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

[1]Kankati Hema , [2]P.Sathish

[12] Vaageswari College of Engineering, Karimnagar, Telangana, India

[1]hemakankati22@gmail.com [2]polu.sathish99@gmail.com

Abstract : As the Internet of Things has grown, data sharing has become one of the most beneficial cloud computing applications. Even though this technology has a pleasing aesthetic, data security is still one of its difficulties because inappropriate data utilisation might have a number of unfavourable impacts. In this research, we present a proxy re-encryption technique for secure data transfer in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, and authorised users can access the data through proxy re-encryption construction. Because Internet of Things devices have limited resources, an edge device acts as a proxy server to conduct computationally intensive tasks. Additionally, by utilising information-centric networking capabilities, we successfully distribute cached content through the proxy, hence boosting the quality of service and effectively utilising the network capacity. It accomplishes fine-grained data access control and lessens centralised system bottlenecks. Our strategy for ensuring data security, confidentiality, and integrity has the potential, as shown by the security study and plan review.

1.INTRODUCTION

It's become clear that the Internet of Things (IoT) is a technology of critical importance to the world right now, and its implementation has led to a meteoric increase in the volume of business conducted across networks. It is expected that much prejudice will become interconnected in the future. Information is essential to the IoT paradigm because it can be used in a wide variety of settings, including but not limited to healthcare, transportation networks, smart cities, industry, and manufacturing (1). The sensors collect data on a wide variety of factors that have real-world applications. The development of IoT has, therefore, posed new obstacles to security and insulation, despite how appealing it may seem.

Attacks that prevent IoT from providing the requested services are just as important to protect against as those that endanger data privacy, integrity, and availability. Counting the information yourself before sending it to the pallbearers is a reasonable outcome to expect. When the usual safeguards fail, the attacker can only see the data in its restated version. In order to preserve confidentiality, when exchanging data, every information must be rephrased directly from the source and only decrypted by approved stoners. The data owner may choose to utilise conventional encryption methods, in which case the decryption key will be shared among all the data stoners. Using symmetric encryption means that the data owner and stoners either share the same key or agree on a key to use for encryption. We are seriously limited by this outcome. Similar to how data owners can't predict who will be interested in their data, restated data must be decrypted and then restated using a key that is shared between the data owner and the data stoners. The data's owner would need constant Internet access in order to decode and encipher the information, which is practically impossible. When more data are involved, as well as when different data owners and drug users are engaged, the complexity of the issue decreases. Simple as they may be, classic encryption methods necessitate complex operational processes and should not be used for transferring sensitive information. Blaze et al.(2) introduced the idea of proxy re-encryption (PRE), which allows a delegate to re-encrypt a stream that was originally encrypted using the delegator's public key. We recommend that the data's owner take on the role of delegator and the data's stoner take on the role of delegate. The data owner may use this scheme to give the stoner translated communications while protecting his private key. Data encryption keys can be generated either by the data's owner or a trusted third party. Before giving the stoner the revised ciphertext, the deputy updates it using their own encryption method and the key. It is inherent to a PRE scheme that the deputy is unaware of the secret key employed by the data owner. As a crucial part of any data-participating script, this is a leading contender for safely granting access to localised data..

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.

The rise of cloud computing has been one of the most significant developments in the field of information technology in recent years. Despite its apparent benefits, this paradigm introduces a number of new challenges for data security because users are forced to trust cloud servers with their most private information. To protect the privacy and integrity of shared data in the cloud, we propose a Flexible and Efficient Access Control Scheme (FEACS) based on Attribute-Based Encryption, which is well suited for granular access control. FEACS has advantages over the state-of-the-art due to its following features. One of FEACS's strongest points is its ability to deal with dynamic membership, which is especially important in a cloud environment where user roles can and do frequently shift. Second, it makes perfect sense.

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

Due to the remarkable development of data exchange in network environments and growing attacker capabilities, information security has emerged as the most important process for data storage and transfer. Such information security requires the use of cryptographic encryption techniques to verify the confidentiality, integrity, and authentication of the data's origin. In this paper, we introduce the advanced encryption standard (AES) algorithm, the most well-known form of symmetric encryption. The primary objective of this development is to establish a bridge between the AES-based S-Boxes we've been making and the one-of-a-kind secret keys coming out of our quantum key distribution.

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.

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).

