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.2025.1203063

A Proxy Re-Encryption Model for Secure and Confidential Cloud Data Sharing

G.Sirisha[1], K.Shivapriya[2], N.Aditya[3], N.Srikar[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India[2,3,4]

ABSTRACT: This project presents a Proxy Re-Encryption (PRE) framework designed for secure information sharing and control in a cloud environment. Its primary aim is to enable a cloud data owner to upload, partition, and allow a user to interact with their data, while preserving confidentiality and integrity. Initially, the data owner uploads a file, which is divided into four separate segments. Each of these segments is hashed using the SHA algorithm, producing four unique hash outputs that function as integrity checks for each data fragment. To safeguard the data during sharing, it is first encrypted by the owner before being made accessible to an authorized user. The encrypted file is then processed through a proxy re encryption step, allowing a proxy server to re-encrypt it without accessing its actual contents. This mechanism enables the user to securely decrypt the data using a corresponding key. The cloud server coordinates this process, handling the re-encryption and delivering the encrypted file and key to the user. Only users with explicit authorization from the data owner can access the content. By employing proxy re-encryption, this approach ensures that the cloud server does not require visibility into the plaintext data, enhancing security and privacy.

I. INTRODUCTION

The Internet of Things (IoT) has become a key technological advancement with widespread impact and has significantly contributed to the surge in global network traffic over time. With expectations of billions of devices becoming interconnected in the near future, data has taken a central role within the IoT landscape, as it supports numerous functionalities. In sectors such as healthcare, intelligent transport, urban infrastructure, industrial automation, and production, the data collected is vital for informed decision-making. Sensors deployed in these systems gather a wide range of critical parameters that provide valuable insights to relevant stakeholders. Proxy Re-Encryption (PRE), a concept introduced by Blaze et al., offers a more adaptable solution. PRE enables an intermediary to convert encrypted content, originally encrypted with the owner's public key, into a form that another recipient can decrypt. Here, the data owner plays the role of the delegator, and the recipient is the 1 delegate. Through PRE, the owner can grant temporary access to encrypted data without sharing their private key. A re-encryption key, generated either by the owner or a trusted party, is provided to the proxy, which uses it to transform the ciphertext. Notably, the proxy does not need to be trusted, as it lacks access to the actual decryption keys. This approach is highly suited for secure delegation in data-sharing scenarios. It allows encrypted data stored in the cloud to be safely shared with authorized users, without exposing it to unauthorized entities. Encryption ensures that only users explicitly approved by the data owner can view the data, reducing the risk of unintended disclosures. Building on this concept, the proposed solution integrates PRE with Identity-Based Encryption (IBE), Information-Centric Networking (ICN), and blockchain to enhance IoT data sharing. This model simplifies key distribution and supports various advanced cryptographic schemes, such as searchable encryption, private handshake protocols, and secure encryption schemes resistant to chosen-ciphertext attacks. Compared to Attribute Based Encryption (ABE), IBE is more compatible with IoT devices due to its lighter computational load, making it more suitable for constrained environments. To further support the scalability of information sharing, this work incorporates ICN principles, which allow content to be named, distributed, and cached within the network itself. ICN enables fast data access and efficient bandwidth usage, which is essential for the growing demands of IoT networks. In terms of ensuring trust, the approach leverages blockchain—a decentralized ledger concept introduced by Nakamoto—as a framework for secure, verifiable data exchanges. Although managing large volumes of data on a blockchain presents challenges, its implementation in emerging systems has proven effective for decentralized access control. With blockchain, sensitive data can remain protected while allowing for user access revocation and enhanced data confidentiality.

