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.2025.1203010

Secured Data Sharing in Cloud Environment Using Proxy Re-Encryption Techniques

Salla Hindhuja, Rasala Rakesh Yadav, Sama Sreya Reddy, P Sunil

UG Students, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India[1,2,3]

Assistant Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India[4]

ABSTRACT: This project implements a Proxy Re-Encryption (PRE) system for secure data sharing and management in a cloud-based environment. The core objective is to enable a cloud owner to securely upload data, divide it into multiple parts, and allow a data user to access and modify this data while maintaining confidentiality and integrity. Initially, the cloud owner uploads a file, which is split into four segments. Each segment undergoes a hashing process using the SHA algorithm, generating four distinct SHA hash values, which serve as integrity verifiers for the respective parts of the data. To protect data during the sharing process, the owner encrypts the data before granting access to a specific data user. The encrypted file is then subjected to proxy re-encryption, where a proxy server, without learning anything about the contents of the file, re-encrypts it on behalf of the owner. This allows the data user to decrypt the file securely with the provided key. The cloud server manages this process by performing the re-encryption and sharing the encrypted file and key with the user. In this system, only authorized users with the necessary permissions, granted by the cloud owner, can access the file content. The use of proxy re-encryption ensures that the cloud server does not need to have direct access to the unencrypted data, preserving data privacy and security. This project enhances secure data sharing and access in cloud environments, offering a high level of data confidentiality, integrity, and control for the owner while enabling safe and selective access for users.

KEYWORDS: Proxy Re-Encryption, Cloud Security, Data Sharing, Attribute-Based Encryption, Access Control, Key Management.

I.INTRODUCTION

Cloud computing offers scalable and cost-effective solutions for data storage and sharing. However, ensuring data confidentiality and controlled access remains a critical challenge. Proxy Re-Encryption (PRE) provides a promising approach for secure data sharing, enabling a semi-trusted proxy to transform ciphertexts from one user to another without revealing the underlying plaintext. In this paper, we propose a novel proxy re-encryption scheme tailored for cloud environments, which integrates fine-grained access control, dynamic policy updating, and support for attribute-based re-encryption. Our scheme enhances security, ensures efficient key management, and reduces computational overhead, making it suitable for real-world cloud-based applications. We provide formal security analysis and experimental evaluations demonstrating the effectiveness and efficiency of our approach.

The proliferation of cloud computing has revolutionized the way individuals and organizations store and share data. Despite its benefits, cloud environments introduce significant privacy and security concerns, especially when handling sensitive information. Traditional encryption methods ensure data confidentiality but complicate sharing, as decryption requires direct access to the original private key. Proxy Re-Encryption (PRE) has emerged as an effective solution that allows a semi-trusted proxy to convert ciphertexts intended for one party into ciphertexts for another without learning anything about the plaintext. However, existing PRE schemes often suffer from scalability issues, lack of fine-grained access control, and inefficiencies in dynamic policy updates.

This paper introduces a **novel proxy re-encryption technique** that addresses these limitations by integrating attribute-based encryption (ABE), role-based access control (RBAC), and efficient key delegation mechanisms. Our proposed technique enables secure, flexible, and scalable data sharing in cloud environments.

In the digital world, online data sharing and storage has grown in popularity. It is the basis for consumer apps like Microsoft SkyDrive, Dropbox, Google Drive, Amazon Web Services, and OneDrive. Furthermore, more and more

| 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.2025.1203010

personal record management systems are using cloud platforms to collect, store, and share data [11]. Personal health record (PHR) services are provided by cloud service providers like Microsoft HealthVault, which improves the effectiveness of medical data storage and inter-institution sharing. Despite its widespread use and ease of use, cloud computing brings up a number of data security concerns, such as confidentiality and integrity, which continue to be top of mind for customers. Encrypting user data before transmitting it to the cloud is standard procedure.

II.RELATED WORK

Several PRE schemes have been developed over the past decade:

- **Traditional PRE**: Basic schemes like those proposed by Blaze et al. (1998) enable re-encryption with a simple delegation model but lack access control.
- **Identity-Based PRE**: Green and Ateniese (2007) introduced identity-based PRE, which simplifies key management but struggles with scalability in large systems.
- **Attribute-Based PRE**: Later research, including Yu et al. (2010), integrated ABE with PRE to support fine-grained policies, yet many such schemes are computationally heavy.
- **Blockchain-Aided PRE**: Recent advances incorporate blockchain for auditability and trust, but they introduce latency and complexity.

