A Review on Document Privilege Access

[1]Miss. S.V.Sarode, [2]Prof. M.B.Wagh
[1]PG student, [2]Assi. Professor
[1]Computer Engineering Department,
[1]SVIT, Chincholi, Sinner, Nashik, India

***Abstract*— Cloud storage is an efficient way to store and maintain user's data. With data storage cloud provides appropriate storage management, data sharing, data maintenance etc. Recently, users survived from cloud misbehave services as it breaks the organization bounds. Due to this user loses control over their data & it raises the security issues which slow down the confirmation of cloud computing. In this paper we presents SecRBAC, a data-centric access control solution for self-protected data that can run in untrusted CSPs and provides extended Role-Based Access Control expressiveness. The proposed authorization solution provides a rule-based approach following the RBAC scheme, where roles are used to ease the management of access to the resources. Proxy-re-encryption technique is used to protect authorization model. Proposed solution enables the semantic conflict detection. Implementation concept is the type of prototypical deployment and it is combined with Google services.**

***IndexTerms*— Data-centric security, Cloud computing, Role-based access control, Authorization**

I. INTRODUCTION

A data-centric access control solution for self-protected data that can run in untrusted CSPs and provides extended Role-Based Access Control expressiveness is discussed in[1]. It provides a rule-based approach following the RBAC scheme, where roles are used to ease the management of access to the resources. This approach can help to control and manage security and to deal with the complexity of managing access control in Cloud computing. A data centric approach is used for self protection in which some novel cryptographic techniques are used such as, PRE (Proxy-Re-encryption), IBE (Identity Based Encryption) and IBPRE (Identity Based Proxy Re-encryption). This technique allows re-encrypt data from one key to another without getting access & to use identities in cryptographic operations, it also allows protecting both data and authorization model. Each piece of data is ciphered with its own encryption key linked to the authorization model and rules are cryptographically protected to preserve data against the service provider access or misbehavior when evaluating the rules. It also combines a user-centric approach for authorization rules, where the data owner can define a unified access control policy for his data. A rules-based approach can use for user authorization in which rules are under the control of data owner and access control computations is outsourced to the CSP. From an authorization point of view, this can be seen as a simple rule where only the user with privilege to access the data will be able to decrypt it (i.e. the one owning the key). However, no access control expressiveness is provided by this approach. Only that simple rule can be enforced and just one single rule can apply to each data package. Thus, multiple encrypted copies should be created in order to deliver the same data to different receivers. Problem to generate more data copies that can be further delivered to other receiver. To cope with this issue SecRBAC utilized a data centric approach. Existing schemes are Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE).Then, the key issuer just asserts the attributes of users by including them in private keys. However, either in KP-ABE or CP-ABE, the expressiveness of the access control policy is limited to combinations of AND-ed or OR-ed attributes. RBAC may require the definition of a large number of roles for fine-grain authorization (role explosion problem in RBAC). ABAC is also easier to set up without need to make an effort on role analysis as needed for RBAC.On another hand, ABAC may result in a large number of rules since a system with n attributes would have up to 2 n possible rule combinations (rule explosion problem in ABAC). ABAC separates authorization rules from user attributes, making it difficult to determine permissions available to a particular user, while RBAC is deterministic and user privileges can be easily determined by the data owner.In this final conclusion of related work is that, no user-centric approach for authorization rules is provided by current ABE solutions.In proposed SecRBAC approach a single access control policy defined by data owner can protect more than one piece of data.

II. RELATED WORK

A.Lawall, D. Reichelt et al. [1], proposed an approach to request the automatic deployment of resources from a cloud provider. The access rights to the resources are managed and administered by the proprietary company, even if partner organizations are involved. This allows for the consistent definition of permissions, dynamic roles etc. across all connected systems. In this paper Service Provisioning Markup Language (SPML) approach provides proof of validity. It can be attempted to map the deployment requests generated by this approach to structures defined in SPML. In this paper attribute authorization of requested system might be invalid and it is defined as future scope.

V. Goyal, O. Pandey et al. [2], developed a cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In proposed cryptosystem ciphertexts are labeled with sets of attributes and private keys

are associated with access structures that control which ciphertexts a user is able to decrypt. Author demonstrate that the applicability of their construction to sharing of audit-log information and broadcast encryption. The development supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE). In this paper, they leave the problem of hiding the set of attributes as open.