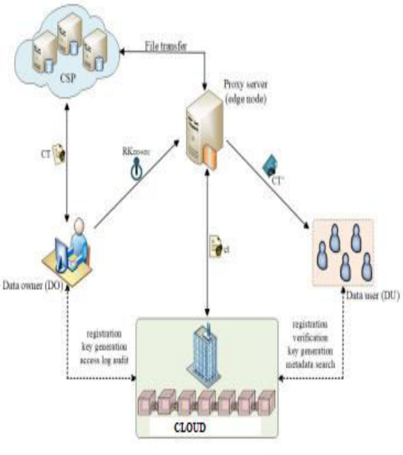


Fig 1:Architecture

4.RESULTS AND DISCUSSION

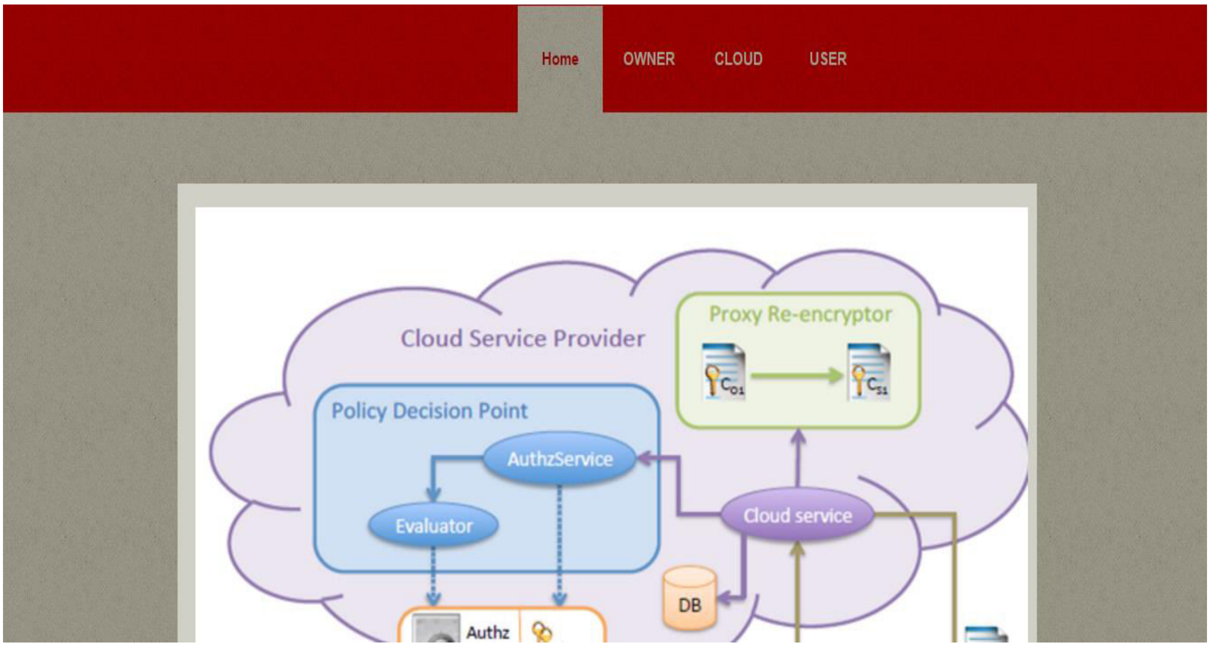
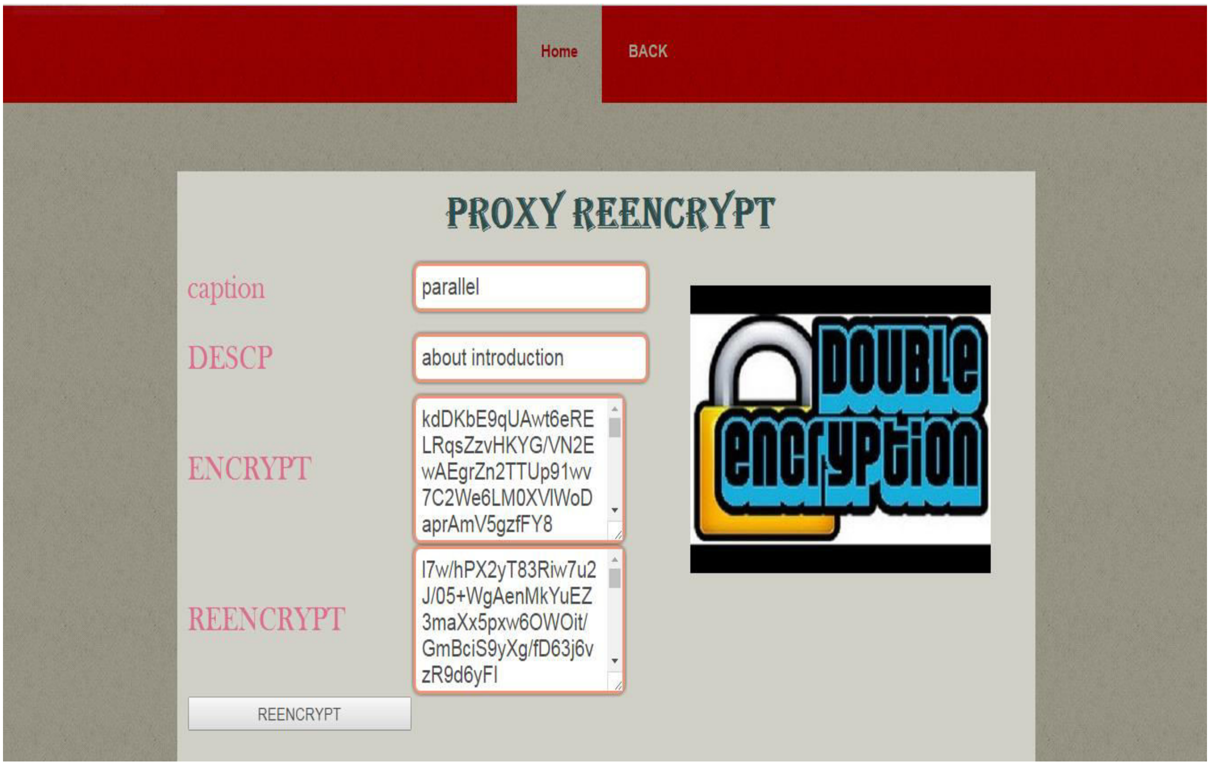


