International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 19th Nov 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 11

DOI: 10.48047/IJIEMR/V11/ISSUE 11/07

Title **A Proxy Re-Encryption Approach to Secure Data Sharing In Cloud For Data Security**

Volume 11, ISSUE 10, Pages: 43-50

Paper Authors

MISS. GANGARAJU SURESH CHANDANA , MS. E.STUTHI

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A Proxy Re-Encryption Approach to Secure Data Sharing In Cloud For Data Security

MISS. GANGARAJU SURESH CHANDANA [1], MS. E.STUTHI[2]

#1PG SCHOLAR, DEPT OF CSE AT CHADALAWADA RAMANAMMA ENGINEERING COLLEGE, TIRUPATHI.
#2 ASSISTANT PROFESSOR, DEPT OF CSE AT CHADALAWADA RAMANAMMA ENGINEERING COLLEGE, TIRUPATHI

Abstract : Data sharing has emerged as one of the Internet of Things' most advantageous cloud computing applications as it has developed. Even if this technology has been visually appealing, data security is still one of its challenges because improper usage of data can result in a variety of negative effects. We provide a proxy re-encryption method in this paper for safe data exchange in cloud contexts. Identity-based encryption enables data owners to outsource their encrypted data to the cloud, while proxy re-encryption construction allows authorised users to access the data. Due to the limited resources of Internet of Things devices, an edge device serves as a proxy server to handle demanding calculations. Additionally, we successfully distribute cached material in the proxy by utilising information-centric networking capabilities, hence enhancing the quality of service and making efficient use of the network capacity. It achieves fine-grained access control to data and reduces bottlenecks in centralised systems. The security study and evaluation of our plan demonstrate the potential of our strategy for guaranteeing data security, confidentiality, and integrity.

1.INTRODUCTION

The Internet of effects(IoT) has surfaced as a technology that has great significance to the world currently and its application has given rise to an expanded growth in network business volumes over the times. It's anticipated that a lot of bias will get connected in the times ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposes in operations similar as healthcare, vehicular networks, smart metropolises, diligence, and manufacturing, among others(1). The detectors measure a host of parameters that are veritably useful for stakeholders involved. Accordingly, as enticing as IoT seems to be, its advancement has introduced new challenges to security and sequestration. IoT needs to be secured against attacks that hamper it from furnishing the needed services, in addition to those that pose pitfalls to the confidentiality, integrity, and sequestration of data. A feasible result is to cipher the data before outsourcing to the pall waiters. bushwhackers can only see the data in its translated form when traditional security measures fail. In data sharing, any information must be translated from the source and only deciphered by authorized druggies in order to save its protection. Conventional encryption ways can be used, where the decryption key is participated among all the data druggies

designated by the data proprietor. The use of symmetric encryption implies that the same key is participated between the data proprietor and druggies, or at least the actors agree on a key. This result is veritably hamstrung. likewise, the data possessors don't know in advance who the intended data druggies are, and, thus, the translated data needs to be deciphered and latterly translated with a crucial known to both the data proprietor and the druggies. This decrypt- and- cipher result means the data proprietor has to be online all the time, which is virtually not doable. The problem becomes decreasingly complex when there are multiple pieces of data and different data possessors and druggies Although simple, the traditional encryption schemes involve complex crucial operation protocols and, hence, aren't apt for data sharing. Proxy re-encryption(PRE), a notion first proposed by Blaze etal.(2), allows a deputy to transfigure a train reckoned under a delegator's public key into an encryption intended for a nominee. Let the data proprietor be the delegator and the data stoner be the delegate. In such a scheme, the data proprietor can shoot translated dispatches to the stoner temporarily without revealing his secret key. The data proprietor or a trusted third party generates there-encryption key. A deputy runs there-encryption algorithm with the key and revamps the ciphertext before transferring the new ciphertext to the stoner. An natural particularity of a PRE scheme is that the deputy isn't completely trusted(it has no idea of the data proprietor's secret key). This is seen as a high seeker for delegating access to translated data in a secured manner, which is a pivotal element in any data-participating script.

