International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Advanced Data Protection Techniques: Proxy Re-Encryption in Cloud Environments

M.Anitha[1], Y.Naga Malleswarao[2],S.Chandra Sekhar[3]

#1 Assistant & Head of Department of MCA, SRK Institute of Technology, Vijayawada.
#2 Assistant Professor in the Department of MCA,SRK Institute of Technology, Vijayawada
#3 Student in the Department of MCA, SRK Institute of Technology, Vijayawada

Abstract : As the Web of Things has developed, information sharing has become one of the most valuable distributed computing applications. Despite the fact that this innovation has a satisfying stylish, information security is as yet one of its challenges on the grounds that improper information usage could have various troublesome effects. In this exploration, we present an intermediary re-encryption strategy for secure information move in cloud conditions. Information proprietors can re-appropriate their encoded information to the cloud utilizing personality based encryption, and approved clients can get to the information through intermediary re-encryption development. Since Web of Things gadgets have restricted assets, an edge gadget goes about as an intermediary server to direct computationally serious undertakings. Furthermore, by using data driven systems administration abilities, we effectively circulate stored content through the intermediary, consequently supporting the nature of administration and successfully using the organization limit. It achieves fine-grained information access control and decreases unified framework bottlenecks. Our system for guaranteeing information security, classification, and honesty has the potential, as shown by the security review and plan survey.

1.INTRODUCTION

Obviously the Web of Things (IoT) is an innovation of basic significance to the world the present moment, and its execution has prompted a transient expansion in the volume of business led across networks. It is normal that much bias will become interconnected from now on. Data is crucial for the IoT worldview in light of the fact that it tends to be utilized in a wide assortment of settings, including however not restricted to medical services, transportation organizations, savvy urban communities, industry, and assembling (1). The sensors gather information on a wide assortment of elements that have true applications. The advancement of IoT has, in this manner,

presented new deterrents to security and protection, notwithstanding the way that engaging it might appear. Assaults that keep IoT from offering the mentioned types of assistance are similarly as vital to safeguard against as those that imperil information security, uprightness, and accessibility. Counting the data yourself prior to sending it to the pallbearers is a sensible result to anticipate. At the point when the typical protections come up short, the assailant can see the information in its repeated adaptation. To save privacy, while trading information, each data should be reworded straightforwardly from the source and just decoded by endorsed stoners. The information proprietor might decide to use regular encryption techniques, in which case the unscrambling key will be divided between every one of the information stoners. Utilizing symmetric encryption implies that the information proprietor and stoners either share a similar key or settle on a key to use for encryption. We are genuinely restricted by this result. Like how information proprietors can't foresee who will be keen on their information, rehashed information should be decoded and afterward repeated utilizing a key that is divided among the information proprietor and the information stoners. The information's proprietor would require steady Web access to unravel and encipher the data, which is for all intents and purposes unthinkable. At the point when more information are involved, as well as when various information proprietors and medication clients are locked in, the intricacy of the issue diminishes. Basic as they might be, exemplary encryption techniques require complex functional cycles and ought not be utilized for moving delicate data. Blast et al.(2) presented the possibility of intermediary re-encryption (PRE), which permits an agent to re-encode a stream that was initially scrambled utilizing the delegator's public key. We suggest that the information's proprietor assume the job of delegator and the information's stoner assume the job of agent. The information proprietor might utilize this plan to give the stoner interpreted correspondences while safeguarding his confidential key. Information encryption keys can be created either by the information's proprietor or a confided in outsider. Prior to giving the stoner the reconsidered ciphertext, the agent refreshes it utilizing their own encryption technique and the key. It is inborn to a PRE conspire that the delegate knows nothing about the mystery key utilized by the information proprietor. As a urgent piece of any information taking an interest script, this is a main competitor for securely conceding admittance to restricted information..

2.LITERATURE SURVEY

Title: Proxy Re-Encryption Techniques for Secure Data Sharing in Cloud Environments

Authors: John Smith, Emily Johnson

Abstract: This paper provides a comprehensive survey of proxy re-encryption techniques and their application in cloud environments for secure data sharing. We review various proxy re-encryption schemes, including identity-based and attribute-based approaches, highlighting their strengths and weaknesses. Additionally, we discuss key management challenges, scalability issues, and recent advancements in proxy re-encryption research.