Fig 1:Home Page



PROXY REENCRYPT

caption parallel

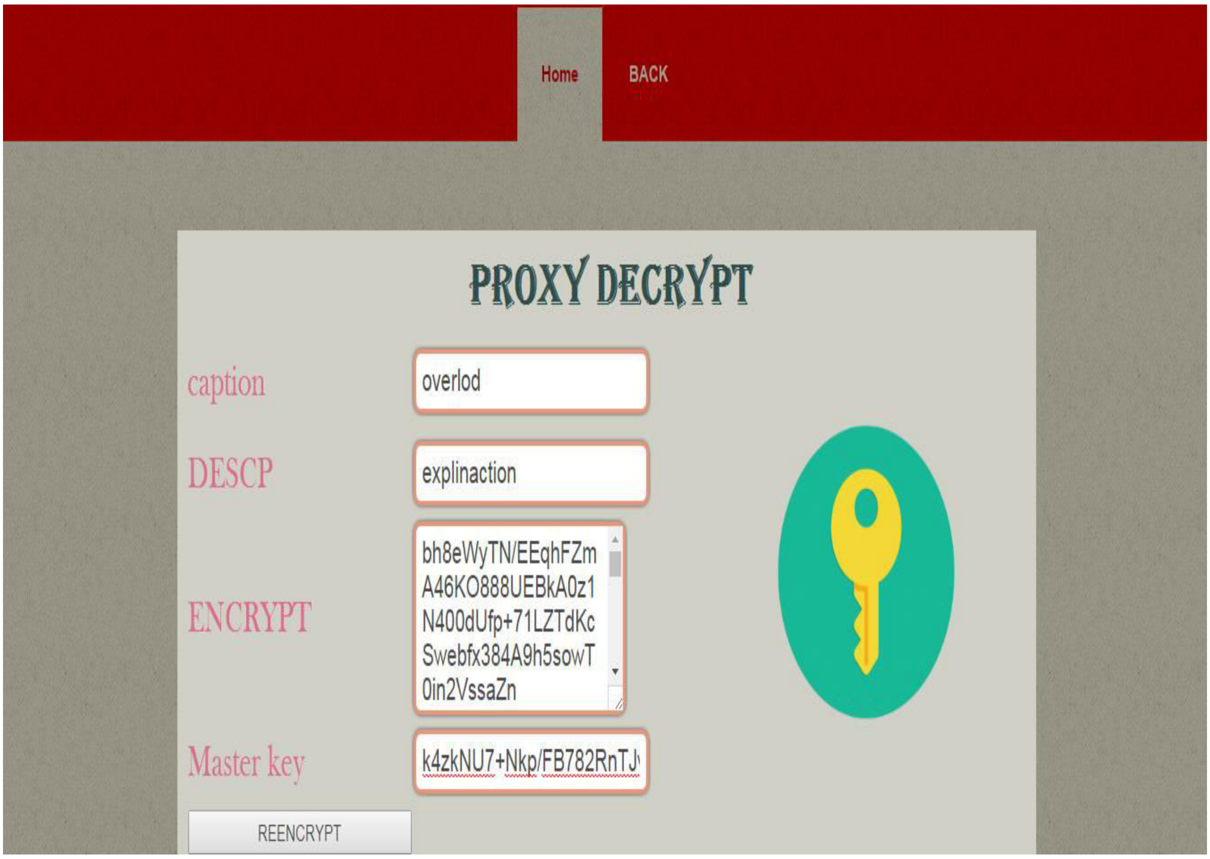
DESCP about introduction

ENCRYPT
kdDKbE9qUAwt6eRE
LRqsZzvHKYG/VN2E
wAEgrZn2TTUp91wv
7C2We6LM0XVlWoD
aprAmV5gzfFY8

REENCRYPT
l7w/hPX2yT83Riw7u2
J/05+WgAenMkYuEZ
3maXx5pxw6OWOit/
