Cloud Data Sharing with Privacy Safeguards

T Pruthviraj Singh[1], Velaga Sohith Raghava[2], Pulakandam Venkata Siva Naga Hemanth[3], T Mahima Singh[4]
[1]*Madanapalle Institute of Technology & Science*
[2,3,4]*Amrita Vishwa Vidyapeetham*

Abstract—**Ensuring The trend and the road breaker of data storage is followed increasingly by cloud computing. In this continuous increase of technology, cloud computing is playing a significant function. There are several types of clouds, which include private, public, and hybrid clouds, where numerous people share and store the data. This process is described as multi-party data storage. Using the multi-party idea, the data of the legit person cannot be read or accessed by the not-legitimate person since the data of the legit person who tries to store it in the cloud throughout this procedure will be encrypted before it is stored. To decrypt the data that is saved. We need to have the key, for sure. The key illumination of the problem is that the data can be traced. In a cloud system, one file is stored where two to three persons access the data, whom we declare are legitimate users. But the patterns may be traced by the outsider. Additionally, the changes performed by the legit users are saved in the form of logs so that outsiders can examine the contents in the file. The existing method cannot keep up with the dynamic environment. To circumvent these, as clearly stated in this paper, the group manager is going to share a unique key with the user following the registration. After the manager's approval, the user can upload a file, and here the files will be encrypted. Access to the file will be given to just the authentic persons who are in the same group, and to add on to this, they only access it when they use a verification method involving group keys and signatures sent at registration. The user privacy is established because no one from the group knew who posted it. In addition to this, to decrypt the file even if it is secure because the key was sent by mail.**

I. INTRODUCTION

The advent of cloud computing has entirely transformed the way data is shared, accessed, and stored in this era of rapid digital transformation. Both organizations and individuals are increasingly relying on cloud platforms for their data management needs due to its unparalleled ease and scalability. But along with the advantages come serious worries about data security, confidentiality, and privacy especially in situations where group data sharing is involved. It is impossible to exaggerate the importance of safe and private-preserving procedures while sharing data in groups. Making sure that only the legit people can only access the shared data which is very important, it might be the company delicate documents or the personal health documents. Beyond that, protecting the privacy of individuals within a group and keeping their personal information safe adds another layer of complexity to the challenge. The main focus is to create a strong and authentic system for group data sharing in cloud computing. The main goal is to maintain privacy and ensure that no one can trace and misuse the data. Using advanced encryption methods, effective access controls, and strict verification processes, this approach aims to make data sharing among multiple users both secure and efficient.

The main objectives of this study are twofold: first is to ensure the security and confidentiality of the shared data by using access control and advanced encryption techniques. Second is to safeguard the users' privacy within the group by preventing unauthorized access to personal data and ensuring that conversations between users remain private. The proposed framework introduces various innovative features to obtain these objectives. It includes the strong user registration and authentication processes this helps to ensure that only authorized individuals can access the shared data. To maintain this end-to-end security, data is encrypted using the techniques like AES256 before being transferred to external cloud services. Access control methods, is managed by a designated group manager, which also make easier to approve and authorize users and files within the group. The suggested approach also highlights the significance of untrace ability, guaranteeing that user communications and data access patterns are not tracked down or recorded. The

framework tries to improve overall privacy and hide data access patterns by implementing strategies like oblivious random-access memory (ORAM) and proxy re-encryption.he goal of this project is to provide cloud computing environments with safe, private-preserving, and untraceable group data sharing solutions.

To upgrade the security in data sharing in this digital era, due to the various types of attacks at the moment this work provides a comprehensive framework. which accommodates the advanced cryptographic algorithms, strong access control mechanisms, and privacy-preserving techniques. Cloud computing, it is rapidly evolving domain, which is playing a pivotal role in the modern data management and collaboration by offering unparalleled accessibility and storage capabilities.

However, there are serious security risks when exchanging data across several users in this digital environment. Data untrace ability and secrecy rank first among these worries. By limiting access to shared information to just authorized users, data confidentiality protects the privacy of that information.