2.LITERATURE SURVEY

2.1) FEACS: A Flexible and Efficient Access Control Scheme for Cloud Computing

AUTHORS: Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhount.

In the past few years, cloud computing has emerged as one of the most influential paradigms in the IT industry. As promising as it is, this paradigm brings forth many new challenges for data security because users have to outsource sensitive data on untrusted cloud servers for sharing. In this paper, to guarantee the confidentiality and security of data sharing in cloud environment, we propose a Flexible and Efficient Access Control Scheme (FEACS) based on Attribute-Based Encryption, which is suitable for fine-grained access control. Compared with existing state-of-the-art schemes, FEACS is more practical by following functions. First of all, considering the factor that the user membership may change frequently in cloud environment, FEACS has the capability of coping with dynamic membership efficiently. Secondly, full logic expression is supported to make the access policy described accurately and efficiently. Besides, we prove in the standard model that FEACS is secure based on the Decisional Bilinear Diffie-Hellman assumption. To evaluate the practicality of FEACS, we provide a detailed theoretical performance analysis and a simulation

comparison with existing schemes. Both the theoretical analysis and the experimental results prove that our scheme is efficient and effective for cloud environment.

2.2) Innovative method for enhancing key generation and management in the AES-algorithm

AUTHORS: O. K. J. Mohammad, S. Abbas, E. M. El-Horbaty, and A. M.Salem

With the extraordinary maturity of data exchange in network environments and increasing the attackers capabilities, information security has become the most important process for data storage and communication. In order to provide such information security the confidentiality, data integrity, and data origin authentication must be verified based on cryptographic encryption algorithms. This paper presents a development of the advanced encryption standard (AES) algorithm, which is considered as the most eminent symmetric encryption algorithm. The development focuses on the generation of the integration between the developed AES based S-Boxes, and the specific selected secret key generated from the quantum key distribution.

2.3) Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption

AUTHORS: R. Bobba, H. Khurana, and M. Prabhakaran

In distributed systems users need to share sensitive objects with others based on the recipients' ability to satisfy a policy. Attribute-Based Encryption (ABE) is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. Ciphertext-Policy ABE (CP-ABE) is a form of ABE where policies are associated with encrypted data and attributes are associated with keys. In this work we focus on improving the flexibility of representing user attributes in keys. Specifically, we propose Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) - a new form of CP-ABE - which, unlike existing CP-ABE schemes that represent user attributes as a monolithic set in keys, organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. We show that the proposed scheme is more versatile and supports many practical scenarios more naturally and efficiently. We provide a prototype implementation of our scheme and evaluate its performance overhead.

2.**4) Identity-based proxy re-encryption,"in Proceedings of the 5th International Conference on Applied Cryptography and Network Security**

AUTHORS: M. Green and G. Ateniese

In a proxy re-encryption scheme a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext. A number of solutions have been proposed in the public-key setting. In this paper, we address the problem of Identity-Based proxy re-encryption, where ciphertexts are transformed from one identityto another. Our

schemes are compatible with current IBE deployments and do not require any extra work from the IBE trusted-party key generator. In addition, they are non-interactive and one of them permits multiple re-encryptions. Their security is based on a standard assumption (DBDH) in the random oracle model.

2.5) Detection of semantic conflicts in ontology and rule-based information systems

AUTHORS: J. M. A. Calero, J. M. M. Perez, J. B. Bernabe, F. J. G. Clemente,

G. M. Perez, and A. F. G. Skarmeta

Nowadays, managers of information systems use ontologies and rules as a powerful tool to express the desired behaviour for the system. However, the use of rules may lead to conflicting situations where the antecedent of two or more rules is fulfilled, but their consequent is indicating contradictory facts or actions. These conflicts can be categorised in two different groups, modality and semantic conflicts, depending on whether the inconsistency is owing to the rule language expressiveness or due to the nature of the actions. While there exist certain proposals to detect and solve modality conflicts, the problem becomes more complex with semantic ones. Additionally, current techniques to detect semantic conflicts are usually not considering the use of standard information models. This paper provides a taxonomy of semantic conflicts, analyses the main features of each of them and provides an OWL/SWRL modelling for certain realistic scenarios related with information systems. It also describes different conflict detection techniques that can be applied to semantic conflicts and their pros and cons. Finally, this paper provides a comparison of these techniques based on performance measurements taken in a realistic scenario and suggests a better approach. This approach is then used in other scenarios related with information systems and where different types of semantic conflicts may appear.

