IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203025

Secure Group Key Management Protocol on Cloud Storage over Unreliable Channels

Shaik Samreen, Thatigiri Mahindra, Vuduthala Harish, S Sivasankar Rao

UG Students, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

Associate Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

ABSTRACT: The project focuses on developing a secure data management system that utilizes QR codes, encryption, and role-based access to ensure the confidentiality and integrity of sensitive information. The system involves several key participants: the Manager, File Owner, Group Members, Trusted Authority, and Cloud Service Provider (CSP). The workflow begins with the Manager generating a QR code, which contains a password for secure access. The Manager is responsible for managing the login process and granting necessary permissions to the File Owner and Group Members. Once the Manager has authorized the File Owner, the File Owner can upload data into the system. This data is automatically encrypted to ensure its security and prevent unauthorized access. The Group Members, who have been granted permission, can view the data. However, to decrypt and access the data, they must possess a private key. The private key, which is essential for decryption, is securely shared by a Trusted Authority, ensuring that only trusted individuals can access the data. The Cloud Service Provider (CSP) plays a crucial role in storing all the data and its associated information. The CSP ensures that the data remains secure, but it does not have direct access to the encrypted contents. The decryption process, managed through private keys, is strictly handled by authorized users, maintaining the confidentiality and integrity of the data. This system combines QR code-based access, encryption techniques, and secure key sharing mechanisms to provide a robust solution for managing sensitive data. It ensures that only authorized individuals can view the data, and the centralized role of the Trusted Authority guarantees that private keys are distributed securely. The CSP ensures reliable and secure storage of data, making the system ideal for environments where data security, confidentiality, and controlled access.

KEYWORDS: Cloud storage, group key, _le sharing, key distribution.

I. INTRODUCTION

Given the cutting-edge explosion of cloud technology nowadays, cloud-based reconstruction services have grown in popularity. Data from many customers that can be housed on distinct virtual machines may live on a same physical system in a shared-tenancy cloud computing environment [1]. Data owners are left exposed and must rely entirely on the cloud provider to secure their data under this paradigm, which gives the cloud provider complete authority over data management and storage. According to recent reports, Google gave the FBI access to all of a user's papers after obtaining a search order; nevertheless, the individual was unaware of the search until they were taken into custody. Because cloud provider has the full access to the data, the privacy of data could be violated if user's data is intercepted or modified by the cloud provider.

In theory, key management for file sharing may be accomplished by group key management and access control. But certain special characteristics of cloud storage present fresh issues that haven't been thoroughly thought through. First of all, shared files are sent across the network, and different network monitoring tools have the ability to intercept them. This issue cannot be completely resolved by only implementing access control for cloud storage. Second, group key management relies on the encryption key being managed by the cloud provider. This can stop the network from intercepting the shared files, but the cloud provider can still intercept the shared files. In this paper, we proposed a secure group key management protocol on cloud storage over unreliable channels, aiming at protecting the shared files on the cloud storage. Mixed encrypiton technology is used to generate and distribute group keys, which resistance attacks from network monitor. In addition, we propose a verified protocol that against the attacks from the fille sharers or the cloud provider.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203025

II. LITERATURE SURVEY

The security of file sharing in cloud environments heavily depends on the underlying key management mechanisms, particularly in scenarios involving dynamic user groups. This section surveys existing research efforts on Group Key Management Protocols (GKMPs) with a focus on their application in cloud storage systems.

Traditional Group Key Management Techniques

a. Logical Key Hierarchy (LKH): Proposed by Wallner et al. (1999), LKH is a tree-based structure that reduces rekeying overhead during group membership changes. It is efficient in terms of key updates but incurs storage and communication costs proportional to the logarithm of the group size. While suitable for multicast communications, adapting LKH to cloud environments requires secure channels and does not address access control at the file level.

One-Way Function Trees (OFT): OFT was introduced to improve upon LKH by using one-way hash functions to derive keys, significantly reducing the computational overhead. This method ensures forward and backward secrecy but still depends on a central key distribution authority. Its reliance on tree structures makes it vulnerable to scalability issues in highly dynamic cloud storage groups.