A. Problem Statement

The sharing of data among parties has become commonplace in modern cloud computing environments. As data sharing increases, there are many issues related to privacy, security, and confidentiality that need to be addressed. It is important to come up with a solid plan to deal with these difficulties of group data sharing in cloud environments. A major challenge is ensuring the security of user information and the privacy of data shared within a group. By using traditional data exchange methods, sensitive information is commonly not sufficiently protected against unwanted access or unintentional exposure. It is crucial to protect shared data in an era of increasingly sophisticated cyber-attacks. Shared information integrity and confidentiality are seriously threatened by unauthorized access, data breaches, and malicious attacks. In group data sharing settings, controlling access control can be challenging, especially when there are many individuals and different kinds of data involved. It is quite difficult to maintain cooperation convenience while ensuring only authorized users may access certain files. It is possible for user communication and data to compromise confidentiality and privacy. Traceable patterns can be accessed. Without adequate steps to hide data access patterns, sensitive data might be subject to illegal tracking or spying. Among the components of safe group data sharing are confirming users' identities and ensuring they have appropriate permissions. Cloud computing is used in every corner of the world these days because of its applicability. In any form of industry, data plays an influential role. And the saved data is needed by others in the same business. The key worry here is that if the data is saved on local devices, it cannot be viewed by far-away users. To store that data, we need huge-scale hardware. But hardware investment is impossible. By leveraging the cloud to store industry data, it is a practical solution. Because that industry franchise can be employed. By using the cloud, data is protected. The cloud data is too secure, but the real concern begins when a group of people need to access the same data. If a college has to save its marks and so on, before saving the data on the cloud server, the institution can encrypt it. But the biggest concern starts when this college joins another college for placement. The data stored in the cloud is sensitive information. Even that college has access to the files. But if any outsider distorts the data, it is a significant issue. The files are encrypted, but an outsider can track what and how he accesses the data. The group manager can generate a pass for a user to access the data. But creating so many passes would not be hypothetical. The primary concern begins when the data is traceable. Hence in this paper, we explicitly describe how data cannot be traceable. For an individual group key validated by the group manager, users register by email. Encrypted files are safely saved on a cloud server, providing privacy and security. Only authorised group members can access the files using email-based authentication keys. motive: The motive of this study is that the pupils' data is valuable and sensitive information. The file should be encrypted using a cryptographic algorithm to halt the connectivity between the data and the cloud server. This is because an outsider can attack the server, therefore that would be an important step. Add to this, the files in the cloud will not get one series of memory addresses; they will be random. Because of this, outsiders cannot follow memory addresses. Mostly a needed protocol, the user needs to prove himself to the group manager. The server shows the user's access level without forecasting additional information.