| 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.2025.1203063

II. LITERATURE REVIEW

In their 2023 paper, P. K. Tysowski and M. A. Hasan discussed the Hybrid attribute-and re-encryption based key management for secure and scalable mobile applications in clouds. Outsourcing data to the cloud are beneficial for reasons of economy, scalability, and accessibility, but significant technical challenges remain. Sensitive data stored in the cloud must be protected from being read in the clear by a cloud provider that is honest-but-curious. Additionally, cloud-based data are increasingly being accessed by resource-constrained mobile devices for which the processing and communication cost must be minimized. Novel modifications to attribute-based encryption are proposed to allow authorized users access to cloud data based on the satisfaction of required attributes such that the higher computational load from cryptographic operations is assigned to the cloud provider and the total communication cost is lowered for the mobile user. Furthermore, data re-encryption may be optionally performed by the cloud provider to reduce the expense of user revocation in a mobile user environment while preserving the privacy of user data stored in the cloud. The proposed protocol has been realized on commercially popular mobile and cloud platforms to demonstrate real-world benchmarks that show the efficacy of the scheme. A simulation calibrated with the benchmark results shows the scalability potential of the scheme in the context of a realistic workload in a mobile cloud computing system.

In their 2023 paper,E. M. Kornaropoulos, N. Moyer, C. Papamanthou, and A. Psomas, discussed on Decentralizing privacy: Using blockchain to protect personal data, The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data. Bit coin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. In this paper, we describe a decentralized personal data management system that ensures users own and control their data. We implement a protocol that turns a block chain into an automated access-control manager that does not require trust in a third party. Unlike Bit coin, transactions in our system are not strictly financial -- they are used to carry instructions, such as storing, querying and sharing data. Finally, we discuss possible future extensions to block chains that could harness them into a well-rounded solution for trusted computing problems in society

In their 2023 paper, R. S. Da Silva and S. D. Zorzo, discussed on An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges, For future Internet, information-centric networking (ICN) is considered a potential solution to many of its current problems. However, concern regarding the protection of user data persists. This paper presents an access control mechanism that will allow users to set fine-grained access policies for applications in named data networking (NDN), a popular ICN architecture. Using an attribute-based encryption scheme with an immediate revocation of privileges, data security is guaranteed. The mechanism inserts a Cloud Proxy Server to mediate the access to the protected data and to inspect for revocation. As an optional feature, the NDN router can add Cloud Proxy Server functions. According to the experiments, the proposed security mechanism proved functional in terms of processing time, memory usage, and file size, which influence both storage and transmission and demonstrate efficiency in manipulating dozens of attributes in an access policy.

In their 2022 paper,E. M. Kornaropoulos, C. Papamanthou, and R. Tamassia ,discussed on
A Revocable Certificateless Sanitizable Signature Scheme With Batch Verification, In medical and healthcare application scenarios, data integrity and user privacy are often concerned the most. A subitizable signature scheme is a common adopted approach since it admits an authorized person to sanitize partial sensitive information of signed messages while keeping the correctness of preserved message and signature pairs. A certificateless subitizable signature scheme further enjoys the merits of certificateless public key systems. That is, it is unnecessary to maintain the public key certificates in traditional cryptosystems or deal with the key escrow problem in identity-based systems. However, the functionality of batch verification for retained message-signature pairs and the revocation mechanism are still lack in previous works. To resolve these issues, the authors propose a revocable certificateless subitizable signature scheme with batch verification in this paper. The revocation mechanism is fulfilled by combining user's private key with an updatable time key. Hence, a revoked user is unable to request the renewed time key. We also provide a formal proof that our proposed system satisfies the security requirement of existential unforgeability under adaptive chosen-message attacks (EUF-CMA) in the random oracle model. In comparison to related variants, our system demonstrates superior functionality and computational efficiency.

| 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.2025.1203063

III. METHODOLOGY

The data was encrypted using KP-ABE which meant that only an appropriate collection of the attribute secret keys can make decryption possible. Besides the encrypted data, the cloud also managed all attribute secret keys except one special secret key in order to handle revocation of users. When users are revoked, new keys were distributed to the remaining users by the data owner and the encrypted data had to be re-encrypted. Although the scheme was efficient, the re-encryption was performed in a lazy way, and, therefore, the security of the scheme was weakened. Park provided a modification to the scheme. Modules as follows:

- User Interface Design
- Admin
- Cloud Owner
- Cloud Cloud Proxy Server
- Data User

3.1.2 Module Descriptions

User Interface Design: In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page ule Descriptions

Admin: This is the first module. Here admin has a main modules to stores all the information's of the project.Admin is a login with a user id and password.Admin has a stores all information's of details.Admin can also have a data owner details.Admin can have a data user details in the database. The admin can have a file attacker to file attack information
Cloud Owner : This is the Second module of this project. In this module cloud owner should register and Login. Cloud owner can store a data in a text format. Cloud owner can also have a key send to the Cloud Proxy Server should approve then the key will send an authentic user. User can access a data.