Identity-Based and Attribute-Based Encryption (IBE/ABE)

a. Identity-Based Encryption (IBE): IBE schemes, such as Boneh-Franklin (2001), allow user identities to act as public keys, simplifying key management. However, they suffer from scalability and key escrow issues, making them less suitable for large, decentralized groups.

b. Attribute-Based Encryption (ABE): ABE, especially Ciphertext-Policy ABE (CP-ABE), allows access control based on user attributes. It provides fine-grained access and is ideal for complex access structures. However, it is computationally intensive and poses challenges in dynamic environments due to re-encryption requirements during user revocation.

Group Key Agreement Protocols: Protocols such as Burmester and Desmedt (1994) enable members to collaboratively establish a group key without a central authority. These are well-suited for peer-to-peer environments but are complex to implement in cloud architectures where a central server (like a Group Manager) is standard.

Cloud-Specific Solutions

a. Yu et al. (2010): They proposed a scalable and fine-grained access control scheme using ABE for cloud storage. The scheme supports dynamic data sharing and efficient user revocation via proxy re-encryption. However, it introduces high computational costs for encryption and decryption.

b. Wang et al. (2012): Introduced a secure sharing mechanism using proxy re-encryption and lazy revocation, which helps reduce the overhead during user revocation but assumes semi-trusted proxies.

Blockchain-Integrated Key Management: Recent work has investigated the use of blockchain to decentralize key management and provide immutable audit trails. While promising, such systems face performance and complexity issues and are still in early stages of adoption.

S.No	Author(s) & Year	Title	Technique/Protocol	Key Features	Limitations
1	Wong et al., 2000	Secure Group Communications Using Key Graphs	Key Graphs (LKH, OFT)	Efficient rekeying; hierarchical structure	Rekeying overhead on membership changes
2	Sherman et al., 2004	Key Management for Encrypted File Storage in Distributed Systems	Tree-Based Key Management	Reduces storage and communication cost	Requires trusted central authority
3	Sahai & Waters, 2005	Fuzzy Identity-Based Encryption	IBE	Supports flexible identity matching and key derivation	Performance overhead; not suitable for large groups
4	Yu et al.,	Secure, Scalable, and	CP-ABE (Ciphertext-	Fine-grained access	Complex key

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203025

	2010	Fine-Grained Data Access Control in Cloud	Policy ABE)	control; attribute-based sharing	management; high computation
5	Dutta et al., 2014	A Secure and Efficient Group Key Management Protocol	Hybrid Key Tree with Hash Chains	Efficient rekeying; forward/backward secrecy	Not fully decentralized; single point of failure
6	Chen & Li, 2015	Decentralized Group Key Management for Cloud Storage	Distributed Key Agreement Protocol	Removes central authority; supports peer-to-peer sharing	Complex coordination among members
7	Ruj et al., 2016	Key Management for Secure Cloud Storage: A Survey	Survey Paper	Comprehensive review of GKMPs for cloud systems	No novel protocol proposed
8	Akl & Taylor, 2017	Cryptographic Solution for Dynamic Group Communication	Akl-Taylor Key Distribution Scheme	Scalability; supports user revocation	Not efficient for very large groups
9	Ali et al., 2019	Efficient Group Key Management Scheme in Cloud Environment	Binary Tree-based Key Update Mechanism	Reduces rekeying and storage overhead	Vulnerable if tree structure is compromised
10	Zhang et al., 2021	Lightweight Group Key Management for Cloud IoT Systems	Hash-Based Key Distribution Protocol	Low computation and storage; IoT compatibility	Less robust against advanced attacks

Table 1. Literature survey works.

III. RELATED WORKS

Research on storage system security has always been ongoing. Numerous real systems exist, including NASD [10] and CFS [9]. CFS uses user-supplied passwords for data encryption and is designed for single-user workstations. A distributed system with intelligent disks and user-supplied keys as authentication proofs is what NASD suggests. Techniques like NASD and SNAD are primarily concerned with protecting network traffic and thwarting external threats. In cloud computing, Rao suggested a secure method for exchanging personal health information that relies on ciphertext-policy-attributed-based (CP-ABE) signcryption. It focus on restricting unauthorized users on access to the confidential data. Liu et al. [4] proposed an access control policy based on CP-ABE for personal records in cloud computing as well. only one fully trusted central authority in the system is responsible for key management and key generation.