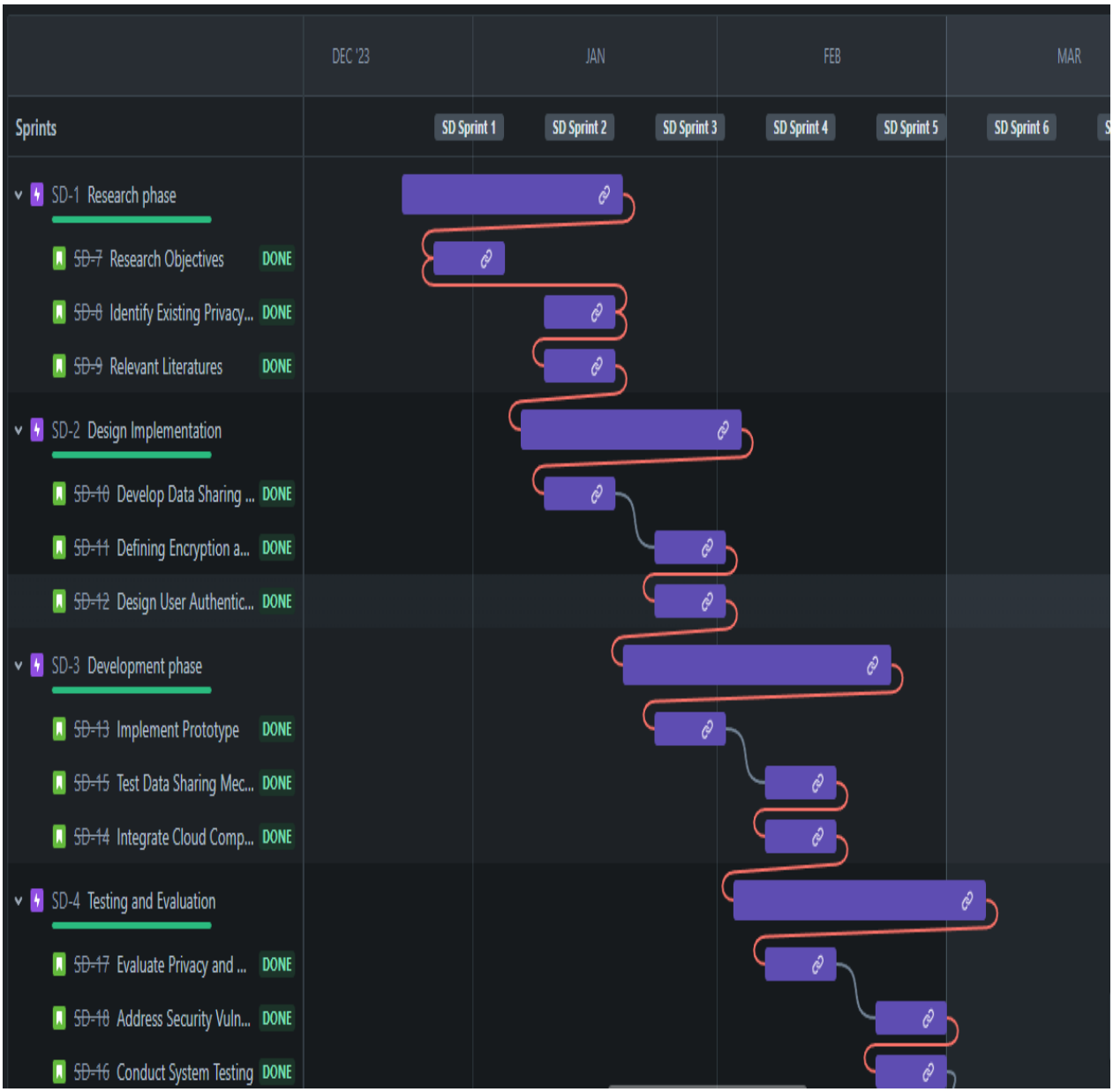

Fig.1.Gantt Chart

II. LITERATURE SURVEY

Secure and privacy-preserving data sharing in cloud environments has been the subject of extensive research. ABE and PRE were early cryptographic techniques that ensured fine-grained access control and anonymity for users. According to Yu et al., ABE methods were introduced. This system was computationally intensive despite being able to manage scalable access and maintain data confidentiality. Homomorphic encryption allows for secure computations on encrypted data, eliminating the need for users to decrypt sensitive information. However, in group settings, these methods face scalability and implementation challenges. The use of Oblivious RAM (ORAM) techniques has enabled the protection of data access patterns in recent years. Studies by Shi et al. Among ORAM's potential benefits is enhanced untraceability, though with increased communication costs. Zhang et al. also explored blockchain-based frameworks, which provide decentralized solutions to ensure immutability and transparency for group data sharing.

A. Analysis of Rsearch Works

S.No	Title	Authors	Techniques Used	Advantages	Year
1	Fast Proxy Re-encryption Scheme for Data Sharing in a Distributed File System	Ateniese et al. [11]	Bilinear mapping	Fast	2006
2	Attribute-Based Encryption with Efficient Revocation for Data Sharing in Cloud Computing	Yu et al. [12]	Attribute-based encryption (ABE)	Fine-grained access control, scalability	2010
3	Ciphertext Mult sharing for Secure Piracy-Preserving Multi-Authority Cloud Storage	Liang et al. [13]	Proxy re-encryption, anonymous techniques	User anonymity, data confidentiality	2010
4	Secure multi-hop Re-encryption with Continuous Hiding for Cloud Storage	Zhang et al. [14]	Secure multihop re-encryption	Secure against untrusted servers	2017
5	Hierarchical ORAM Scheme	Goldreich and Ostrovsky [17]	Hierarchical structure	Secure access patterns	1996
6	Secure Data Storage with Improved Wand Composite Hashing	Pinkas et al. [18]	Hierarchical ORAM, cuckoo hashing, random Hill sorting	Secure data storage	2010
7	Tree ORAM Scheme	Shi et al. [19]	Binary tree structure	Simple data retrieval	-
8	Path ORAM Scheme	Stefanov et al. [20]	Merkel Hash tree	Secure data integrity	2013
9	Binary Search Tree ORAM	Gentry et al. [21]	Binary search algorithm	Low bandwidth and storage overhead	2015
10	Recursive Matrix ORAM (RM-ORAM)	Gordon et al. [22]	Recursive matrix	Low memory overhead	2016

III. PROPOSED MODEL AND SYSTEM ARCHITECTURE

A. Proposed Model:

In cloud computing environments, the proposed model aims to create a framework that ensures security and privacy-preserving group data sharing. In this model, advanced cryptographic techniques such as AES256 encryption are used to secure confidential data and prevent unauthorized access. The model encrypts data with proxy re-encryption and uses obscure random-access memory (ORAM) to maintain privacy and untraceability. With ORAM, attackers cannot track user behaviour because data access patterns remain hidden. The model encrypts data with proxy re-encryption and uses obscure random-access memory (ORAM) to maintain privacy and untraceability. With ORAM, attackers cannot track user behaviour because data access patterns remain hidden.