Balamurugan B and Venkata Krishna P [3], made survey of ABE i.e. attribute based encryption schemes. Cloud application deployment depends on several factors like load balancing, bandwidth, data size and security. Access into the cloud environment is determined by the access control techniques provided by the cloud service provider. A weak access control technique will lead to several attacks like insider attacks, collusion attack, and denial of service attacks. It is necessary for a cloud environment to have an access control policy to give fine grained and scheduled access to users. There are several access control policies available for cloud computing ranging from Discretionary access control (DAC), Mandatory Access control (MAC), Role based access control (RBAC) and Attribute based encryption access control (ABAC). Each of these access control has been designed for policy neutral, administrative convenient access design .The imperative properties of DAC and MAC are combined together to get RBAC. While DAC is user discretionary, MAC is based on lattices. In this paper the comparison table of various ABE based schemes based on various features such as computation overhead, decryption and user revocation efficiency, collusion resistant, application relevancy, association of attributes and association of access policy in a five scale rating form is given.

B.Waters [4], represented a new methodology for realizing CP-ABE i.e. Ciphertext-policy Attribute Encryption. It is under the concrete and non-interactive cryptographic assumptions. The proposed methodology of embeddings LSSS challenge matrix directly into the public parameters. In this paper three constructions are proposed, first is the system proven selectively secure under assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. And the next two constructions provide performance tradeoffs to achieve provable security respectively.

R. Bobba, H. Khurana et al. [5], proposed Ciphertext-Policy ABE (CP-ABE) scheme. It is the form of ABE where policies are associated with encrypted data & attributes are associated with keys. With this work they focused on improving the flexibility of representing users attribute in key. In this paper author defined a future work design of efficient CP-ASBE schemes that are secure in the standard model and extending CP-ASBE to a multi-authority setting.

G. Wang, J. Wu [6], discussed about the scheme to help enterprises s to efficiently share confidential data on cloud servers. To perform this task, HIBE, hierarchical identity based encryption technique is implemented and the Ciphertext Policy Attribute Based Encryption (CP-ABE). In final process they applied Proxy-reencryption and lazy re-encryption techniques to developed scheme. In future work they were mentioned that to design more expressive scheme, which can be proved to have full security under the standard model with best performance.

N.krishna and L.Bhavani [7], proposed Hierarchical Attribute Set Based Encryption (HASBE). It is implemented using cipher text policy by encrypting and decrypting the data in the cloud therefore, cloud system become more flexible and scalable by enforcing data owners to share their data with data consumers controlled by the domain authority.

D. Richard Kuhn, E. Coyne [8], discussed about Role-Based Access Control Models. It is mostly known as, “RBAC”. A pure RBAC technique provides inadequate support for dynamic attributes such as time of day, which might need to be considered when determining user permissions. An appropriate trade-off retains the benefits of RBAC while extending its utility into distributed application. RBAC control model includes the attribute in access control model.

E. Coyne and T. Weil, [9], discussed about ABAC & RBAC schemes. ABAC and RBAC although similar, have particular advantages and disadvantages. When combined judiciously, the combination can provide access control that’s scalable, flexible, auditable, and understandable. Significantly, current research in this topic includes the Role-Centric Attribute-Based Access Control (RABAC) work by Jin Xin and his colleagues, which has realized one of the first reference models combining both roles and attributes in a reliable manner that preserves the best features of both access control methods. Commercial implementations are also developing that use both role-centric and dynamic role capabilities combined with the features of ABAC’s fine-grained authorization, demonstrating that the approach defined by ANSI/INCITS 494-2012 is practical, and can combine the best features of RBAC and ABAC for the enterprise.

G. Ateniese, K. Fu et al. [10], predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Proxy re-encryption allows proxy to transform a ciphertext computed under user ‘X’ public key into one that can open by other user ‘Y’s secret key. They discussed various applications of proxy re-encryption such as, secure file system, outsourced filtering of encrypted form etc. To improve re-encryption schemes they introduced the concept of Bilinear maps. It is pairing based scheme realized important new features.

