 241-256 Jan. 2017.

[7]. S. Roy, A.K. Das, S. Chatterjee, etal, "Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications" IEEE Transactions on Industrial Informatics vol. 5 no. 1 pp. 457-468 Jan. 2019.

[8]. Z. Fu X. Sun S. Ji G. Xie "Towards efficient content-aware search over encrypted outsourced data in cloud" Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM) pp. 1-9 Apr. 2016.

[9]. M. Blaze." A Cryptographic File System for Unix", 1st ACM Conf. Comp. and Commun. Sec., 1992,11, pp 9-15.

[10]. H. Gobioff.:" Security for a High-Performance Commodity Storage Subsystem", PhD thesis, Carnegie MellonUniv, 1999.

[11]. E. Miller." Strong Security for Network-Attached Storage", Conf. File and Storage Tech, 2002,6,pp 1??13.

[12]. Y. S. Rao "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing" Future Gener. Comput. Syst. vol. 67 pp. 133-151 Feb. 2017.

[13]. S. Jin-Shu C. Dan W. Xiao-Feng S. Yi-Pin " Attributed-based encryption schemes". J. Softw. vol. 22 no. 6 pp. 1299-1315 2011.

[14]. H. liu Y. huang J. K. Liu "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption" Future Gener. Comput. Syst. vol. 52 pp. 67-76 Nov. 2015.

[15]. K. Huang et al. "PKE-AET: Public key encryption with authorized equality test" Comput. J. vol. 58 no. 10 pp. 2686-2697 Oct. 2015.

[16]. L. Wu Y. Zhang K.-K. R. Choo D. He "Efficient and secure identity-based encryption scheme with equality test in cloud computing" Future Gener. Comput. Syst. vol. 73 pp. 22-31 Aug. 2017.

[17]. Q. Xu C. Tan Z. Fan W. Zhu Y. Xiao F. Cheng "Secure multi-authority data access control scheme in cloud storage system based on attribute-based signcryption" IEEE Access vol. 6 pp. 34051-34074 2018.

[18]. H. He R. Li X. Dong Z. Zhang "Secure efficient and fine-grained data access control mechanism for P2P storage cloud" IEEE Trans. Cloud Comput. vol. 2 no. 4 pp. 471-484 Oct./Dec. 2014.

[19]. K. Xue et al. "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage" IEEE Trans. Inf. Forensics Secur. vol. 12 no. 4 pp. 953-967 Apr. 2017.

[20]. Z. Pervez A. M. Khattak S. Lee Y.-K. Lee "SAPDS: Self-healing attribute based privacy aware data sharing in cloud" J. Supercomput. vol. 62 no. 1 pp. 431-460 Oct. 2012.

[21]. Courtois, Nicolas T. Bard, Gregory V.:" Algebraic cryptanalysis of the data encryption standard", CRYPTOGRAPHY AND CODING, PROCEEDINGS. 2007, (4887), pp 152-169.

[22]. E. Fujisaki T. Okamoto "Secure integration of asymmetric and symmetric encryption schemes" J. Cryptol. vol. 26 no. 1 pp. 80-101 Jan. 2013.