ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

A Unique Data Centric Authorization Model and Re-Encryption to Secure Cloud Data

P.Vinod[1], G.Sesha Phaneendra Babu[2]

M.Tech Student, Dept. of CSE, SKD Engineering College, Gooty, Affiliated to JNTUA, Andhra Pradesh, India[1]

Assistant Professor & HOD, Dept. of CSE, SKD Engineering College, Gooty, Affiliated to JNTUA, Andhra Pradesh, India[2]

ABSTRACT: Cloud attracts commercial entities and individual customers by its fascinating characteristics and strategic commercial benefits. The main service provided by cloud computing is data storage. Despite cloud service providers claiming to offer security to data they host, there have been cases of security breach. There are cases where information theft and data integrity violations have been experienced to suit certain interests. Third party cloud service administrators have all access privileges to manage storage cloud servers. Malicious insiders can attack the computing infrastructure with relatively easy and less knowledge of hacking, since they have a detailed description of the underlying infrastructure and high-level access privileges. Without using a complete trustworthy solution for defending against insider attacks, malicious insiders can easily obtain the passwords, cryptographic keys, files and gain access to clients' records. This calls for the need to develop and implement data confidentiality protection model for data security in the cloud. Existing Hierarchical approach implies that attributes should be managed by the same root domain authority. To overcome this issue this paper presents a novel a identity-based and proxy re-encryption techniques to protect the authorization model.

I. INTRODUCTION

Cloud Computing sees a technical and cultural shift of computing service provision from being provided locally to being provided remotely, and en masse, by third-party service providers. This increases the risk of unauthorized access to the private data. Even though the cloud continues to gain popularity in usability and attraction, the problems lies with data confidentiality, loss of control, lack of trust, data theft. Encryption is the most widely used method to protect data in the Cloud. In fact, the Cloud Security Alliance security guidance recommends data to be protected at rest, in motion and in use. Encrypting data avoids undesired accesses. However, it entails new issues related to access control management. A rule-based approach would be desirable to provide expressiveness. But this supposes a big challenge for a data-centric approach since data has no computation capabilities by itself. It is not able to enforce or compute any access control rule or policy. This raises the issue of policy decision for a self-protected data package. To overcome the issues, several proposals tried to provide data-centric solutions based on novel cryptographic mechanisms applying Attribute based Encryption (ABE). These solutions are based on Attribute-based Access Control (ABAC) or Role-based Access Control (RBAC).

There is no data-centric approach providing an RBAC model for access control in which data is encrypted and self-protected. when it comes to data-centric approaches in which data is encrypted, ABAC solutions are constrained by the expressiveness of ABE schemes. The cryptographic operations used in ABE usually restrict the level of expressiveness for access control rules. For instance, role hierarchy and object hierarchy capabilities cannot be achieved by current

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

ABE schemes. Moreover, they usually lack some combination with a user-centric approach for the access control policy, where common authorization-related elements like definition of users or role assignments could be shared by different pieces of data from the same data owner.

In this Paper 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 is proposed which provides a rule-based approach following the RBAC scheme, where roles are used to ease the management of access to the resources.

II. LITERATURE SURVEY

1) Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhount - FEACS: A Flexible and Efficient Access Control Scheme for Cloud Computing.

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) 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.

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.

3) R. Bobba, H. Khurana, and M. Prabhakaran - Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption.

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

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.

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

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.

5) 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.

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.

III. EXISTING SYSTEM

- Several data-centric approaches, mostly based on Attribute-based Encryption (ABE), have arisen for data protection in the Cloud. In ABE, the encrypted ciphertext is labeled with a set of attributes by the data owner. Users also have a set of attributes defined in their private keys. They would be able to access data (i.e. decrypt it) or not depending on the match between ciphertext and key attributes.
- The set of attributes needed by a user to decrypt the data is defined by an access structure, which is specified as a tree with AND and OR nodes.
- There are two main approaches for ABE depending on where the access structure resides: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE).
- In KP-ABE the access structure or policy is defined within the private keys of users. This allows to encrypt data labeled with attributes and then control the access to such data by delivering the appropriate keys to users. However, in this case the policy is really defined by the key issuer instead of the encryptor of data, i.e. the data owner. So, the data owner should trust the key issuer for this to properly generate an adequate access policy.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

- To solve this issue, CP-ABE proposes to include the access structure within the ciperthext, which is under control of the data owner. 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 and OR-ed attributes.

