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

1. **Patchala Usha pola Visweswari, Assistant Professor, Department of Computer Science and Engineering,Ideal institute of technology, Kakinada Email:pola.usha21@gmail.com**

2. **Boyapati BhagyaLakshmi , Assistant Professor, Department of Computer Science and Engineering,Ideal institute of technology,Kakinada.**

Email: lakshmi.boyapatibhagya@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:

1.1 About Cloud Computing:

Distributed computing is the utilization of figuring assets (equipment and programming) that are conveyed as a help over a system (regularly the Internet). The name originates from the basic utilization of a cloud-moulded image as a reflection for the mind boggling framework it contains in framework graphs. Distributed computing endows remote administrations with a client's information, programming and calculation. Distributed computing comprises of equipment and programming assets made accessible on the Internet as oversaw outsider administrations. These administrations normally give access to cutting edge programming applications and very good quality systems of server PCs.

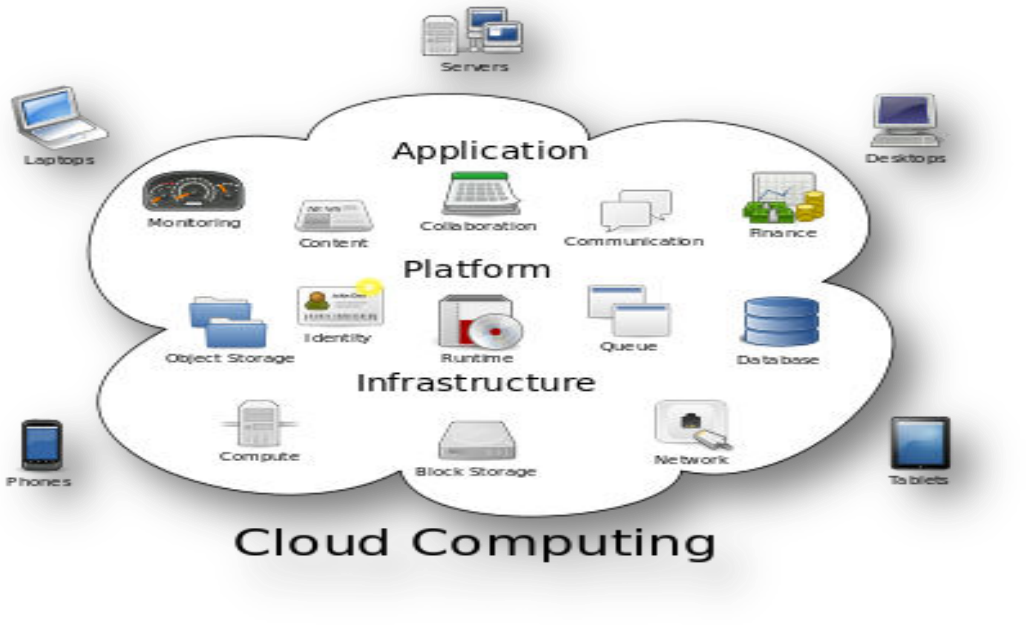

Fig.1.1: Structure of cloud computing

1.2.Cloud Computing Working: The objective of distributed computing is to apply customary supercomputing, or superior processing power, regularly utilized by military and research offices, to perform several trillions of calculations for each second, in buyer arranged applications, for example, money related portfolios, to convey customized data, to give information stockpiling or to influence huge, vivid PC games.

The distributed computing utilizes systems of enormous gatherings of servers commonly running ease purchaser PC innovation with particular associations with spread information preparing tasks crosswise over them. This common IT foundation contains huge pools of frameworks that are connected together. Frequently, virtualization systems are utilized to amplify the intensity of distributed computing.

1.3.Attributes Of Cloud Computing:

The remarkable attributes of distributed computing dependent on the definitions gave by the National Institute of Standards and Terminology (NIST) are sketched out underneath

On-request self-administration: A purchaser can singularly arrangement registering abilities, for example, server time and system stockpiling, as required naturally without requiring human connection with each specialist organization's.

Broad organize get to: Capabilities are accessible over the system and got to through standard instruments that advance use by heterogeneous slim or thick customer stages (e.g., cell phones, PCs, and PDAs).