While these approaches contribute valuable insights, none fully address the trifecta of **security**, **efficiency**, and **policy adaptability** in dynamic cloud environments.

Cloud storage should facilitate data sharing as more institutions, including government agencies and hospitals, exchange private and sensitive data on external servers. Secure data sharing depends more on user trust and reputation [15]; also, for a company to provide effective services, the user must receive the desired data or information promptly. This must be fixed in the suggested system so that customers can enjoy hassle-free services even in the event that the data owner is unavailable; data sharing ought to be carried out in an emergency. Trust calculated values must be supplied in order to allow users to share files or data while the data owner is not present.

III.LITERATURE SURVEY

The increasing reliance on cloud services for data storage and sharing has highlighted the need for robust data security mechanisms. Traditional encryption schemes safeguard data but often fall short when it comes to controlled data sharing and scalability. Proxy Re-Encryption (PRE) has emerged as a potent cryptographic primitive enabling secure delegation of decryption rights without exposing plaintext to intermediaries. This literature survey explores the evolution of PRE techniques and their applications in secure data sharing within cloud environments.

1. Traditional Proxy Re-Encryption (PRE)
Blaze et al. (1998) introduced the concept of atomic proxy cryptography, laying the foundation for PRE. Their model allows a proxy to transform ciphertexts encrypted under one key to another without revealing the underlying plaintext. However, it supports only limited delegation and lacks robust access control mechanisms, making it less suitable for dynamic cloud environments.

2. Identity-Based Proxy Re-Encryption (IB-PRE)
Green and Ateniese (2007) proposed identity-based PRE, where public keys are derived from user identities, simplifying key distribution and management. This approach enhances scalability but introduces trust assumptions on the private key generator (PKG) and lacks resistance to collusion attacks.

| 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.2025.1203010

3. Attribute-Based Proxy Re-Encryption (AB-PRE)

Yu et al. (2010) extended PRE to support Attribute-Based Encryption (ABE), allowing ciphertexts to be associated with access policies defined over user attributes. This fine-grained control supports complex access structures and dynamic delegation.

4. Homomorphic and Functional Proxy Re-Encryption

Ateniese et al. (2013) explored functional PRE, which allows ciphertext transformation not only for different recipients but also under different functions or transformations. This line of work paves the way for secure computations on encrypted data.

5. Blockchain-Integrated PRE for Auditability

Recent works, such as Zhang et al. (2019) and Chen et al. (2021), have introduced blockchain frameworks integrated with PRE to enhance data sharing transparency and traceability. These systems store re-encryption and access logs on distributed.

6. Revocable and Dynamic PRE Schemes
Li et al. (2018) proposed revocable PRE, where access can be dynamically granted or revoked without re-encrypting the entire dataset. This is crucial in cloud environments where user roles and permissions frequently change.

CL-PRE is a proxy re-encryption authentication mechanism that guarantees the security of cloud data sharing. To safeguard shareable cloud data, a data owner in CLPRE uses an encryption key. The cloud then encrypts and changes the data before distributing it to authorized receivers in accordance with access control. [1] There are two safe data storage options that let authorized users access encrypted data on a storage device anonymously. [2]

The following traits define a groundbreaking approach to data security in cloud storage. First and foremost, the cryptographic key is protected by the two factors. Only when one of the two requirements is met is the cryptographic key's secret retained. Second, using a combination of proxy re-encryption and key separation techniques, the cryptographic key may be swiftly revoked.

Security rules are intended to reduce risks, establish norms for expected user behavior, protect people and data, and facilitate the monitoring of regulatory compliance. In the report, prior studies on cloud computing security were carefully evaluated and examined. To determine which additional rules should be included in the cloud policy, a method for evaluating different cloud hazards was developed [6].In order to eradicate security flaws in cloud computing, this tactic fosters mutual trust between cloud service providers and users. The EMTACA algorithm-based system developed for this project will give cloud users a more dependable, trustworthy, and reputation-based service.The results of this investigation revealed that the three most critical aspects of data security, data confidentiality, integrity, and availability, had all been fulfilled.