DISADVANTAGES OF EXISTING SYSTEM:

- Encrypting data avoids undesired accesses. However, it entails new issues related to access control management.
- To the best of our knowledge, there is no data-centric approach providing an RBAC model for access control in which data is encrypted and self-protected.
- Existing Hierarchical approach implies that attributes should be managed by the same root domain authority.
- User privileges are completely independent of their private key. Finally, no user-centric approach for authorization rules is provided by current ABE solutions.

IV. PROPOSED SYSTEM

- This paper 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.
- The main contributions of the proposed solution are:
- 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.

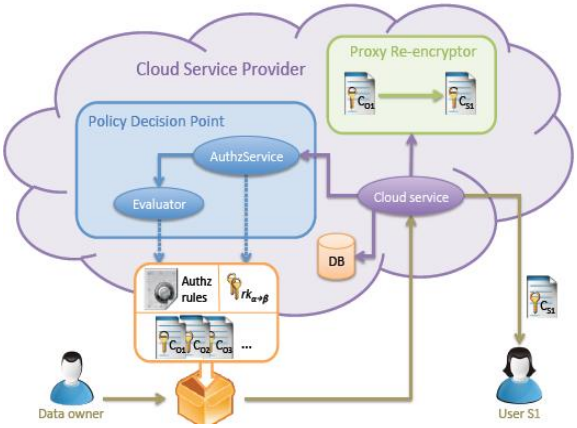

Fig 1.1: architecture of system

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

V. IMPLEMENTATION

1) Multi-use: A multi-use scheme enables the proxy to perform multiple re-encryption operations on a single ciphertext. That is, to re-encrypt from cα to cβ, from cα to cγ and so on.

2) Initializes The Cryptographic Scheme: It takes as input a security parameter k to initialize the cryptographic scheme (e.g. parameters to generate an elliptic curve) and outputs both the Master Secret Key msk and a set of public parameters p that is used as input for the rest of functions.

3) Generates Secret Keys: It takes as input the msk and an identity idα, and outputs the Secret Key skα corresponding to that identity.

4) Encrypts Data: It takes as input an identity idα and a plain text m, and outputs the encryption of m under the specified identity cα.

5) Generates Re-Encryption Keys: It takes as input the source and target identities idα and idα→β as well as the Secret Key of the source identity skα, and outputs the Reencryption Key rkα→β that enables to re-encrypt from idα to idβ.

6) Re-Encrypts Data: It takes as input a ciphertext cα under identity idα and a Re-encryption Key rkα→β, and outputs the re-encrypted ciphertext cβ under identity idβ.

7) Decrypts Data: It takes as input a ciphertext cα and its corresponding Secret Key skα, and outputs the plain text m resulting of decrypting cα.

VI. CONCLUSION

In this Paper SecRBAC, a data-centric access control solution for self-protected data is proposed that can run in untrusted CSPs and provides extended Role-Based Access Control expressiveness which provides a rule-based approach following the RBAC scheme, where roles are used to ease the management of access to the resources. A re-encryption key complement each authorization rule as cryptographic token to protect data against CSP misbehavior. The solution is independent of any PRE scheme or implementation as far as three specific features are supported and a comprehensive and feasible solution.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[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] W3C OWL Working Group, "OWL 2 Web Ontology Language: Document overview (second edition)," World Wide Web Consortium (W3C), W3C Recommendation, Dec. 2012.
[9] 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.
[10] W3C OWL Working Group, "OWL 2 Web Ontology Language: Profiles (second edition)," World Wide Web Consortium (W3C),W3C Recommendation Dec. 2012.