Several group key management techniques have been proposed, including:

Logical Key Hierarchy (LKH): Efficient but incurs rekeying overhead during membership changes.
One-Way Function Trees (OFT): Reduces computation but increases complexity in key derivation.
Identity-Based Encryption (IBE): Simplifies key management but faces scalability issues.
Attribute-Based Encryption (ABE): Provides fine-grained access control but is computationally intensive.

These approaches either lack efficiency, scalability, or fail to maintain desired security properties when applied to cloud environments. Pervez et al. [2] conducted the most current study addressing privacy concerns in cloud-based storage, proposing a privacy-aware data sharing mechanism called SAPDS. Without depending on any reliable third party, it combines attribute-based encryption with proxy re-encryption and secret key update capabilities. However, the attribute encryption scheme determines SAPDS's storage and communication cost. Groups of users and any individual who has access authorization to the shared files are granted the same data access permission by the aforementioned systems. Usually, these group permissions are employed to safeguard the data encryption keys. Our general goal is to develop an efficient group key management protocol for fille sharing on cloud storage, the resulting techniques should be able to confront two main problems. One is ensuring that the content of the shared files cannot be learned by the unauthorized peoples. The other is protecting the files against misoperation by the cloud provider and interception by the network. We can observe that how to securely share data files in a multiple-owner manner for groups while preserving identity privacy from a distrust cloud remains to be a challenging issue.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203025

IV. PROPOSED WORK

A group key distribution protocol that enables a group manager to securely distribute a shared secret key to group members.

A centralized group key management protocol that uses a cloud-based server to manage and distribute group keys. A group key management and sharing protocol that uses a cloud-based server to manage and distribute group keys, and enables secure group communication. Decentralized Group Key Management (DGKM) is a group key management approach where group members collectively manage the group key without a central authority. DGKM requires each group member to be involved in key management, which can lead to increased complexity and overhead. As the group size increases, DGKM can become impractical due to the need for each member to communicate with every other member. The absence of a central authority can make it difficult to resolve disputes or make decisions about key management. DGKM approaches often lack standardization, which can make it difficult to ensure interoperability between different systems.

In Group key management and sharing protocols play a critical role in maintaining the data security by enabling efficient and secure key distribution among group members. Cloud computing is a model wherein resources on the Internet establish a resource pool and may be dynamically assigned to diverse applications as well as services. Ensuring security in cloud storage is not easy. As data on cloud is beyond the control area of authentic participants, shared data should be made usable on demand of authentic users. The QR code generator algorithm is a process that creates a QR code from a given set of data. Here is a brief overview of the steps involved:

Data Encoding: Convert data into a binary format.
Error Correction: Add error correction codes to ensure data recovery.
Data Matrix Creation: Arrange encoded data and error correction codes into a square grid.
Masking: Apply rules to improve readability and symmetry.
Format Information: Add error correction level and mask pattern information.
Version Information: Add QR code size and encoding scheme information.
Finalization: Add zeros to the end of the data matrix.

A hash key algorithm is a one-way function that takes input data of any size and returns a fixed-size string of characters, known as a hash value. AES 256 bit was used for a Asymmetric algorithm

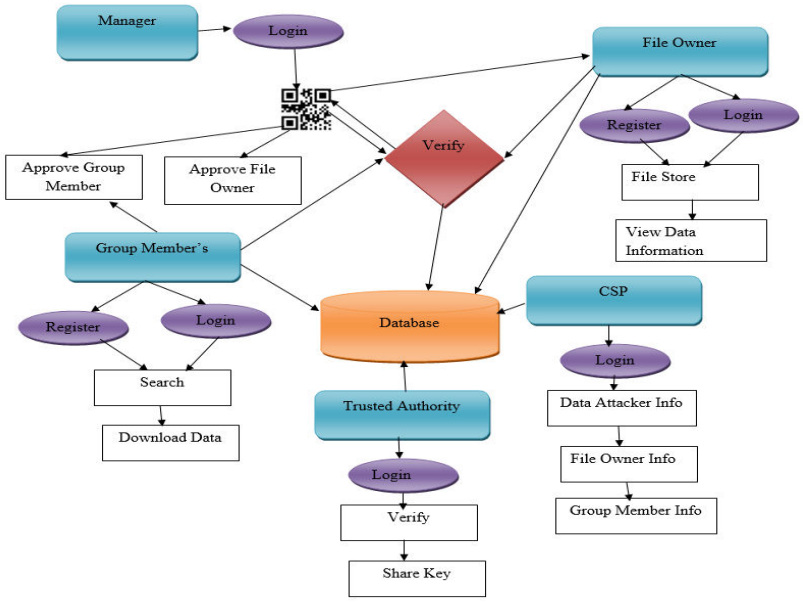

Figure 2. System model.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203025