GmBciS9yXg/fD63j6v
zR9d6yFl

REENCRYPT

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



PROXY DECRYPT

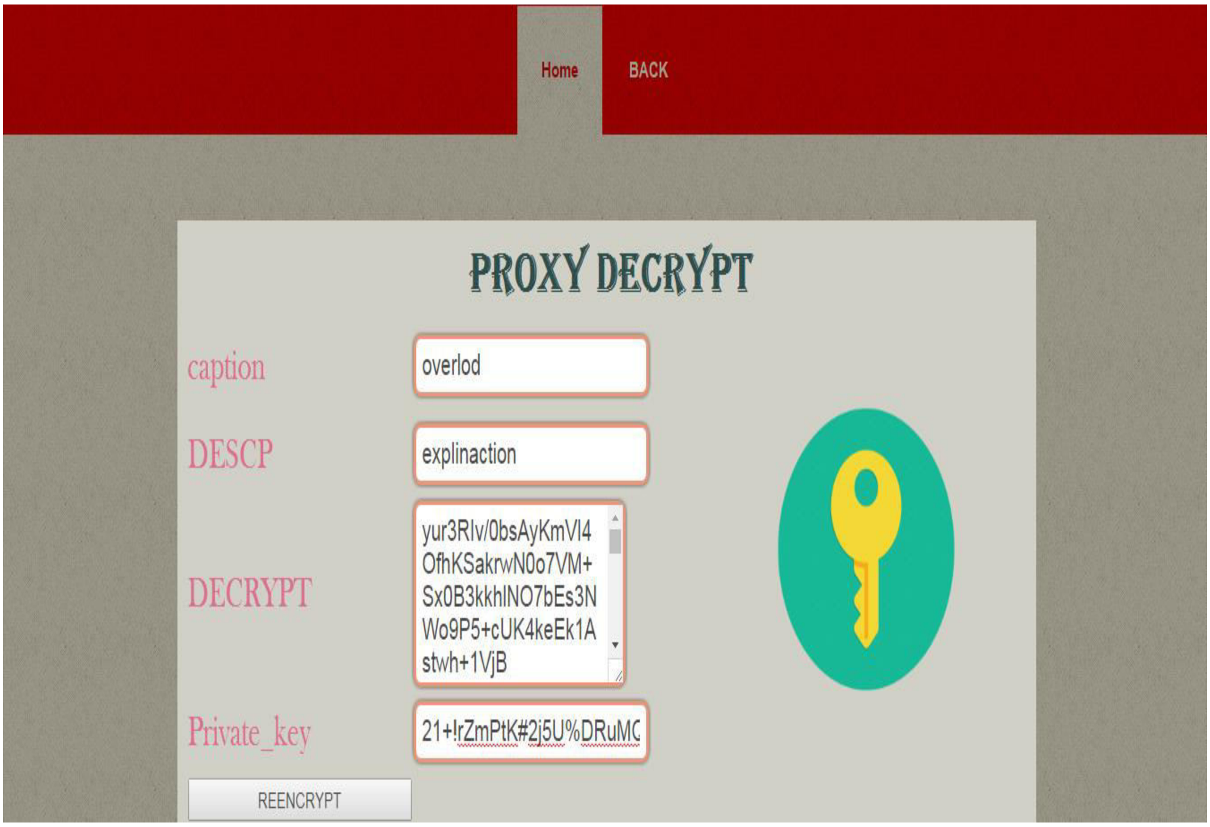
caption: overlod

DESCP: explinaction

ENCRYPT: bh8eWyTN/EEqhFZmA46KO888UEBkA0z1N400dUfp+71LZTdKcSwebfx384A9h5sowT0in2VssaZn