3.PROPOSED SYSTEM

In our article, the data owner propagates an access control list which is stored on the blockchain. Only the authorized users are able to access the data. The contributions of this article are summarized as follows.

1) We propose a secure access control framework to realize data confidentiality, and fine-grained access to data are achieved. This will also guarantee data owners' complete control over their data.
2) We give a detailed description of our PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.
3) To improve data delivery and effectively utilize the network bandwidth, edge devices serve as proxy nodes and perform re-encryption on the cached data. The edge devices are assumed to have enough computation capabilities than the IoT devices and as such provide high performance networking.

3.1 IMPLEMENTATION

Data owner:

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

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:

Cloud server will have Login then server can monitor file details and no owners and user details. And we have one sub module in cloud server I.e proxy. Proxy will reencrypted which is uploaded by data owner. then cloud server will give permissions for the users to access files .

User

In this module, there are n numbers of users are present. User should register before doing some operations . After registration successful he can login by using valid user name and password and location. After Login successful he will do some operations can access data from cloud.

Uses Of Our Approach

Data-centric solution with data protection for the Cloud Service Provider to be unable to access it.

Rule-based approach for authorization where rules are under control of the data owner.

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

Access control computation delegated to the CSP, but being unable to grant access to unauthorized parties.

Secure key distribution mechanism and PKI compatibility for using standard X.509 certificates and keys.

Multi-use. A multi-use scheme enables the proxy to perform multiple re-encryption operations on a single cipher text.

To Provide More Security.

IT makes use of cryptography to protect data when moved to the Cloud. Advanced cryptographic techniques are used to protect the authorization model in order to avoid the CSP being able to disclose data without data owner consent. Concretely, the solution is based on Re-Encryption (RE).