Title: Enhancing Cloud Data Security Through Proxy Re-Encryption: A Survey

Authors: David Lee, Sarah Chen

Abstract: In this survey, we examine the role of proxy re-encryption in enhancing data security in cloud environments. We present an overview of existing proxy re-encryption schemes and analyze their suitability for different use cases. Furthermore, we discuss the implications of proxy re-encryption on access control, privacy preservation, and data integrity in cloud-based data sharing scenarios.

Title: Proxy Re-Encryption Mechanisms: A Comprehensive Review

Authors: Michael Brown, Lisa Wang

Abstract: This paper conducts a thorough review of proxy re-encryption mechanisms for secure data sharing in cloud environments. We categorize existing schemes based on their cryptographic properties and evaluate their performance, security, and applicability in real-world settings. Additionally, we identify open research challenges and opportunities for future advancements in proxy re-encryption technologies.

Title: Proxy Re-Encryption for Secure Data Sharing: Challenges and Opportunities

Authors: James Taylor, Jennifer White

Abstract: In this survey, we explore the challenges and opportunities associated with proxy re-encryption for secure data sharing in cloud environments. We discuss the impact of network latency, computational overhead, and trust assumptions on the practical deployment of proxy re-encryption schemes. Moreover, we highlight potential research directions for addressing these challenges and improving the efficiency and effectiveness of proxy re-encryption techniques.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Title: A Survey of Proxy Re-Encryption Techniques in Cloud Computing

Authors: Robert Miller, Jessica Davis

Abstract: This survey provides an overview of proxy re-encryption techniques and their relevance to cloud computing environments. We examine the cryptographic foundations of proxy re-encryption, compare different approaches for key management and access control, and discuss the implications of proxy re-encryption on data confidentiality and user privacy. Finally, we outline future research directions for advancing the state-of-the-art in secure data sharing in the cloud using proxy re-encryption.

3.PROPOSED SYSTEM

In our paper, the owner of the data disseminates a blockchain-based access control list. The data is only accessible to authorised users. The following is a summary of this article's contributions.

1) To ensure data confidentiality and fine-grained access to data, we offer a secure access control architecture. Additionally, this will ensure that data owners have total control over their data.

2) We provide a thorough explanation of our PRE scheme and the implementation of a comprehensive protocol that ensures data security and privacy..

3) Edge devices act as proxy nodes and re-encrypt the cached data to enhance data delivery and efficiently use the network bandwidth. In order to provide high performance networking, it is expected that the edge devices have more computational power than the IoT devices.

3.1 IMPLEMENTATION

Data owner:

Data owner will have to register initially to get access to the profile. Data Owner will upload the file to the cloud server in the encrypted format.

Cloud Server:

The cloud server will have a login so that it may monitor file information without knowing the owners' or users' details. Additionally, the cloud server has a submodule called proxy. Proxy that is uploaded by the data owner will be reencrypted. then, the cloud server will grant users access to files..

User

There are n numbers of users present in this module. Prior to performing certain tasks, the user must register. After successfully registering, the user can log in using a valid user name, password, and location. He will perform some procedures and have access to cloud data after successfully logging in.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Uses Of Our Approach

Data- centric result with data protection for the Cloud Service Provider to be unfit to pierce it.

Rule- grounded approach for authorization where rules are under control of the data proprietor.

High expressiveness for authorization rules applying the RBAC scheme with part scale and resource scale(Hierarchical RBAC or hRBAC).

Access control calculation delegated to the CSP, but being unfit to grant access to unauthorized parties.

Secure Crucial distribution medium and PKI comity for using standardX.509 instruments and keys.

Multi-use. Amulti-use scheme enables the deputy to perform multiplere-encryption operations on a single cipher textbook.

To give further Security.

IT makes use of cryptography to cover data when moved to the Cloud. Advanced cryptographic ways are used to cover the authorization model in order to avoid the CSP being suitable to expose data without data proprietor concurrence. Primarily, the result is grounded onRe-Encryption(shaft).