Resource pooling: The supplier's processing assets are pooled to serve numerous buyers utilizing a multi-occupant model, with various physical and virtual assets progressively doled out and reassigned by purchaser request. There is a feeling of area autonomy in that the client for the most part has no control or information over the accurate area of the gave assets however might have the option to indicate area at a more significant level of reflection (e.g., nation, state, or server farm). Instances of assets incorporate stockpiling, preparing, memory, organize transfer speed, and virtual machines.

2. LITERATURE SERVEY:

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

Joseph Bonneau, Cormac Herley, said that the theory on passwords has lagged behind practice, where large providers use back-end smarts to survive with imperfect technology. Simplistic models of user and attacker behaviors have led the research community to emphasize the wrong threats. Authentication is a classification problem amenable to machine learning, with many signals in addition to the password available to largeWeb services. Passwords will continue as a useful signal for the foreseeable future, where the goal is not impregnable security but reducing harm at acceptable cost.

Ch Gopal Krishna and R Bala Dinakar, This development brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this tricky, we proposed a novel authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login pointer and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks.

Mr. Rudresh Gurav , Ms. Leena Dabhade, To increase password security, online authentication systems have started to enforce stricter password policies. We introduce a new metric called Coverage to quantify the correlation between passwords and personal information. Personal-PCFG cracks passwords much faster than PCFG and makes online attacks much more likely to succeed. We examine the use of simple distortion functions that are chosen by users to mitigate unwanted correlation between personal information and passwords. To increase password security, online authentication systems have started to enforce stricter password policies. Password re-generation method is available in this system.

3. EXISTING SYSTEM:

Several data-centric techniques, largely based on Attribute-based Encryption (ABE), have evolved for data protection in the Cloud. In ABE, the data owner assigns a set of labels to the encrypted ciphertext. The private keys of users also define a set of characteristics. If the ciphertext and key properties are a good match, the user can decode the data.An access structure, often shown as a tree with AND and OR nodes, specifies the set of attributes a user must possess in order to decode the data. According to the location of the access structure, Key-Policy ABE (KP-ABE) and Cipher text-Policy ABE are the two primary methods for implementing ABE (CP-ABE).

Users' private keys determine the KP-ABE protocol's access structure or policy. Using this method, we can encrypt data that has been annotated with attributes, and then manage who has access to this data by providing them with the right encryption keys. This time around, though, it's not the data encryption, or owner, but the key issuer, who defines the policy. Therefore, the data owner must have faith in the key issuer to create a sufficient access policy.

To tackle this issue, CP-ABE offers to integrate the access structure within the cipher text, which is under control of the data owner. The issuer of a key need only assert user attributes by encoding them within a private key. However, the expressiveness of the access control policy is restricted to AND and OR combinations of characteristics in both KP-ABE and CP-ABE.

3.1Drawbacks:

When information is encrypted, un authorised users are denied access. But it also brings up some fresh challenges in terms of administering access controls.

To the best of our knowledge, no data-centric approach exists that offers an RBAC model for access control in which data is encrypted and self-protected.

The current hierarchical method assumes that all attributes should be administered by the same top-level authority. All permissions granted to a user are fully separate from their private key. In

conclusion, present ABE systems do not provide a user-centric approach to authorising business activities.

4. PROPOSED SYSTEM:

This work introduces Sec RBAC, an extension of Role-Based Access Manage that is data-centric and can be used on untrusted CSPs to control access to self-protected data.

With the suggested authorization system, access to resources may be managed more easily thanks to a role-based, rule-based approach that closely follows the RBAC scheme.

The proposed solution primarily contributes in the following ways:

If you want to ensure that your Cloud Service Provider can't access any of your data, you'll need a data-centric solution with data security. Authorization based on a set of predetermined rules that are managed by the owner of the underlying data. The RBAC scheme, which includes a role hierarchy and a resource hierarchy, allows for highly expressive authorization rules (Hierarchical RBAC or hRBAC). Delegating the calculation of access control to the CSP while maintaining the ability to deny access to unapproved users.

4.1Advantages:

This study presents an alternative to the ABAC model in the form of a proposal for a data-centric RBAC method. In order to manage the complexities of access control in the Cloud, this method can be useful for regulating and controlling security.