Cloud Cloud Proxy Server: In this module Cloud Proxy Server has login. After login it will have a data user requests. Data user after register it will takes a permissions from the server. In server it will approve then the data user can login. Cloud Proxy Server has a send keys to the user. Cloud Proxy Server can also are re-encrypt a file then forward to the user. Cloud Proxy Server has a key will updates and key will modify. Cloud Proxy Server has a maintains a records of a logins of Cloud Owner and data users.

Data User: In this module the data user can also a register with a details. Login it takes permission from the Cloud Proxy Server. Cloud Proxy Server can a approve a user. After approve it was data user can login. Data user can also a search a data. Data user can also a download a file.

IV. EXISTING SYSTEM

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.

V. PROPOSED SYSTEM

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.

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

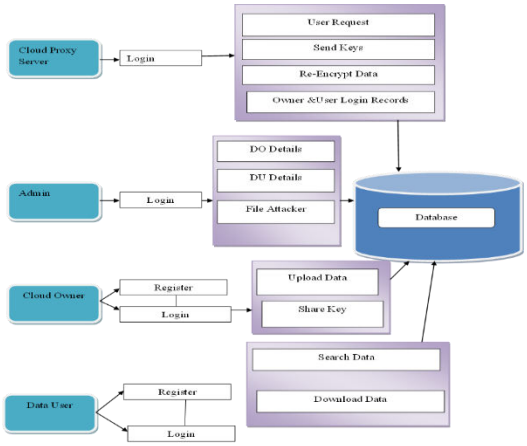
| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

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

DOI:10.15680/IJARETY.2025.1203063

Proposed System Advantage:
It trusted authorities to generate and distribute a parameters It Provides a public platform for data owners to store and share their encrypted data.

System Architecture



VI. IMPLEMENTATION

This project is implements like web application using COREJAVA and the Server process is maintained using the SOCKET & SERVERSOCKET and the Design part is played by Cascading Style Sheet.