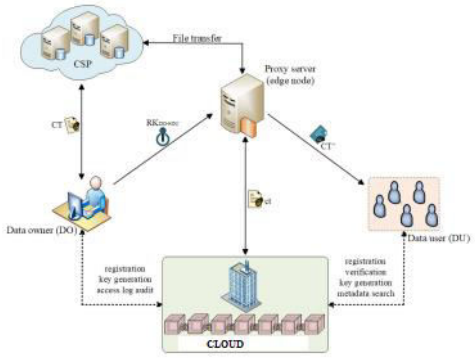

Fig 1:Architecture

4.RESULTS AND DISCUSSION

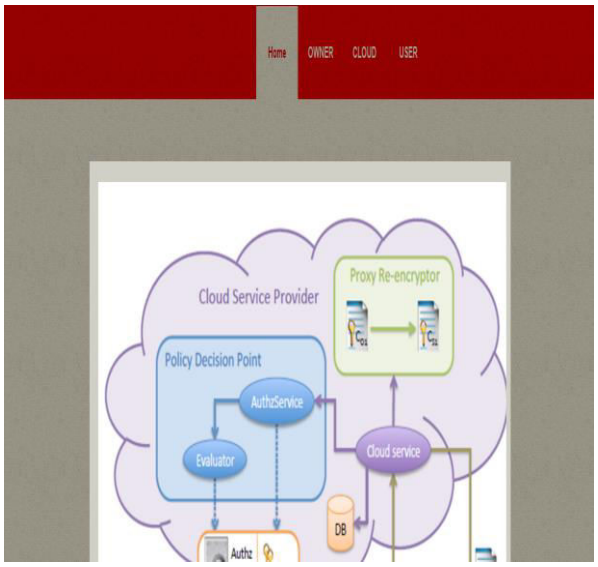

Fig 1:Home Page

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

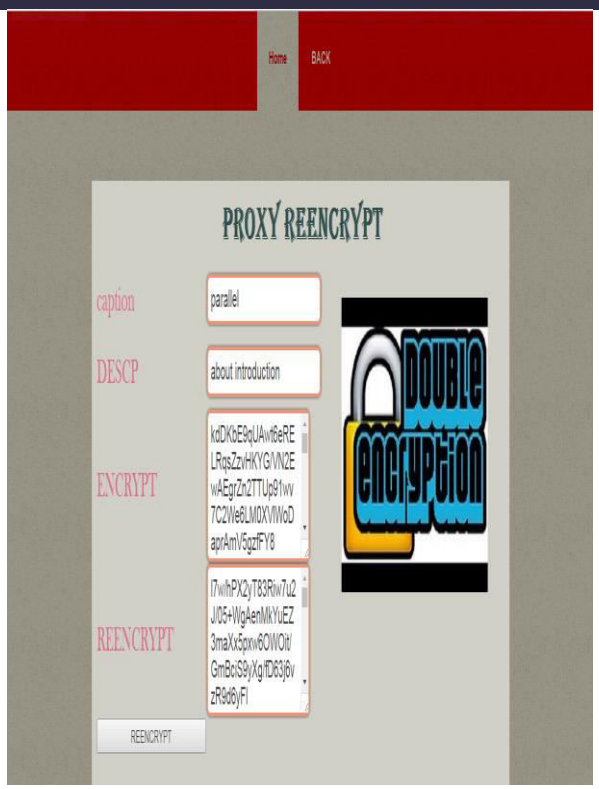

Fig 2:In the above screen we can see re-encrypted data

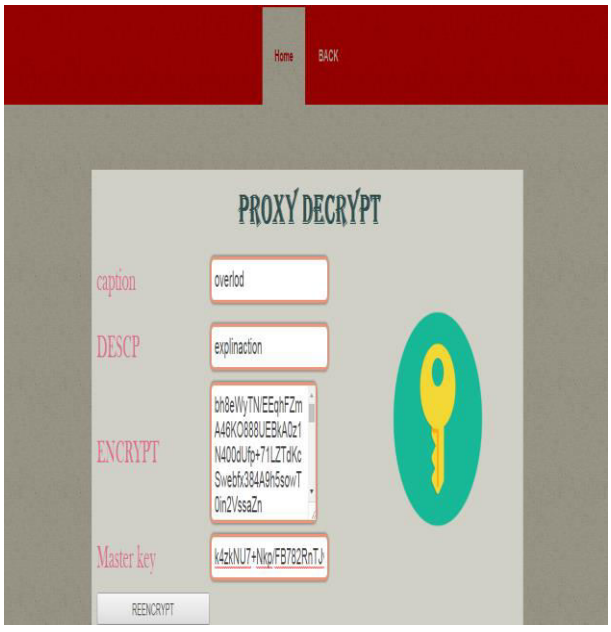

Fig 4:in the above screen use downloading information which was uploading by data owner by using master key

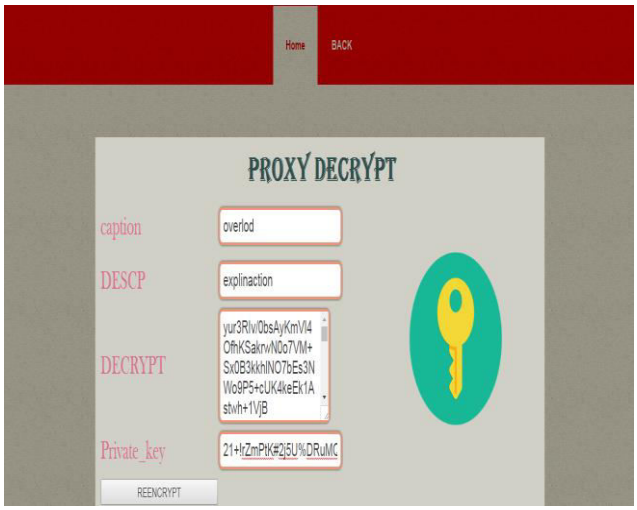

Fig 4:in the above screen use downloading information which was uploading by data owner by using Private key