B.System Architecture:

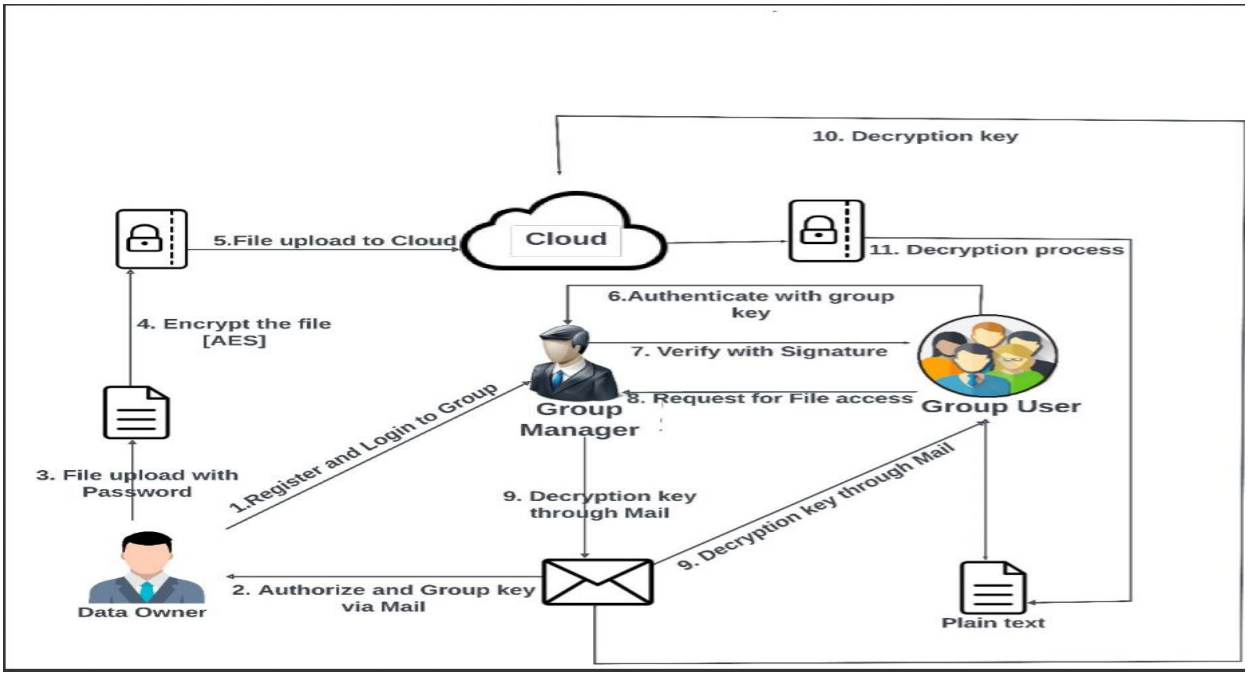

Fig.2.System Architecture

- Data sharing systems integrate multiple layers of security and efficiency. There are several key components, including:
- It is possible for users to upload encrypted files securely through the Data Owner Module.
- A cloud server ensures the availability and reliability of encrypted files.
- The Group User Module facilitates controlled access through the use of group keys and authentication processes.
- Controls access to files, approves files, and it help in the distributing of group keys.
- Group Manager: Oversees access control, file approvals, and group key distribution.

The architecture incorporates AES256 encryption, email-based key distribution, and ORAM for untraceable data access. A flowchart illustrating the data encryption and decryption process further explains the model's workflow, highlighting interactions between the data owner, group members, and the cloud system.

C. Proposed Architecture:

Data owner, cloud storage, and group manager are shown in a diagram of the architecture. Each component is crucial to ensuring secure data sharing and privacy protection.

IV. RESULTS AND DISCUSSION

A. Resultant:

During testing, the proposed model was found to effectively share data in the secure and privacy-preserving manner. By using this AES256, we were able to secure data and we can encrypt/decrypt it reliably. Authentication mechanisms and group key distribution operated smoothly, allowing only authorized users to access the system. In addition to maintaining high security standards, the system handled large volumes of uploads and requests efficiently.

Techniques like ORAM successfully masked access patterns, enhancing privacy. Even under simulated attack conditions, the model safeguarded data integrity and confidentiality. These tests confirmed the scalability and adaptability of the framework, making it suitable for various group data sharing scenarios in cloud environments.