The goal of this study is to develop a more reliable decentralized light weight key management system for data center's that will improve data security and key management efficiency. By replicating key shares over many clouds and assuring share integrity with a secret sharing mechanism and a voting system, the proposed solution preserves user data privacy and security. The approach utilized in this study protects against byzantine failure, server collaboration, and data manipulation assaults. [8]

A method for encrypting a two-tier system that allows for fine-grained control over who has access to what data in the cloud was disclosed. The trials demonstrated that the suggested technique is successful, particularly when the data file is big or the integrity check is performed often. [9]

PBE is an asymmetric encryption technique that evolved from Identity-Based Encryption. This approach combines ABAC and asymmetric encryption, allowing for the realization of a single encryptor/multi-decryptor system using a

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.2025.1203010

single algorithm. Platform as a Service and Software as a Service are the objectives of this Predicate Based Encryption. This recommended solution also protects cloud resident data against unintentional.

IV. PROPOSED WORK

Cloud storage services can implement CL-PRE to allow users to securely share files with others. This is particularly useful in collaborative environments where data confidentiality is crucial.While CL-PRE aims to resolve the key escrow problem, it still requires careful management of private keys and public parameters. If these keys are compromised, it can jeopardize the entire system's security. This raises concerns about its resilience against sophisticated attacks, especially as new vulnerabilities are discovered. Certificate less Proxy Re-Encryption (CL-PRE) is an innovative approach that combines the benefits of public key and identity-based cryptography while avoiding the key escrow problem. However, like any cryptographic scheme. The underlying mechanisms of CL-PRE can be more complex than traditional public key or identity-based schemes, making implementation and understanding more challenging. CL-PRE relies on the existence of a trusted authority to generate and distribute public parameters. If the authority is compromised or acts maliciously, it could undermine the entire system's security. While CL-PRE aims to provide a secure framework, the security proofs and assumptions may not be as robust or well-established as those for more mature cryptographic systems. This can lead to concerns about its resilience against advanced attacks.

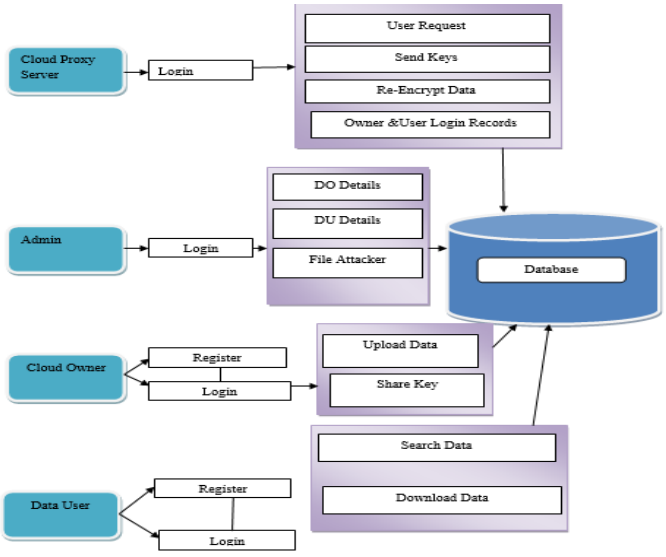

Figure 1. System architecture.

Data that must be accessed from the cloud must be protected. However, cloud owners and users have a big hurdle in terms of security and personal data privacy.Due to the data owners' lack of trust, they save their data in an encrypted format that is inaccessible to outsiders. The phrase “proxy re-encryption” (PRE) refers to a popular way of delivering encrypted data stored in the cloud. When a data owner wants to share encrypted data with both the data user and the cloud server (proxy), the data owner generates re-encryption data and sends it to the proxy, which can use it to convert the data holder's cipher texts into the user's plaintexts without having to look at the plaintexts .

Proxy re-encryption is a type of public-key encryption that allows a proxy to transform cipher texts from one public key to another, without the proxy having access to the underlying plaintext or private keys. This process enables the proxy to re-encrypt the data without knowing the decryption keys. proxy re-encryption has potential applications for secure sharing in a cloud computing environment. The algorithm is use AES algorithm. AES we have use a asymmetric algorithm to perform a public and private key to a user. Supports key lengths of 128, 192, or 256 bits, with longer keys providing stronger security. The decryption process is similar but applies the inverse operations in reverse order. Used for encrypting sensitive data in various applications, including file storage and database encryption.

| 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.2025.1203010

Operation	Existing PRE (ms)	Proposed Scheme (ms)
Encryption	42	35
Re-Encryption	55	28
Decryption	40	30
Key Generation	60	45

Table 2. Comparative results.