Our overarching objective is to create an effective group key management protocol for cloud storage file sharing; the resultant methods need to address two primary issues. One is making sure that unauthorized individuals cannot learn the shared materials' content. The other is safeguarding the data against network eavesdropping and cloud provider errors. A sharing group is made up of users who wish to exchange files, and the cloud provider is in charge of each sharing group. Each member of the sharing group has a pair of keys that they use to process messages. The cloud provider controls the public key, but only the sharers are aware of the private key.

Whenever a sharer wants to share his file within the group, it should generate a group key and encrypt the file with the group key before transmitting the file to the cloud. Then he uses a key distribution scheme to distribute the group key to the other group sharers without the participation of the cloud provider. Recovering the group key needs the collaboration of all the group members.

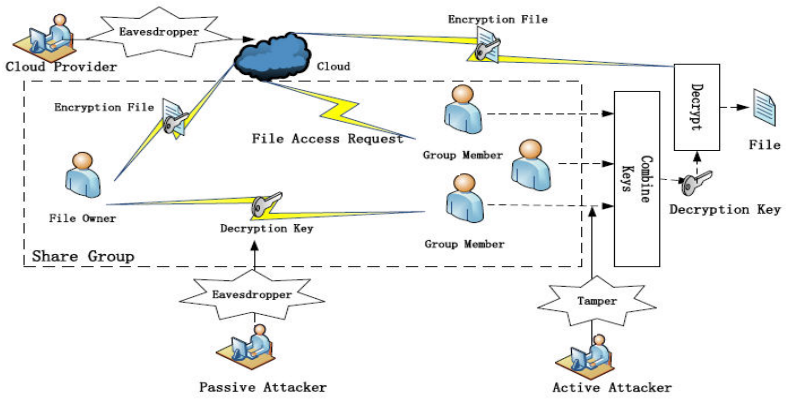

Figure 2. Sharing model of GKMP.

Our protocol might be threatened by three different types of adversaries. The first is the cloud provider or passive adversary, which only collects data without influencing the group members' communication behavior. The second is the potential positive enemy who, as a le sharer, might change the produced data. The last type of adversary is adaptive, which has the capacity to get and modify the output information of one or more group sharers. Our objective is for our protocol to be terminated as soon as a passive or positive opponent is identified, and for the adaptive adversary to beat our protocol, n is the number of group members that must be compromised.

	LKH	SAPDS	GKMP
Access Control	own	own	own
Key Distribution Channel	Security	Security	Public
Encryption File	no	yse	yes
Group member Management	yes	yes	no
Defend Passive Attacker	yes	yes	yes
Defend Cloud Provider	no	yes	yes
Defend Active Attacker	no	no	yes

Table 2. Security comparison.

The comparison between LKH, SAPDS, and GKMP was summed up in Table 3. The functions of key managers are one of the main distinctions between GKMP, SAPDS, and LKH. The cloud provider serves as the key manager in the group key method, while in GKMP and SAPDS, the group members choose the group key and share it without the cloud provider's involvement. Furthermore, a safety transmission channel is required in group key approaches and SAPDS to prevent attackers from stealing the master key. In GKMP, the group key is distributed solely by public transmission after being encrypted using the public keys of each group member.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203025

Group Members	10	20	30	40	50	60	70	80	90	100
GKMP($\times Lbits$)	10	20	30	40	50	60	70	80	90	100
SAPDS($\times Lbits$)	17	20	40	50	61	72	82	93	102	113
Percent(%)	41.1	31.1	25	20	18	16.6	14.6	13.9	11.7	11.5

Table 3. Computing complexity.