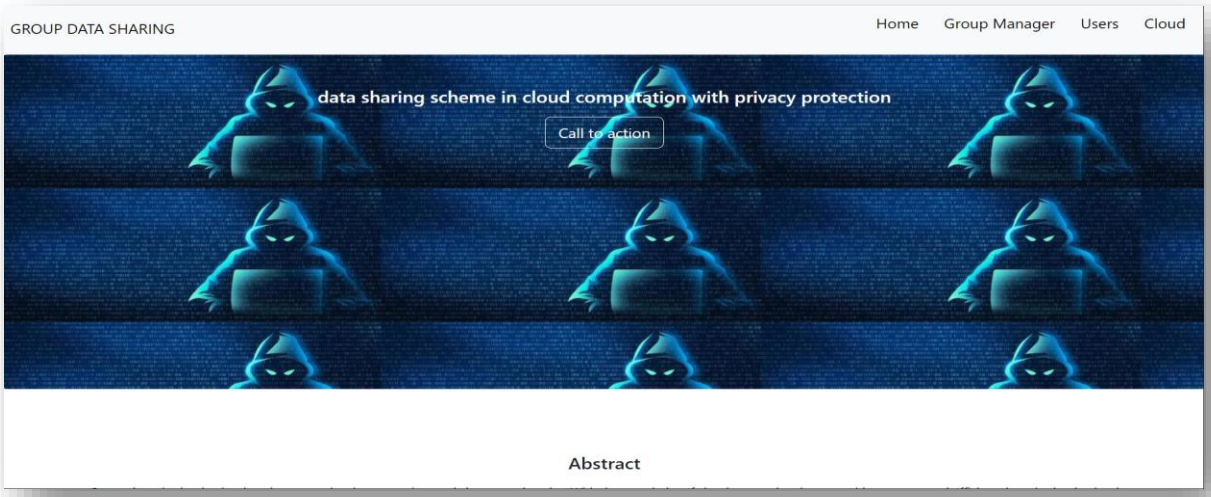

Fig.3.Homepage

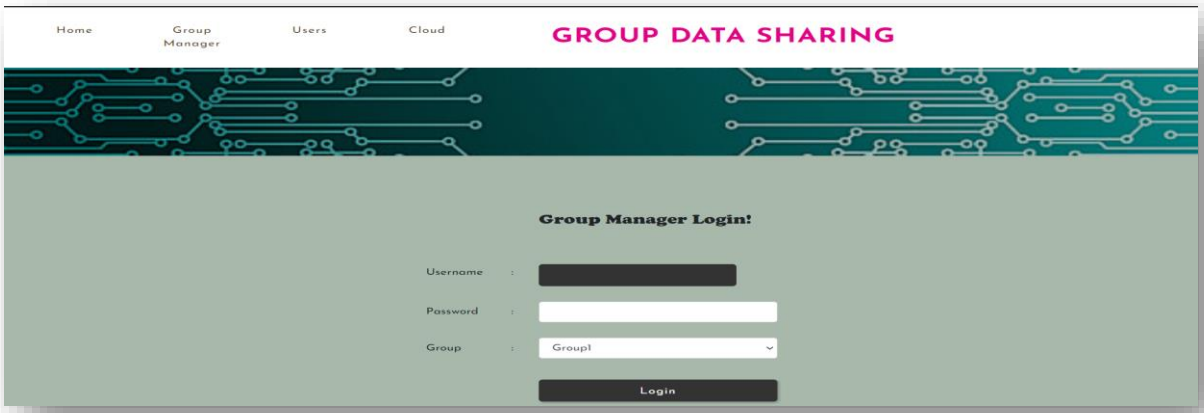

Fig.4. Group Manager

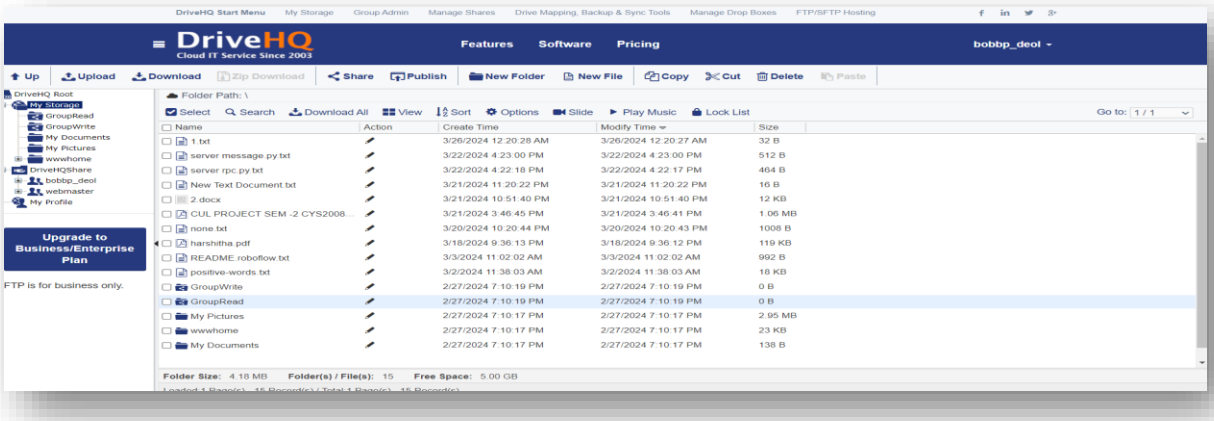

Fig. 5. Cloud sharing part

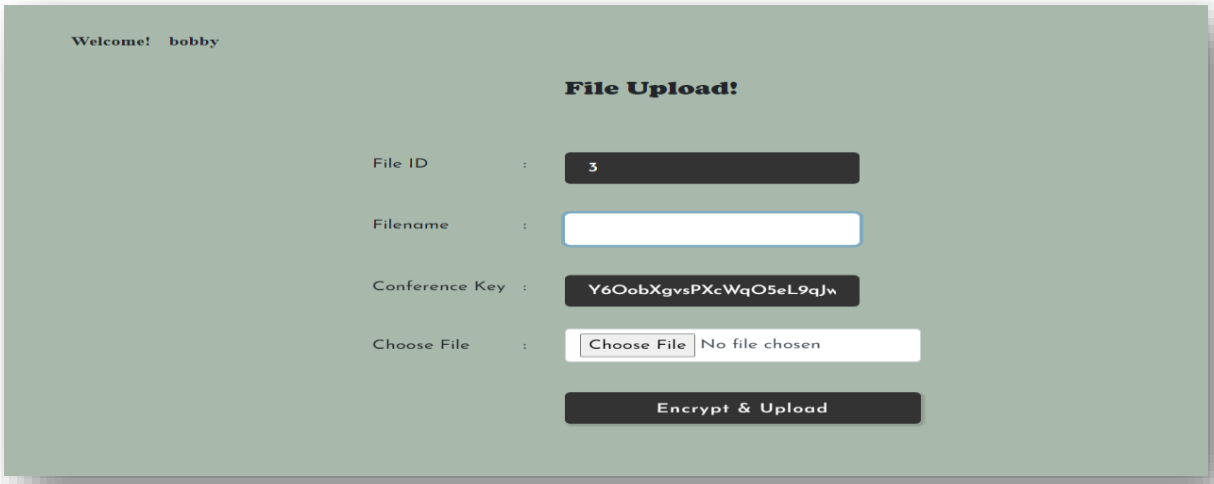

Fig.6. File Uploading with conference key.

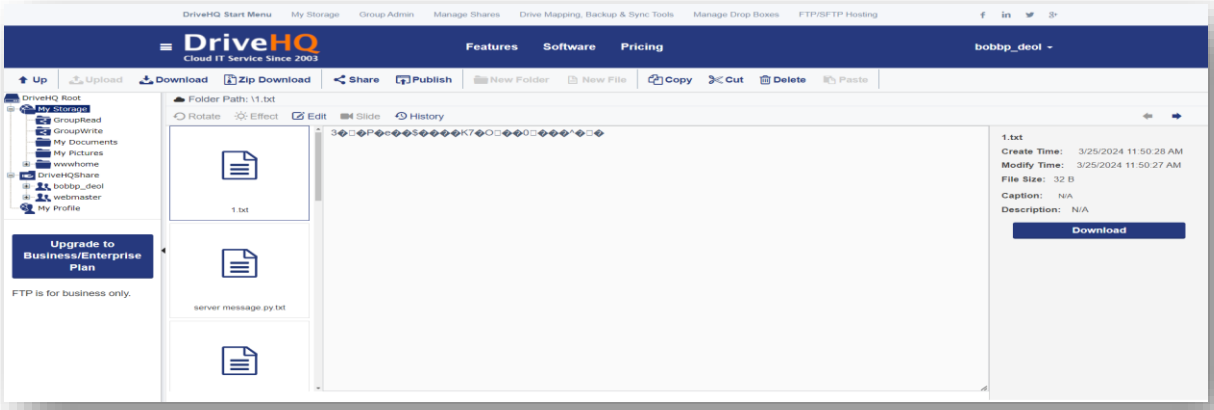

Fig. 7. Verified security attributes.

B. Analysis

The proposed framework demonstrated a clear reduction in computational overhead when compared to traditional methods. The AES256 encryption proved efficient, with negligible delays in encrypting and decrypting files. ORAM's inclusion helped in protecting data access patterns, although it introduced a minor increase in communication overhead, which stayed within manageable limits. By Safe guarding the data sharing the proxy re-encryption will be able to protect the data integrity and prevent the unauthorized changes in the data sharing.

During trials, users found the system easy to operate and reliable across various scenarios. While compared it to other models, it provides more security, resulting in excellent performance. Due to this, here the encryption methods increased storage requirements, but compression methods mitigated this. Despite its shortcomings, the system proved to be a practical and robust technique for sharing data in cloud environments. There is still room for improvement in the future.