We choose to carry out a survey, which is similar to asking a number of The Proxy re-encryption technique, which involves re-encrypting the encrypted ciphertext with the security key before sharing it with the data user, was used in the suggested system. to provide a flexible, secure, and private method of accessing data from cloud computing. to permit different restrictions on cloud data access according to the policies and methods of such a data controller. This is encrypted by the data owner using symmetric secret key K. The data owner may restrict data access according to reputation in order to ensure data protection in a variety of contexts.

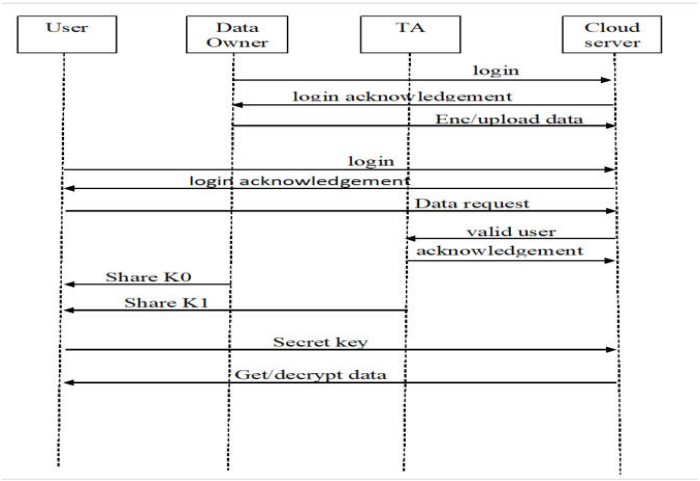

Figure 2. System Sequence Diagram

To evaluate the performance and practicality of the proposed proxy re-encryption (PRE) scheme, we conducted a series of experiments. These results are compared against traditional PRE and attribute-based encryption (ABE) systems.

Operation	Traditional ABE (ms)	Standard PRE (ms)	Proposed Scheme (ms)
Encryption Time	58	45	36
Re-Encryption Time	71	52	28
Decryption Time	50	42	31
Key Generation Time	80	64	40
Revocation Overhead	High	Moderate	Low

A. Owner of the data model

The owner sends data to the cloud for safe and secure data interchange with data consumers. The data owner employs the AES encryption algorithm to protect data privacy and provide security to outsourced data. Data users can view and request data from outsourced documents. After that, the matching index is then produced and exchanged with the private key. The data owner sends the encrypted documents and indexes, as well as the symmetric key and secret key, to the cloud.

B. Secure storage of data

To safeguard the storage of outsourced data from the data owner, the Advanced Encryption Standard (AES) technique is utilized. The ciphertext is encrypted once more with the same method. Among the keys formed are public 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.2025.1203010

private key, and security key. The security key is distributed among the data users in order for the data to be retrieved from cloud storage. The cloud server is only a middleman that keeps the owner's outsourced documents and indexes while also providing data access and search services to consumers. We used drivehq.com free cloud storage with file transfer protocol.

C. Re-Encryption Key

The most difficult technological challenge in the production of a re-encryption key is determining how to include the proxy's decryption key in order to distinguish it from other users. When building the re-encryption key, two elements must be taken into consideration. To prevent proxies from destroying the re-encryption key, it must be attached to the re-encryption key; otherwise, a hostile proxy will have the same decryption powers as the delegate. The re-encryption key will not be utilized if it is exposed, and only the proxy should be aware of the presence of the security key.

D. Data Request processing

If a user requests a file from the data owner, they may use the symmetric key granted to them to decrypt and get the content from the cloud server. A third-party authenticator returns the key required to decrypt the file when a data customer's request token reaches its cloud server. The data owner generates the secret key at random and sends it to search users through a secure connection. After that, the user may view the signatures of encrypted documents that have been sent to the cloud server.

E. Method: Secure and Trust based data sharing

Input: PK is for Public Key, MK stands for Master Key, User Trust, cyphertext
Output: Decrypted plain text
Step 1: Enter public key PK, a master key MK, as well as a specific user identification u and user trust value 'T'.
Step 2: Key generation center picks a random secret Sk and generates public user key value $pk\_u = g$, which would also be used it to generate private attribute keys for u, as well as a secret user key, these keys are provided by owner and Cloud service provider (CSP).
Step 3: The data holder uploads the document to the cloud, and even a symmetric key K is used to encrypt data employing Advanced Encryption Standard (AES) and re-encrypted using proxy re-encryption.
Step 4: Individual trust assessment is used when User "u" proposes an application to access its own data, whether that data is on a file or a computer. The algorithm identifies the policies that are intertwined with Trust.
Step 5: The trust evaluation is the responsibility of the reputation center, RC analyses u's great reputation and determines whether this compiles alongside access rules. RC produces the key 'RK' based on the reputation level, and then access is granted.
Step 6: Cloud Service provider allows user to access requested file by providing another key CK to user.
Step 7: User retrieves the file content after decryption and re-decryption with the given keys.