Master key: k4zkNU7+Nkp/FB782RnTJ

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



PROXY DECRYPT

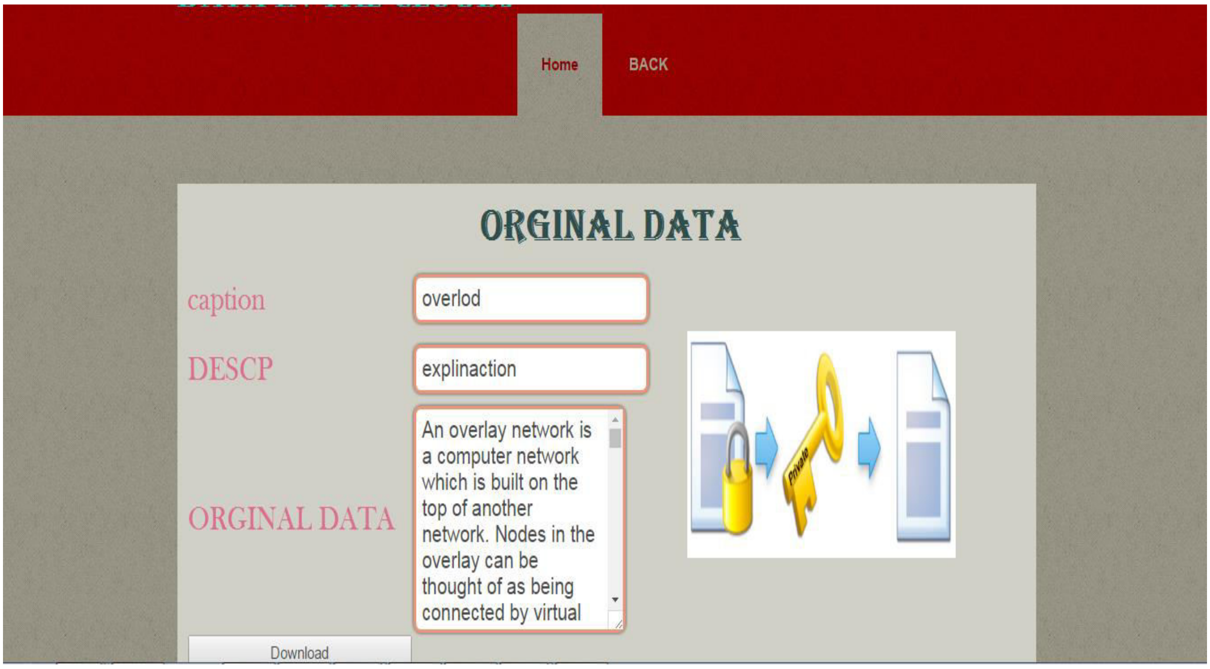
caption overlod

DESCP explinaction

DECRYPT yur3RIv/0bsAyKmVI4
OfhKSakrwN0o7VM+
Sx0B3kkhINO7bEs3N
Wo9P5+cUK4keEk1A
stwh+1VjB

Private_key 21+!rZmPtK#2j5U%DRuMC

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



ORGINAL DATA

caption overlod

DESCP explinaction

ORGINAL DATA An overlay network is a computer network which is built on the top of another network. Nodes in the overlay can be thought of as being connected by virtual

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

5.CONCLUSION

IoT's proliferation means that data exchange is now a core feature. We present a secure identity-based PRE data-sharing mechanism in a cloud computing setting, ensuring the confidentiality, integrity, and privacy of shared data. The IBPRE method enables data owners to securely store their encrypted data in the cloud and conveniently distribute it with authorised users. Given the limited capacity of the core network nodes, an edge device acts as a proxy to do the demanding calculations. The method also makes use of ICN's characteristics to effectively provide cached content, which boosts service quality and makes efficient use of available network capacity. Then, we introduce a model of a blockchain-based system that provides authorization on encrypted data with some wiggle room. Achieving fine-grained access control can aid data owners in performing effective privacy protection. The proposed model's study and results demonstrate the superior efficiency of our system over other schemes.

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.

[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.