VII. EXPERIMENTAL RESULTS

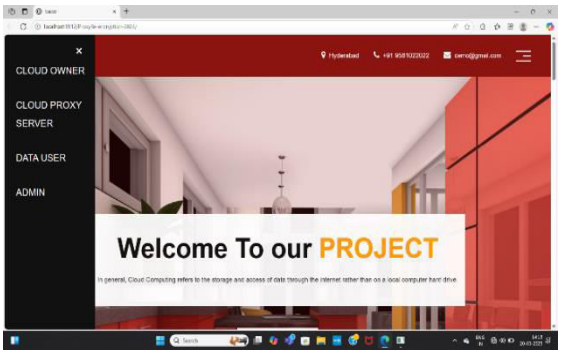


Figure 1: Home Page

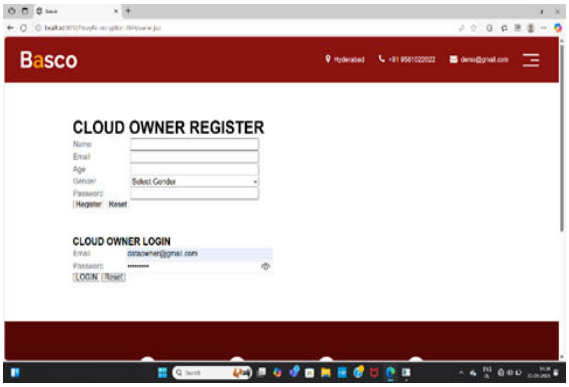


Figure 2: Cloud Owner Registration Page

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.2025.1203063

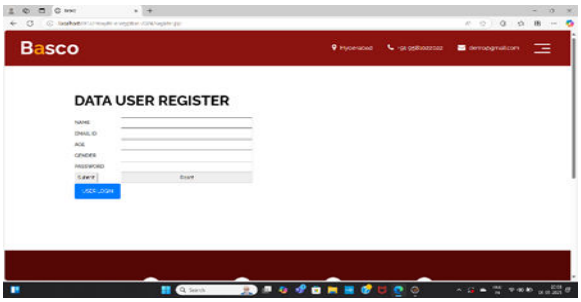


Figure 3: User Registration page

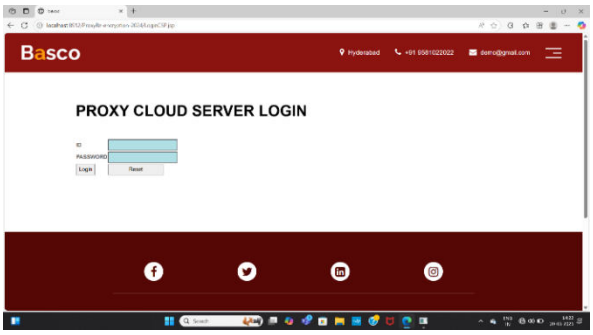


Figure 4: Server login page

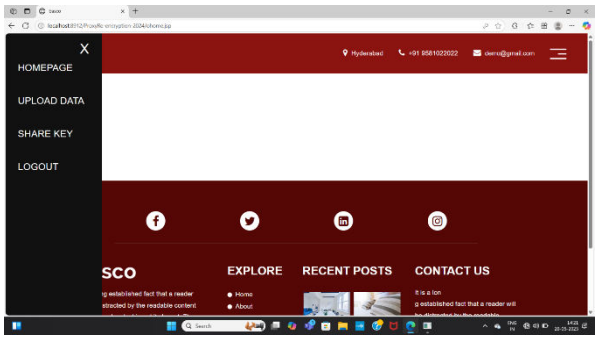


Figure 5 Cloud Owner Interface

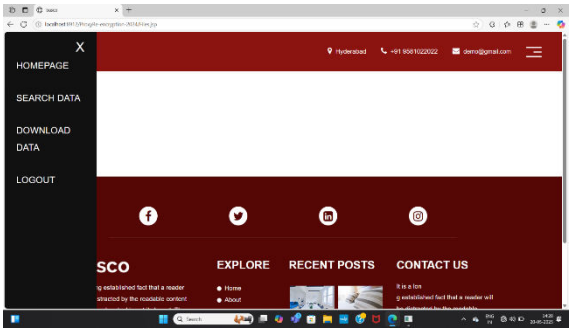


Figure 6: Data User Interface

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.2025.1203063

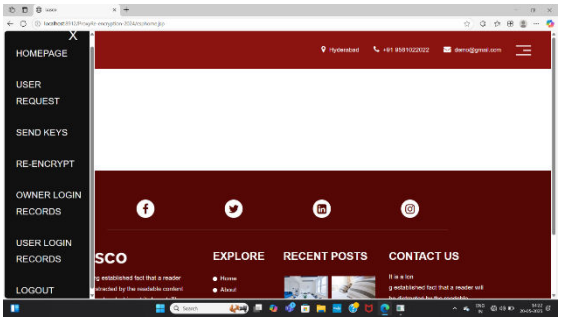


Figure 7 **:** Proxy Cloud Server Interface

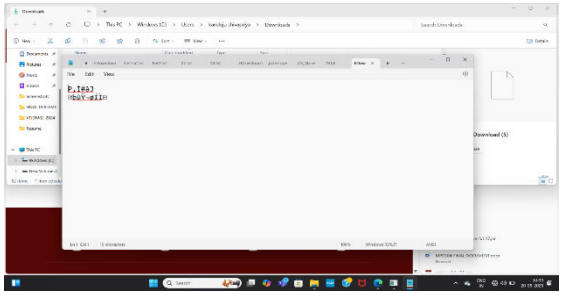


Figure 8:Encrypted File Content Before User Obtains Decryption Keys from Data Owner