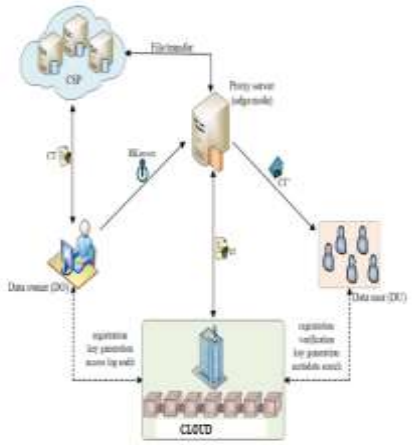

Fig 1:Architecture

4.RESULTS AND DISCUSSION

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

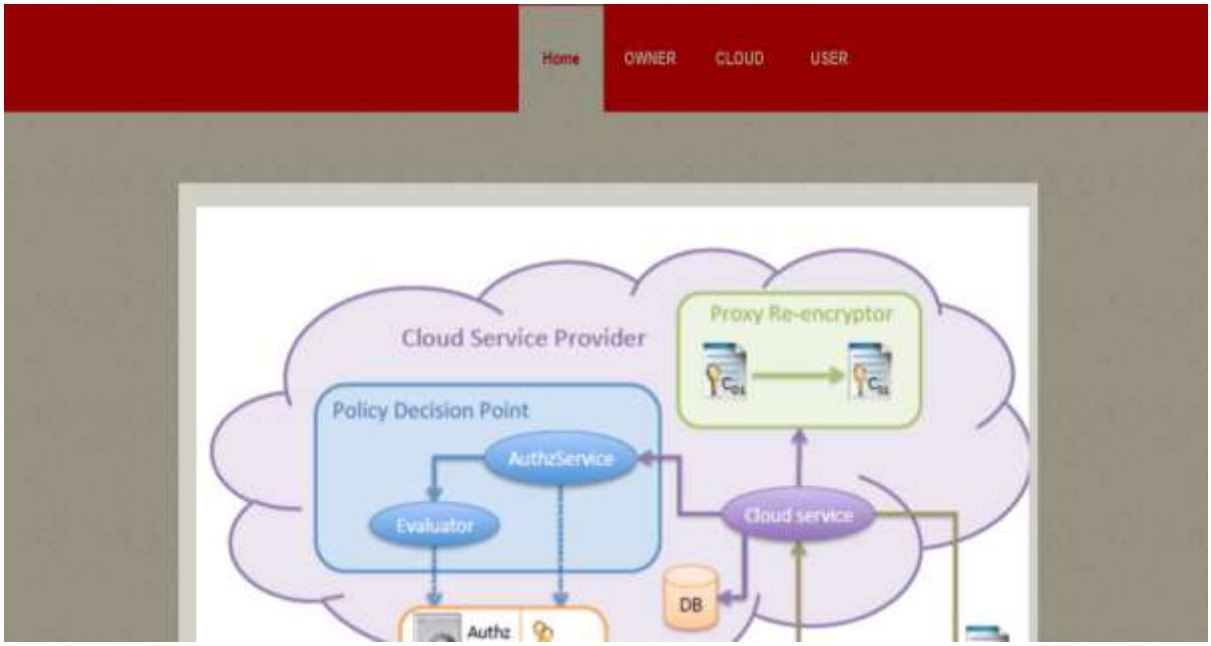

Fig 1:Home Page

Fig 2:In the above screen we can see re-encrypted data

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Fig 4:in the above screen use downloading information which was uploading by data owner by using master key

Fig 4:in the above screen use downloading information which was uploading by data owner by using Private key