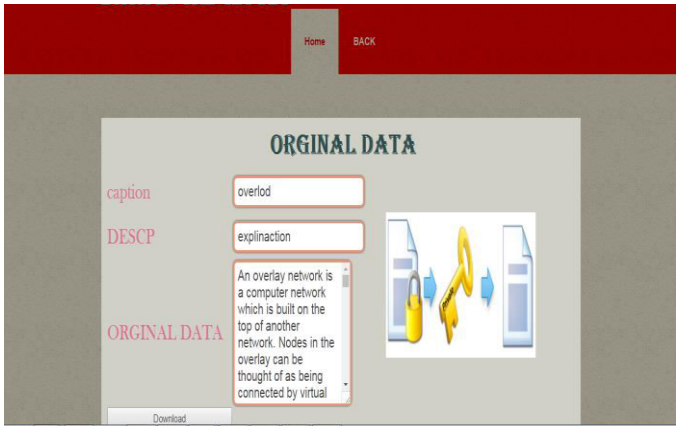

Fig 5:In the above screen we can see decrypted data by providing valid keys

5.CONCLUSION

Data sharing has become one of the IoT's most well-known uses as a result of its development. In a cloud computing environment, we provide a secure identity-based PRE data-sharing mechanism to ensure data confidentiality, integrity, and privacy. The IBPRE technology enables secure data sharing and enables data

owners to effectively share their encrypted data with authorised users while storing it in the cloud. An edge device acts as a proxy to manage the intense calculations due to resource limitations. The plan also makes use of ICN's capabilities to effectively serve cached material, enhancing service quality and optimising network bandwidth. Then, we describe a system paradigm built on a blockchain that enables flexible permission for encrypted data. It is possible to implement fine-grained access control, which can effectively assist data owners in preserving privacy. The analysis and outcomes of the suggested model demonstrate how effective our plan is when compared to other plans.

[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.

[9] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to rolebased access control," Computer, vol. 43, no. 6, pp. 79–81, 2010.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-encryption schemes with applications to secure distributed storage," ACM Transactions on Information and System Security, vol. 9, no. 1, pp. 1–30, 2006.

[11] F. Wang, Z. Liu, and C. Wang, "Full secure identity-based encryption scheme with short public key size over lattices in the standard model," Intl. Journal of Computer Mathematics, pp. 1–10, 2015.

[12] M. Green and G. Ateniese, "Identity-based proxy re-encryption,"in Proceedings of the 5th International Conference on Applied Cryptography and Network Security, ser. ACNS '07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 288–306.

[13] A. Lawall, D. Reichelt, and T. Schaller, "Resource management and authorization for cloud services," in Proceedings of the 7th International Conference on Subject-Oriented Business Process Management,ser. S-BPM ONE '15, New York, NY, USA, 2015, pp. 18:1–18:8.

[14] D. Y. Chang, M. Benantar, J. Y.-c. Chang, and V. Venkataramappa, "Authentication and authorization methods for cloud computing platform security," Jan. 1 2015, uS Patent 20,150,007,274.

[15] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets:A practically motivated enhancement to attribute-based encryption," in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 587–604.

[16] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM Conference on Computer and Communications Security, ser. CCS '10, New York, NY, USA, 2010, pp. 735–737.

AUTHOR PROFILES

Miss. Gangaraju Suresh Chandana, M. Tech student in the department of CSE at CHADALAWADA RAMANAMMA ENGINEERING COLLEGE, Tirupathi. She has completed B. E in Electronics &Communication Engineering from MEENAKSHI SUNDARARAJAN ENGINEERING COLLEGE, Affiliated to ANNA University, Chennai. Her areas of interests are Networks Security & Internet of Things.

.

Ms. E.STUTHI completed her Bachelor of Technology in Computer Science and Engineering. She completed her Masters of Technology in Computer Science and Engineering. She has published more than 2 papers in international Journals. Currently working as an Assistant Professor in the department of CSE at CREC (Autonomous), Tirupathi. Her areas of interest include, Network security, Computer Networks and Artificial Intelligence.