The degree of shared security between these three approaches is another significant difference. The security of the items became more crucial because they are kept in an open atmosphere. The master key at LKH is just used to manage access, and the files are kept on the cloud in an unencrypted format. In SAPDS and GKMP, shared files are also encrypted using the group key. The shared files are now safer than previously as the cloud provider only controls the participants' public keys and encrypted shared files. It goes without saying that GKMP and SAPDS are better suited for cloud storage. However, SAPDS believed that group members acted honorably,

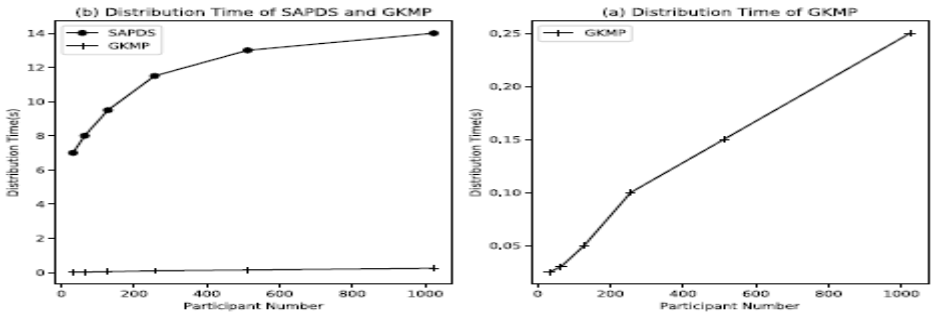

Figure 4. Computation overhead with different participant number of SAPDS and GKMP.

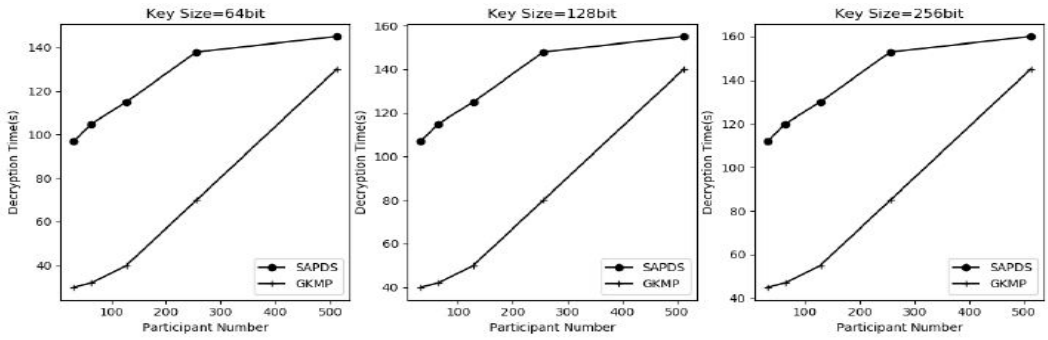

Figure 5. Computation overhead with different encryption key of SAPDS and GKMP.

The data indicates that it would take SAPDS a maximum of 14.3 seconds to process the encryption key with five distinct group members. Nevertheless, GKMP only takes 191 ms at most, and its computational cost is not significantly impacted by the size of the decryption keys. When encrypted using the same size of encryption key, SAPDS and GKMP show varying decryption times for secret key K sizes. As seen in Fig. 9, SAPDS often takes a little longer than GKMP. Additionally, GKMP exhibits a linear decryption overhead as the group size grows.

V. CONCLUSION

In this work, we provide a brand-new group key management protocol for cloud storage file sharing. GKMP uses public keys to ensure that the group key is distributed equitably and to fend against attacks from compromised cars or cloud providers. We provide a thorough examination of potential security flaws and their related countermeasures, proving that GKMP is safe even when assumptions are weakened. Additionally, we show that the protocol has lower processing and storage complexity. This paper introduces a secure and efficient Group Key Management Protocol for file sharing on cloud storage. The protocol ensures data confidentiality and secure key distribution while supporting dynamic group membership. Future work includes integrating blockchain for auditability and decentralized key control.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203025