By allowing privilege propagation across roles and hierarchies, the authorization model makes it possible to define simple but powerful rules that apply to multiple people and resources, therefore increasing the model's expressiveness.

By utilising Semantic Web technologies, policy rule specifications may be made that allow for enhanced rule definitions and sophisticated policy management capabilities, such as conflict detection.

4.2 IMPLEMENTATION:

Data owner:

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

Cloud Server:

The cloud server will have a login sothat it may monitor file information without knowing the owners' or users' details. Additionally, the cloudserver has a submodule called proxy.Proxy that is

uploaded by the data owner will be encrypted. then, the cloud server will grant users accessto files..

User:

There are n numbers of users presentin 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 ServiceProvider to be unfit to pierce it.Rule- grounded approach forauthorization where rules are under control of the data proprietor. High expressiveness forauthorization rules applying the RBAC scheme with part scale and resource scale(Hierarchical RBACor hRBAC).

Access control calculation delegatedto 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 multiplier-encryption operations ona single cipher textbook. To give further Security.IT makes use of cryptography to cover data when moved to the Cloud. Advanced cryptographicways are used to cover the authorization model in order to avoidthe CSP being suitable to expose data without data proprietorconcurrence. Primarily, the result is grounded on Re-Encryption (shaft).

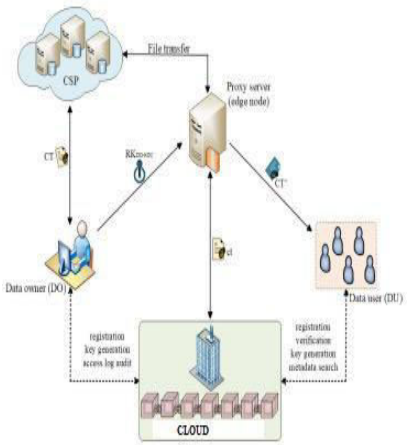

Fig 4: Architecture

5. RESULTS AND DISCUSSION:

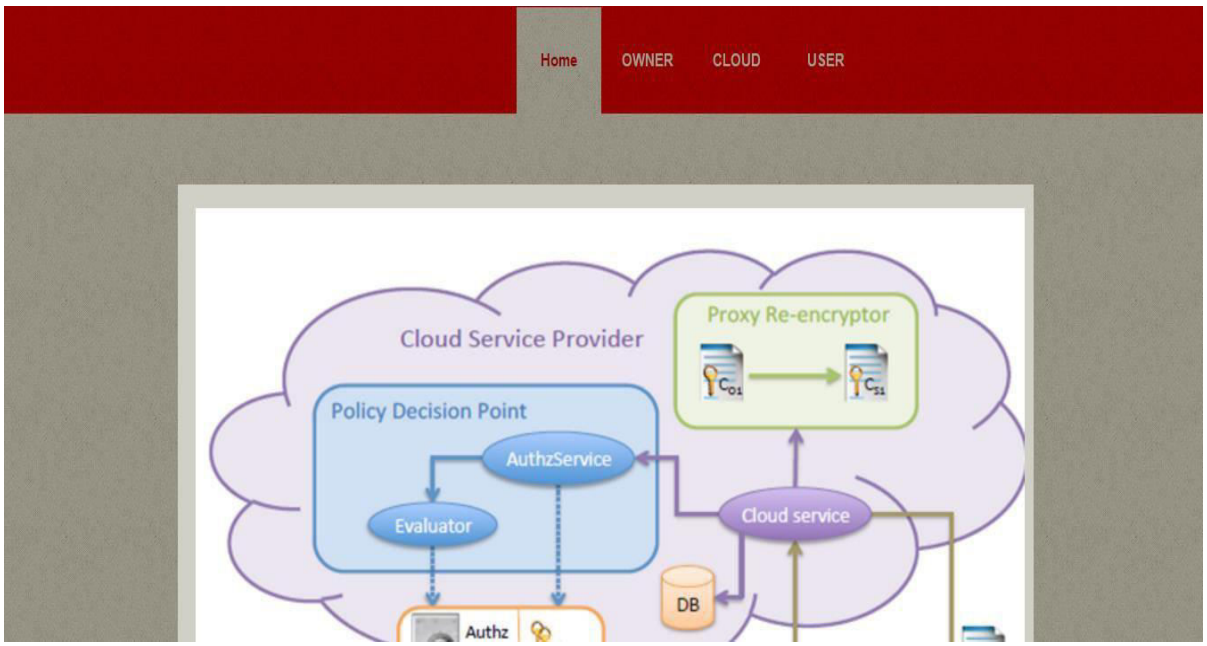

Fig 1:Home Page

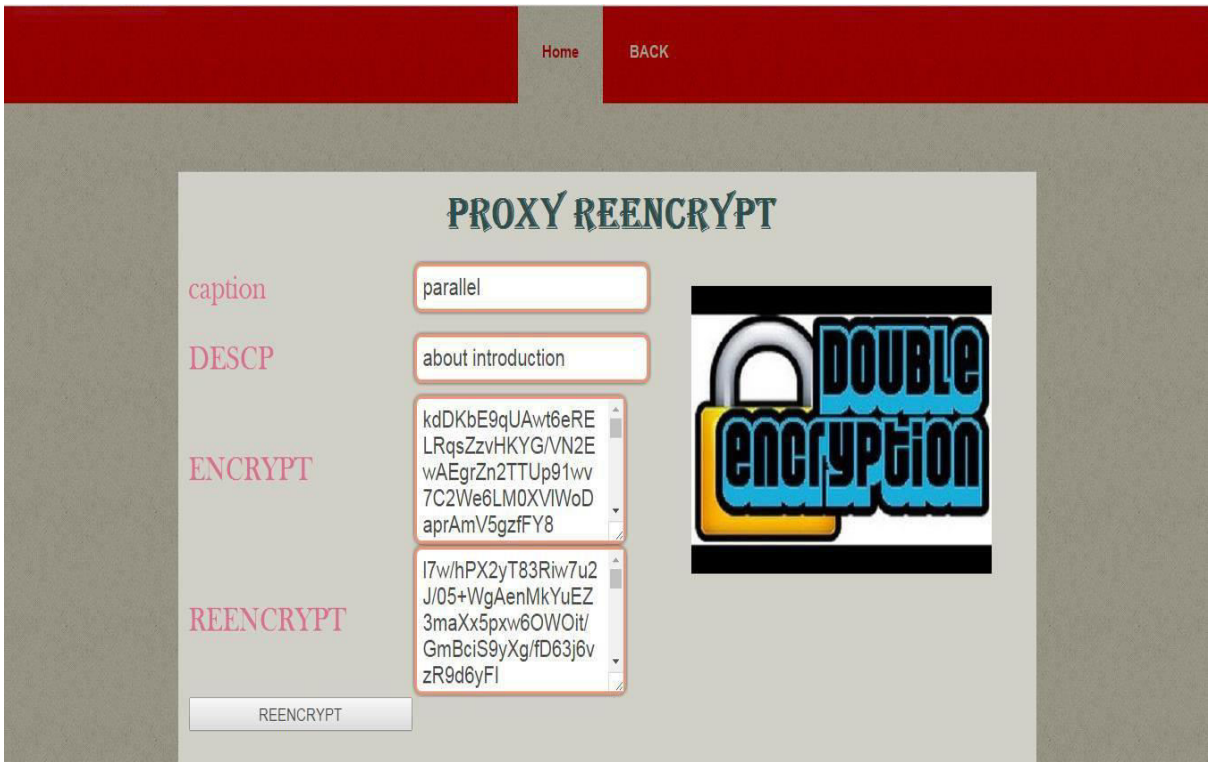

Fig 2: In the above screen we can see re-encrypted data

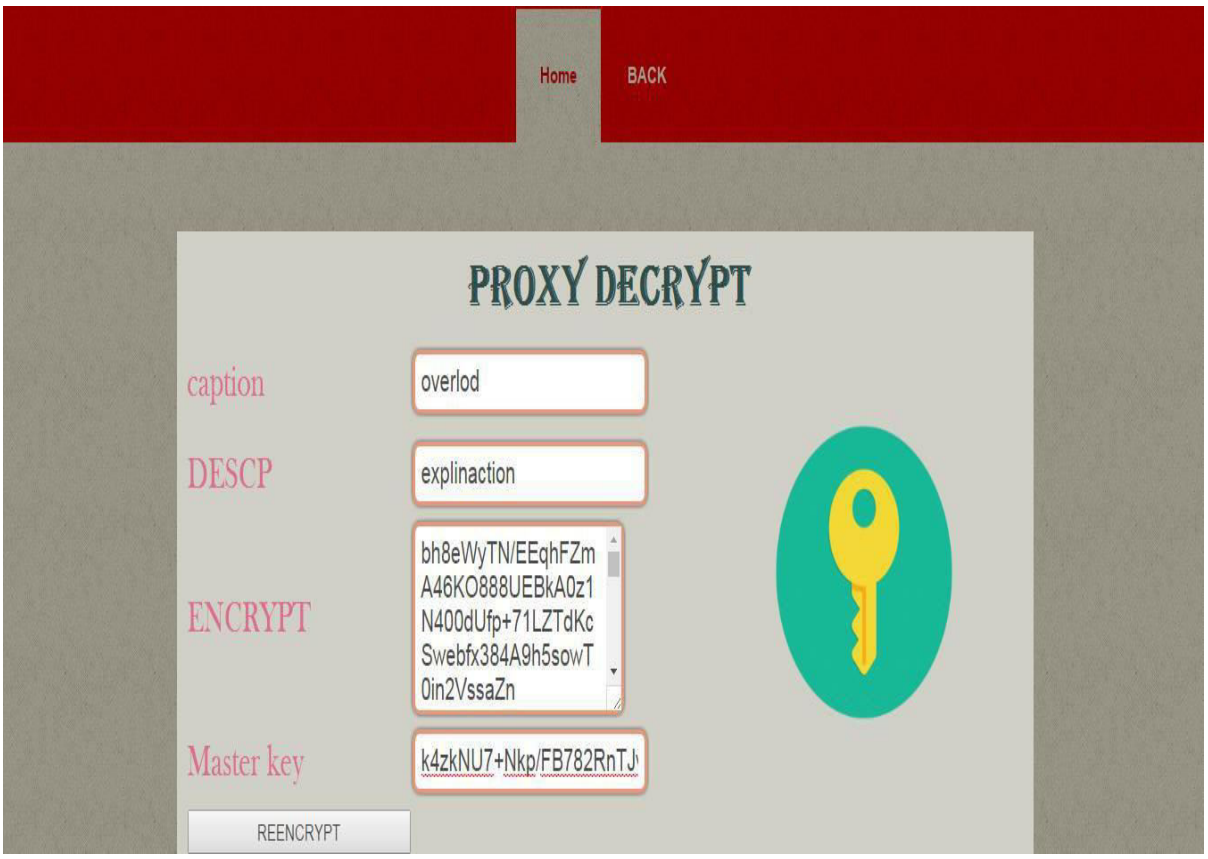

Fig 4:in the above screen use downloading information which was uploading by data owner by using master key