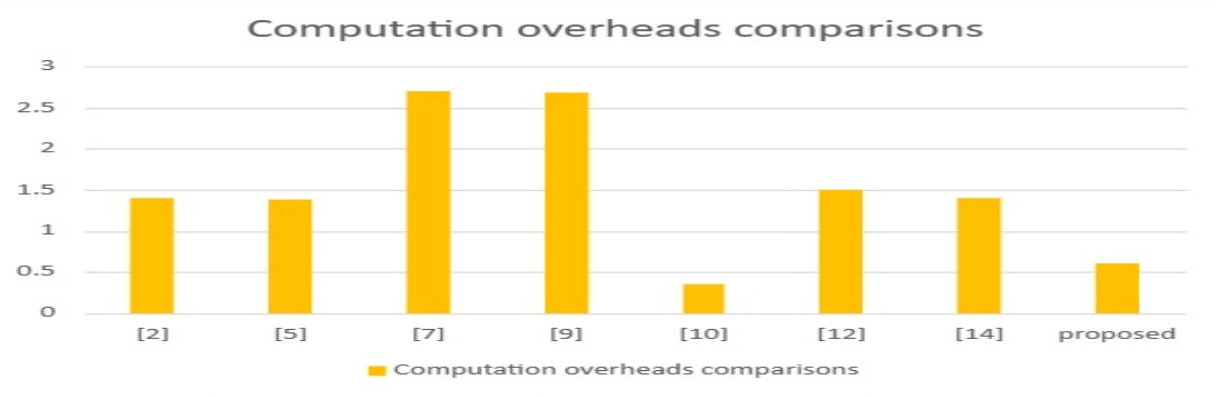

Table 1: Computation overhead comparisons

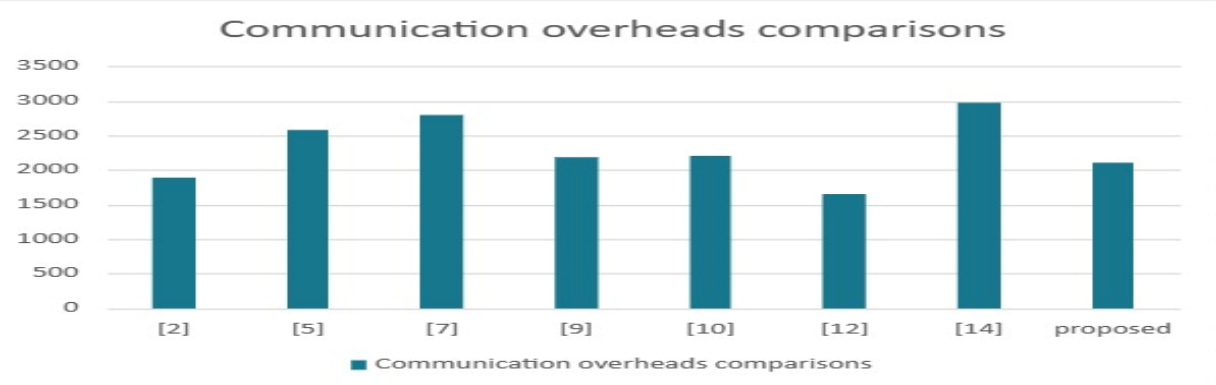

Table 2: Communication overhead comparisons

Encryption algorithm	Key length	Number of data division
RC4	104	2
AES	128	3
AES	192	4
AES	256	5
Blowfish	448	6

Table 3: shows the output sizes of data

Galois Field	m	k	Times of exhaustion
$GF(2^4)$	1	6	256^3
$GF(2^4)$	2	6	256^6
$GF(2^8)$	1	6	256^6
$GF(2^8)$	2	6	256^{12}
$GF(2^{16})$	1	6	256^{12}
$GF(2^{16})$	2	6	256^{14}

Table 4: Derivations of Message Size.

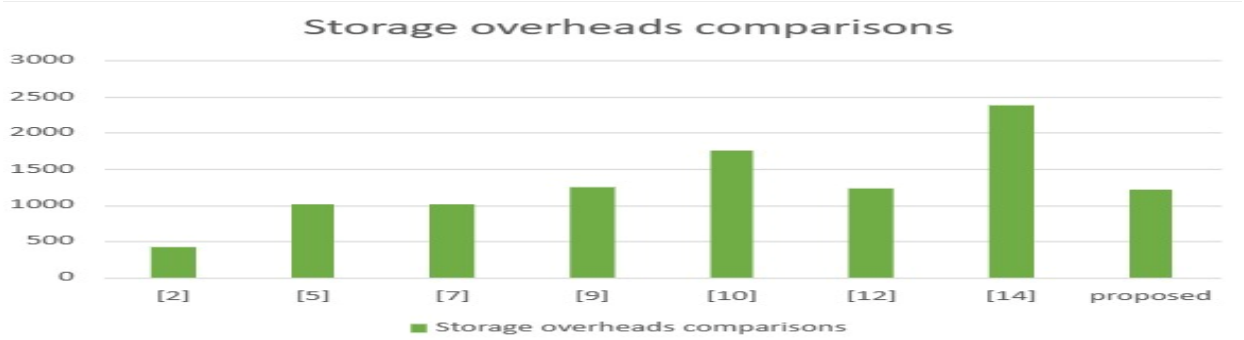

Table 5: Storage overhead comparisons

V. CONCLUSION

The proposed framework had addressed all the challenges that are faced in group data sharing on the cloud. AES256 is an encryption which protects the data against unauthorized access, while ORAM here ensures all the privacy by concealing access patterns. Based on the results of the testing, it was confirmed that the framework is effective, scalable, and easy to use, which helps to improve performance. The system can handle a large amount of data without affecting performance in this case. The encryption demands the additional storage because of the compression techniques that mitigate because it uses very efficiently to get the best output. This solution stands out to this innovative approach is to secure cloud data sharing. Enhancements like AI-driven anomaly detection and computational optimizations can further improve its relevance in evolving technological scenarios.