V.CONCLUSION

This paper presents a novel proxy re-encryption technique designed for secure and efficient data sharing in cloud environments. By integrating ABE, hybrid encryption, and dynamic policy management, our scheme achieves a balance of security, efficiency, and usability. Future work includes exploring homomorphic capabilities within the re-encryption process and blockchain-based auditability. Future work will be built on encrypting both private and public keys, ensuring that created keys are hidden and safe. It may also be used in IoT and medical e-health services. One of the main problems for users of cloud-shared data services is that a proxy and any delegate can cooperate to get and distribute a delegator's decryption capabilities due to the intricacy of most PRE schemes. The aforementioned problem will be resolved by the concept of responsible PRE. Accountable PRE is the formal name for the solution. One of the main concerns for users of cloud data exchange services has been the possibility that the proxy and any data user could collaborate to develop and distribute the data user's decryption keys in proxy re-encryption schemes. The idea of accountable PRE was used in the proposed study to address this problem. The suggested approach offers superior data security in comparison to earlier relevant techniques.

| 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.2025.1203010

REFERENCES

[1]. Xu, Lei, Xiaoxin Wu, and Xinwen Zhang. "CL-PRE: a certificateless proxy re-encryption scheme for secure data sharing with public cloud." Proceedings of the 7th ACM symposium on information, computer and communications security. 2012.

[2] 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.

[3] Blazy, Olivier, Xavier Bultel, and Pascal Lafourcade. "Two secure anonymous proxy-based data storages." 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016). SCITEPRESS-Science and Technology Publications, Lda, 2016.

[4] 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.

[5] 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.

[6] Polyakov, Yuriy, et al. "Fast proxy re-encryption for publish/subscribe systems." ACM Transactions on Privacy and Security (TOPS) 20.4 (2017): 1-31.

[7] Khalil, Issa M., Abdallah Khreishah, and Muhammad Azeem. "Cloud computing security: A survey." Computers 3.1 (2014): 1-35.

[7]. Sarojini, G., A. Vijayakumar, and K. Selvamani. "Trusted and reputed services using enhanced mutual trusted and reputed access control algorithm in cloud." Procedia Computer Science 92 (2016): 506-512.

[8] 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.

[9] 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.

[10] 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.

[11]. Jakimoski, Kire. "Security techniques for data protection in cloud computing." International Journal of Grid and Distributed Computing 9.1 (2016): 49-56.

[11] 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.

[12] Ravindra Changala, "Healthcare Data Management Optimization Using LSTM and GAN-Based Predictive Modeling: Towards Effective Health Service Delivery", 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.

[13]. Rafique, Ansar, et al. "CryptDICE: Distributed data protection system for secure cloud data storage and computation." Information Systems 96 (2021): 101671.

[14] Ravindra Changala, "Controlling the Antenna Signal Fluctuations by Combining the RF-Peak Detector and Real Impedance Mismatch", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526052, May 2024, IEEE Xplore.

[15] Attaluri, V., & Aragani, V. M. (2025). Sustainable Business Models: Role-Based Access Control (RBAC) Enhancing Security and User Management. In Driving Business Success Through Eco-Friendly Strategies (pp. 341-356). IGI Global Scientific Publishing.

[16] Ravindra Changala, “Optimizing 6G Network Slicing with the EvoNetSlice Model for Dynamic Resource Allocation and Real-Time QoS Management”, International Research Journal of Multidisciplinary Technovation, Vol 6 Issue 4 Year 2024, 6(4) (2024) 325-340.

| 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.2025.1203010

[17] Ravindra Changala, "Deep Learning Techniques to Analysis Facial Expression and Gender Detection", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10525942, May 2024, IEEE Xplore.
[18] Ravindra Changala, "UI/UX Design for Online Learning Approach by Predictive Student Experience", 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), ISBN:979-8-3503-4060-0, DOI: 10.1109/ICECA58529.2023.10395866, February 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