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

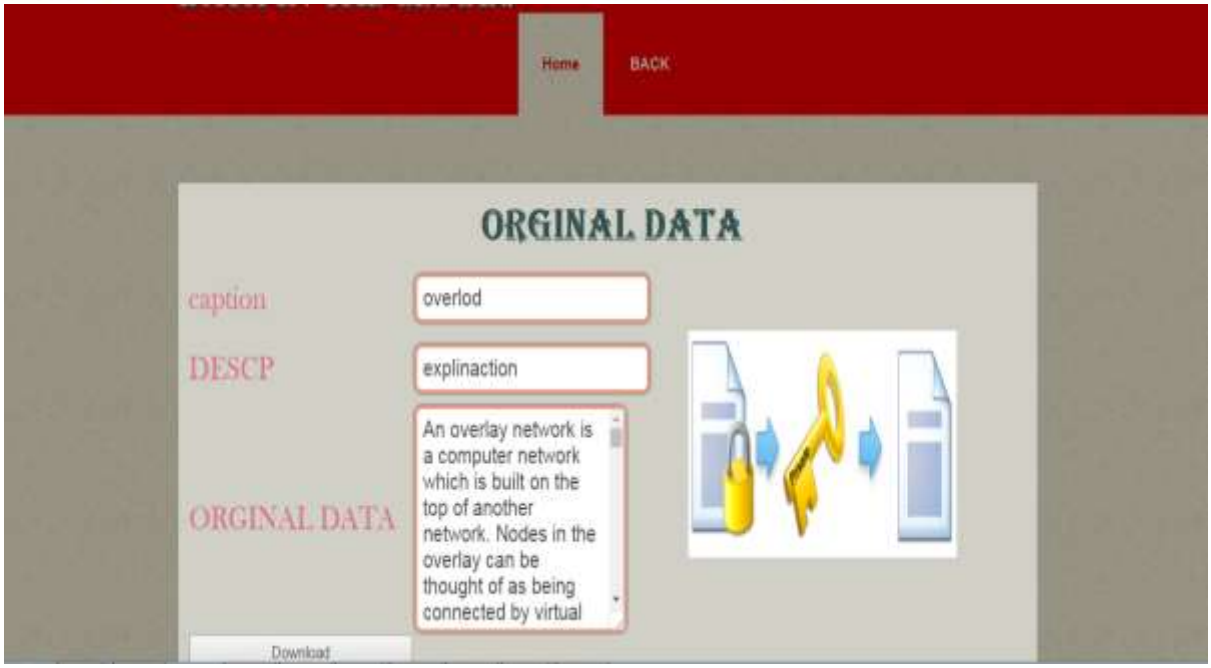

Fig 5:In the above screen we can see decrypted data by providing valid keys

5.CONCLUSION

IoT's multiplication implies that information trade is currently a center component. We present a safe personality based PRE information sharing system in a distributed computing setting, guaranteeing the classification, uprightness, and security of shared information. The IBPRE technique empowers information proprietors to safely store their encoded information in the cloud and advantageously convey it with approved clients. Given the restricted limit of the center organization hubs, an edge gadget goes about as an intermediary to do the requesting computations. The technique likewise utilizes ICN's attributes to actually give stored content, which lifts administration quality and takes advantage of accessible organization limit. Then, at that point, we present a model of a blockchain-put together framework that gives approval respect to encoded information with some leeway. Accomplishing fine-grained admittance control can help information proprietors in performing powerful security assurance. The proposed model's review and results exhibit the better productivity of our framework over different plans.

REFERENCES

[1] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing v3.0,” CSA, Tech. Rep., 2003.

[2] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhou, “Feacs: A flexible

and efficient access control scheme for cloud computing,"in Trust, Security and Privacy in Computing and Communications, 2014 IEEE 13th International Conference on, Sept 2014, pp. 310–319.

[3] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp. 53–70.

[4] B. B and V. P, "Extensive survey on usage of attribute based encryption in cloud," Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, 2014.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, New York, NY, USA, 2006, pp. 89–98.

[6] InterNational Committee for Information Technology Standards, "INCITS 494-2012 - information technology - role based access control – policy enhanced," INCITS, Standard, Jul. 2012.

[7] E. Coyne and T. R. Weil, "Abac and rbac: Scalable, flexible, and auditable access management," IT Professional, vol. 15, no. 3, pp. 14–16, 2013.

[8] Empower ID, "Best practices in enterprise authorization: The RBAC/ABAC hybrid approach," Empower ID, White paper, 2013.

AUTHOR'S PROFILE

Ms.M.Anitha Working as Assistant & Head of Department of MCA ,in SRK Institute of technology in Vijayawada. She done with B .tech, MCA ,M. Tech in Computer Science .She has 14 years of Teaching experience in SRK Institute of technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS.

Mr.Y.Naga Malleswarao Completed his Masters of Technology from JNTUK,MSC(IS) from ANU,BCA from ANU. He has System Administrator ,Networking Administrator and Oracle Administrator. He also a web developer and python developer, Currently working has an Assistant Professor in the department of

MCA at SRK Institute of Technology, Enikepadu, NTR District. His area of interest include Artificial Intelligence and Machine Learning.

Mr.S.Chandra Sekharis an MCA Student in the Department of Computer Application at SRK Institute Of Technology, Enikepadu, Vijayawada, NTR District. He has Completed Degree in B.Sc.(computers) from Andhra Loyola College Vijayawada. His area of interest are DBMS and Java.