REFERENCES

[1] D. Shin, K. Yun, J. Kim, P.V. Astillo, J.N. Kim, I. You, A security protocol for route optimization in DMM-based smart home IoT networks, IEEE Access 7 (2019) 142531–142550

[2] Z. Jiang, P. Dong, R. Wei, Q. Zhao, Y. Wang, D. Zhu, N. Audsley, PSpSys: a timepredictable mixed-criticality system architecture based on ARM TrustZone, J. Syst. Archit. 123 (2022), 102368.

[3] S. Kumari, X. Li, F. Wu, A.K. Das, K.K.R. Choo, J. Shen, Design of a provably secure biometrics-based multi-cloud-server authentication scheme, Fut. Gen. Comput. Syst. 68 (2017) 320–330.

[4] H. Far, M. Bayat, A.K. Das, M.I Fotouhi, S. Pournaghi, M. Doostari, LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT, Proc. 8th Int. Conf. Transparent Opt. Networks, 5th Eur. Symp. Photonic Cryst., 5th Workshop All-Opt. Routing, 3rd Global Opt.

[5] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, Y. Park, A secure and lightweight authentication protocol for IoT-based smart Homes, Sensors 21 (4) (1488) 2021.

[6] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, Novel chaotic mapbased privacy-preserving authenticated key agreement scheme without the electricity service provider involvement, Secur. Privacy 2 (5) (2019) e74.

[7] A.A. Khan, V. Kumar, M. Ahmad, S. Rana, LAKAF: Lightweight authentication and key agreement framework for smart grid network, J. Syst. Archit. 116 (2021), 102053.

[8] J. Lansky, A.M. Rahmani, S. Ali, N. Bagheri, M. Safkhani, O. Hassan Ahmed, and M.Hosseinzadeh, "BCmECC: a lightweight blockchain based authentication and key agreement protocol for Internet of Things," Mathematics, 9(24), 3241, 201.

[9] S. Debroy, P. Calyam, M. Nguyen, R.L. Neupane, B. Mukherjee, A.K. Eeralla, K. Salah, Frequency-minimal utility-maximal moving target defense against DDoS in SDN-based systems, IEEE Trans. Netw. Serv. Manage. 17 (2) (2020) 890–903.

[10] J. Patman, D. Chemodanov, P. Calyam, K. Palaniappan, C. Sterle, M. Boccia, Predictive cyber foraging for visual cloud computing in large scale IoT systems, IEEE Trans. Netw. Serv.

Manage. 17 (4) (2020) 2380–2395.

[11] H. Far, M. Bayat, A.K. Das, M.I Fotouhi, S. Pournaghi, M. Doostari, LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT, Proc. 8th Int. Conf. Transparent Opt. Networks, 5th Eur. Symp. Photonic Cryst., 5th Workshop All-Opt. Routing, 3rd Global Opt. Wireless Networking Semin., 2nd COST 270 Workshop Reliab. Issues Next Gener. Opt. Networks, 2nd Photonic Integr. Compon. Appl. Workshop 27 (2021) 1389–1412

[12] M. Tao, J. Zuo, Z. Liu, A. Castiglione, F. Palmieri, Multi-layer cloud architecturalmodel and ontology-based security service framework for IoT-based smart homes, Fut. Gener. Comput. Syst. 78 (2018) 1040–1051.

[13] V.O. Nyangaresi, provably secure protocol for 5G HetNets, in: 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), IEEE, 2021, pp. 17–22.

[14] J. Li, W. Zhang, S. Kumari, K.K.R. Choo, D. Hogrefe, Security analysis and improvement of a mutual authentication and key agreement solution for wireless sensor networks using chaotic maps, Trans. Emerg. Telecommun. Technol. 29 (6) (2018) e3295.

[15] S. Debroy, P. Calyam, M. Nguyen, R.L. Neupane, B. Mukherjee, A.K. Eeralla, K. Salah, Frequency-minimal utility-maximal moving target defense against DDoS in SDN-based systems, IEEE Trans. Netw. Serv. Manage. 17 (2) (2020) 890–903.

[16] A.A. Khan, V. Kumar, M. Ahmad, S. Rana, LAKAF: Lightweight authentication and key agreement framework for smart grid network, J. Syst. Archit. 116 (2021), 102053.

[17] M. Wazid, A.K. Das, V. Odelu, N. Kumar, W. Susilo, Secure remote user authenticated key establishment protocol for smart home environment, IEEE Trans. Dependable Secure Comput. 17 (2) (2020) 391–405