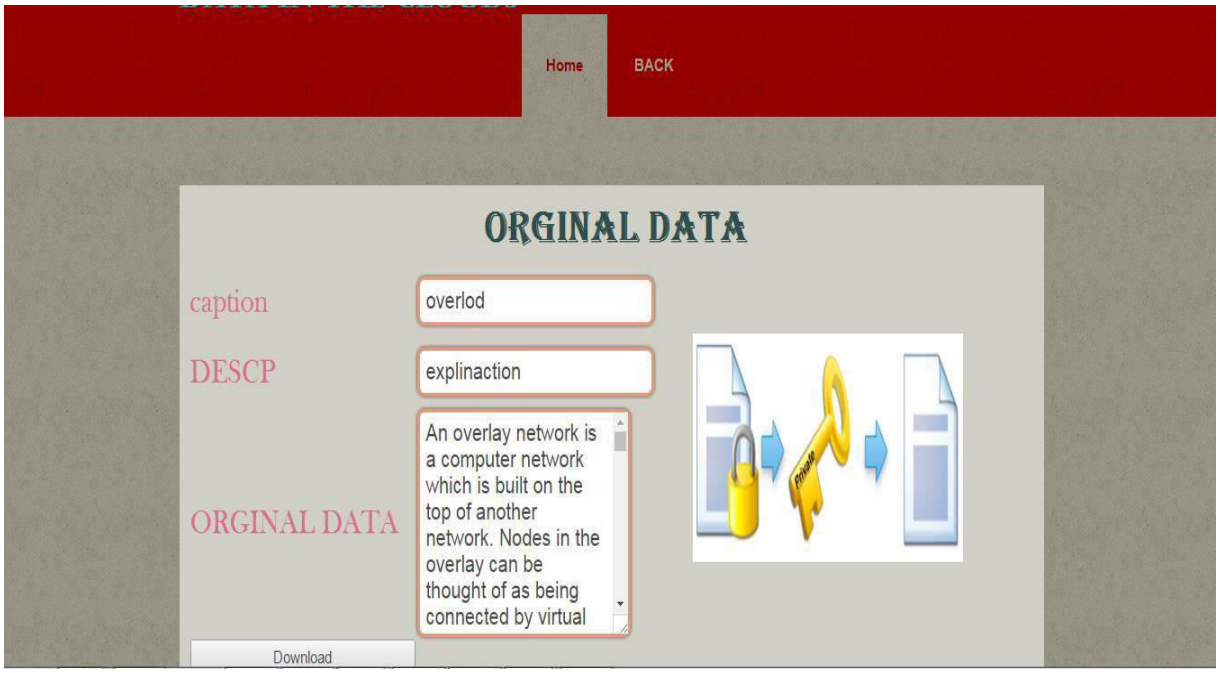

Fig 5 :In the above screen we can see decrypted data by providing valid keys

6.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. Then, we present a block chain-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.

7.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.

[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.

[17] J. Liu, Z. Wan, and M. Gu, “Hierarchical attribute-set based encryption for scalable, flexible and fine-grained access control in cloud computing,” in Information Security Practice and Experience. Springer Berlin Heidelberg, 2011, vol. 6672, pp. 98–107.

[18] W3C OWL Working Group, “OWL 2 Web Ontology Language: Document overview (second edition),” World Wide Web Consortium (W3C), W3C Recommendation, Dec. 2012.

[19] J. M. A. Calero, J. M. M. Perez, J. B. Bernabe, F. J. G. Clemente,G. M. Perez, and A. F. G. Skarmeta, “Detection of semantic conflicts in ontology and rule-based information systems,” Data & Knowledge Engineering, vol. 69, no. 11, pp. 1117 – 1137, 2010.

[20] W3C OWL Working Group, “OWL 2 Web Ontology Language: Profiles (second edition),” World Wide Web Consortium (W3C),W3C Recommendation Dec. 2012.

[21] ——, “SPARQL 1.1 overview,” World Wide Web Consortium (W3C), W3C Recommendation, Mar. 2013.

[22] R. Housley, “Cryptographic message syntax (CMS),” Internet Engineering Task Force (IETF), RFC 5652, Sep. 2009.

[23] E.-J. G. Dan Boneh and T. Matsuo, “Proposal for p1363.3 Proxy Re-encryption,” Aug. 2006.

[24] O. K. J. Mohammad, S. Abbas, E. M. El-Horbaty, and A. M.Salem, “Innovative method for enhancing key generation and management in the aes-algorithm,” CoRR, vol. abs/1504.03406, 2015.

authorization model in order to avoidthe CSP being suitable to expose data without data proprietor concurrence. Primarily, the result is grounded onRe-Encryption(shaft).

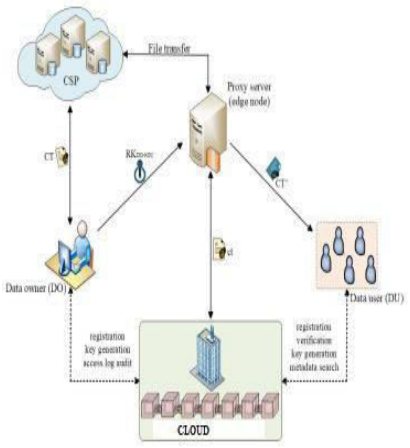

Fig 1:Architecture

1. RESULTS AND DISCUSSION