F. Wang, Z.Liu et al [11], proposed an efficient identity based encryption scheme. This scheme is secure against the adaptive chosen identity and chosen plaintext attack in the standard model. To improve the efficiency of the lattice-based IBE scheme, unlike the identity string is encoded into a matrix by a group of public matrices in several known constructions, the identity string of l bits is encoded into a vector with the help of l + 1 vectors in this paper. As a result, the public key size of the proposed scheme is shorter than that of the known constructions of the lattice-based IBE scheme. There are still many open problems which need to be studied in the lattice-based IBE scheme, such as how to design a lattice-based HIBE in the standard model by their design techniques.

III. SYSTEM ARCHITECTURE

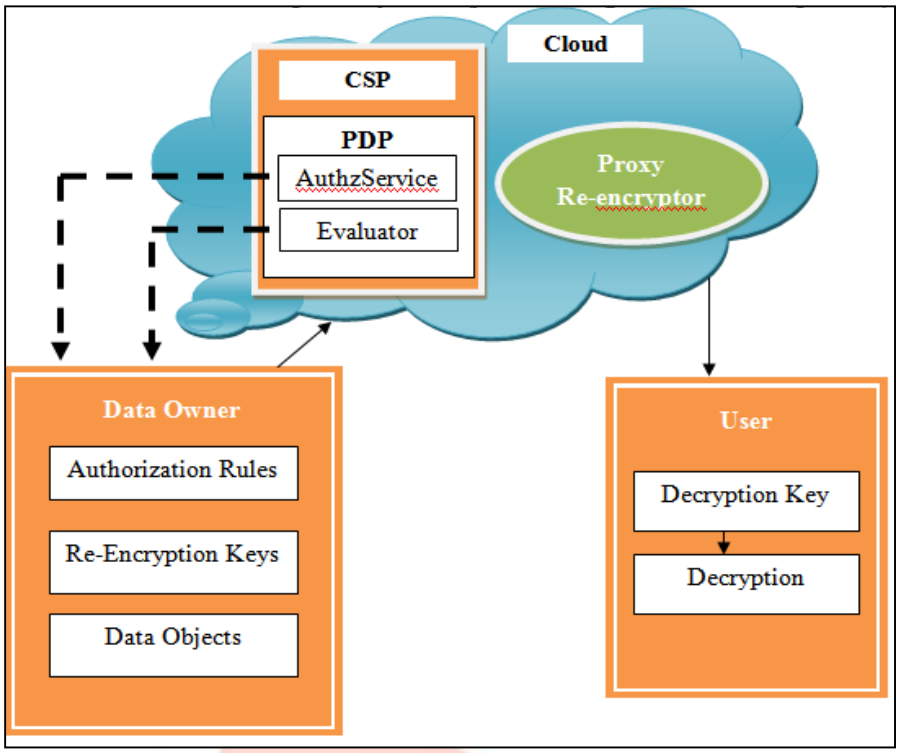

Figure 1 System Architecture

Figure 1 represents the system architecture. As shown in figure there are five entities present in the proposed system. The responsibilities of each one in given as below:

1. **Data owner**: It uploads encrypted data on cloud. A symmetric key encryption i.e. AES algorithm is used for data encryption.
   Data owner defined authorization rules and it is compared with AuthModel of cloud. Binary relations are included in it.
2. **Cloud:** It consists of PDP model to manage uthorization model and proxy re-encryptor.
3. **AuthzService:** It is entry point to PDP which allows query authorization. It returns the granted access/ denied.

IV. CONCLUSION

In this review paper, some existing techniques of data security in cloud environment have discussed. Existing approaches are based on outline security. Many time cloud crack this security outline which leads to data security challenges also user can lose their control over their data. The process of encryption avoids undesired accesses. However, it entails new issues related to access control management. RBAC: Rule based access control restrict system access to authorized users. However, there is need of efficient and effective technique to provide data security in cloud environment. From literature survey analysis, a centric approach known as, SecRBAC can be a better solution to provide data security guarantee

REFERENCES

[1] 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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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

[8] R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to rolebased access control," Computer, vol. 43, no. 6, pp. 79–81, 2010.
[9] Coyne and T. R. Weil, "Abac and rbac: Scalable, flexible, and auditable access management," IT Professional, vol. 15, no. 3, pp. 14–16, 2013.
[10] 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] 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