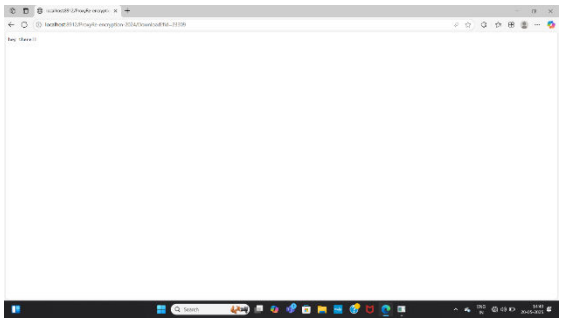


Figure 9: Display of Original File Content After Successful Decryption and Download

VIII. CONCLUSION

The emergence of the IoT has made data sharing one of its most prominent applications. To guarantee data confidentiality, integrity, and privacy, we propose a secure identity-based PRE data-sharing scheme in a cloud computing environment. Secure data sharing is realized with IBPRE technique, which allows the data owners to store their encrypted data in the cloud and share them with legitimate users efficiently. Due to resource constraints, an edge device serves as the proxy to handle the intensive computations. The scheme also incorporates the features of ICN to proficiently deliver cached content, thereby improving the quality of service and making great use of the network bandwidth.

IX. FUTURE ENHANCEMENT

Then, we present a blockchain-based system model that allows for flexible authorization on encrypted data. Fine grained access control is achieved, and it can help data owners achieve privacy preservation in an adequate way. The analysis and results of the proposed model show how efficient our scheme is, compared to existing schemes..

| 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.2025.1203063

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347–2376, Oct./Dec. 2015.

[2] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., SpriMay 1998, pp. 127–144.

[3] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984, pp. 47–53.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 2004, pp. 506–522.

[5] B.R.Waters,D.Balfanz,G Durfee,and D.K. Smetters,"Building an encrypted and searchable audit log,"in NDSS,vol.4.Citeseer,Feb.2004,pp. 5–6.

[6] D. Balfanz et al., "Secret handshakes from pairing-based key agreements," in Proc. IEEE, Symp. Secur. Privacy, 2003, pp. 180–196.

[7] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption Techn., Springer, 2004, pp. 207–222.

[8] T. Koponen et al., "A data-oriented (and beyond) network architecture," in Proc. Conf. Appl., Techn., Architectures, Protec. Compute. Commun., Aug. 2007, pp. 181–192.

[9] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, "Developing information networking further: From PSIRP to pursuit," in Proc. Int. Conf. Broadband Commun., Newt. Syst., Springer, Oct. 2010, pp. 1–13.

[10] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in Proc. INFOCOM IEEE Conf. Compute. Commun. Workshops,2010, pp. 1–6. [11] A. Carzaniga, M. J. Rutherford, and A. L. Wolf, "A routing scheme for content-based networking," in Proc. IEEE INFOCOM 2004, vol. 2, 2004,

[12] I. Psaras, W. K. Chai, and G. Pavlou, "Probabilistic in-network caching for information-centric networks," in Proc. 2nd ed. ICN Workshop Inform.- Centric Newt., Aug. 2012, pp. 55–60.

[13] Y. Sun et al., "Trace-driven analysis of ICN caching algorithms on video on-demand workloads," in Proc. 10th ACM Int. Conf. Emerging Newt. Exp. Technol., Dec. 2014, pp. 363–376.

[14] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, vol. 4. Bitcoin.org, 2008. Available: https://bitcoin. org/bitcoin. pdf

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing,", Mar, pp. 1–9.

[16] N. Park, "Secure data access control scheme using type-based reencryption in cloud environment," in Semantic Methods Knowledge Management and Communications. Berlin, Germany: Springer, 2011, pp. 319– 327.

[17] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,"vol.30,no.5,pp.320–331,Jul. 2011.

[18] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng.,vol. 25, no.10, pp. 2271–2282, Apr. 2011.

[19] P. K. Tysowski and M. A. Hasan, "Hybrid attribute-and re-encryptionbased key management for secure and scalable mobile applications in clouds," IEEE Trans. Cloud Compute., vol. 1, no. 2, pp. 172–186, Nov. 2013.

[20] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inform. Sci., vol. 258, pp. 355–370, Feb. 2014.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152

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