REFERENCES

[1] P.-W. Chi and C.-L. Lei, ``Audit free cloud storage via deniable attribute based encryption," IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 414-427, Apr. 2018.
[2] Ravindra Changala,"Proactive Market Crash Prediction: Investigating GNN-LSTM Networks for Early Detection in Stock Markets", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10726065, November 2024, IEEE Xplore
[3] J. Zhou, H. Duan, K. Liang, Q. Yan, F. Chen, F. R. Yu, J.Wu, and J. Chen, ``Securing outsourced data in the multi authority cloud with grained access control and efficient attribute revocation," Comput. J., vol. 60, no. 8, pp. 1210-1222, Aug. 2017.
[4] Ravindra Changala, "Implementing Cross-Lingual Information Retrieval Systems to Enhance Resource Accessibility in English Language Learning", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10725465, IEEE Xplore
[5] Ravindra Changala, "Integration of Adaptive Neuro-Fuzzy Systems in Mobile Commerce Strategy: Enhancing Customer Relationship Management through Personalized Recommendations",2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10725950, IEEE Xplore.
[6] J. Wu, Y. Li, T. Wang, and Y. Ding, ``CPDA: A confidentiality-preserving deduplication cloud storage with public cloud auditing," IEEE Access, vol. 7, pp. 160482-160497, 2019.
[7] Ravindra Changala, "Optimization of BERT Algorithms for Deep Contextual Analysis and Automation in Legal Document Processing", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10723962, IEEE Xplore
[8] H. Xiong and J. Sun, ``Comments on veriable and exculpable outsourced attribute based encryption for access control in cloud computing," IEEE Trans. Depend. Sec. Comput., vol. 14, no. 4, pp. 461-462, Jul. 2017.
[9] Ravindra Changala, "Real-Time Multilingual Communication Enhancement Using Transformer Model for Social Media Platform", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10725522, IEEE Xplore
[10] Ravindra Changala, "Swarm Intelligence for Multi-Robot Coordination in Agricultural Automation", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.
[11] J. Shao, R. Lu, and X. Lin, ``Fine-grained data sharing in cloud computing for mobile devices," in Proc. IEEE Conf. Comput. Commun.(INFOCOM),Apr. 2015, pp. 2677-2685.
[12] Ravindra Changala, "Advanced Integration of Graph Neural Networks for Collaborative Interfaces in Immersive Virtual Reality Environments", 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), ISBN:979-8-3503-7024-9, DOI: 10.1109/ICCCNT61001.2024.10724828, IEEE Xplore
[13] R. Ahuja, S. K. Mohanty, and K. Sakurai, ``A scalable attribute-set-based access control with both sharing and full-edged delegation of access privileges in cloud computing," Comput. Elect. Eng., vol. 57, pp. 241-256, Jan. 2017.
[14] Ravindra Changala, "Sustainable Manufacturing through Predictive Maintenance: A Hybrid Jaya Algorithm and Sea Lion Optimization and RNN Model for Industry 4.0", 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.
[15] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. P. C. Rodrigues, ``Provably secure fine grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," IEEE Trans. Ind. Informat., vol. 15, no. 1, pp. 457-468, Jan. 2019.
[16] Ravindra Changala, "Enhancing Robotic Surgery Precision and Safety Using a Hybrid Autoencoder and Deep Belief Network Approach: Real-Time Feedback and Adaptive Control from Image Data",2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.
[17] Z. Fu, X. Sun, S. Ji, and G. Xie, ``Towards efficient content-aware search over encrypted outsourced data in cloud," in Proc. IEEE 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM), Apr. 2016, pp. 1-9.
[18] Ravindra Changala, "Next-Gen Human-Computer Interaction: A Hybrid LSTM-CNN Model for Superior Adaptive User Experience", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718496, October 2024, IEEE Xplore.
[19] Ravindra Changala, "Enhancing Early Heart Disease Prediction through Optimized CNN-GRU Algorithms: Advanced Techniques and Applications", 2024 Third International Conference on Electrical, Electronics, Information

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203025

and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718395, October 2024, IEEE Xplore

[20] Ravindra Changala, "Sentiment Analysis in Mobile Language Learning Apps Utilizing LSTM-GRU for Enhanced User Engagement and Personalized Feedback", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718406, October 2024, IEEE Xplore.

[21] M. Blaze, ``Acryptographic file system for UNIX," in Proc. 1st ACMConf.Comput. Commun. Secur. (CCS), 1993, pp. 91.

[22] Ravindra Changala, "Image Classification Using Optimized Convolution Neural Network", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.

[23] Ravindra Changala, "Sentiment Analysis Optimization Using Hybrid Machine Learning Techniques", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore

[24] Ravindra Changala, "Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore

[25] Ravindra Changala, "Advancing Surveillance Systems: Leveraging Sparse Auto Encoder for Enhanced Anomaly Detection in Image Data Security", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com