International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

SECRBAC : An Efficient and Secured Data Access Control Schemes in Cloud

P. Goutham
IFET College of Engineering,Villupuram, Tamil Nadu, India

ABSTRACT

An organizational data is to be encrypted for security reasons. In an institution the data stored in cloud by admin need authorization from an authorized person. Preliminary plans of authentication include an authorized person to gather information provided by admin with the help of code which is a private one and to be maintained by all non-users i.e. authorized persons. This process of providing code will take some time, and the wise usage of that time can be achieved by a direct authentication from authorized person with a considered code generation on direct authentication. This proposal contains identity based and proxy re-encryption algorithm widely used to protect from cloud computing. The authorization models contain evaluator key for user enrollment and also used to secret key generating for authorized user. Proxy means entity and re-encryption means without decryption it contains one more encryption. Identity encryption means a type of public key cryptography. This type of authorization model will result in a technical improvement in knowledge of computer usage.

Keywords: SECRBAC, Data Access Control, Cloud, CSP, HASBE, CP-ABE

I. INTRODUCTION

The Cloud Computing has become a cross-discipline that covers the computer science technology became a gap between technical services and IT industrial services. The technology platform includes Web services, cloud computing, networking, utilities, process contains modeling, transformation and integration. This scope of cloud Computing covers the entire life-cycle of services innovation research that includes business , various services such as creation, realization, annotation, deployment, discovery, composition, delivery, collaboration, monitoring, optimization, and management. The aim of cloud Computing is to enable and protect an information due an efficient and secured data in cloud computing.

The data can be stored by data owner in cloud services provider (CSP) otherwise cloud storage. The user authorized can access the cloud for gathering an information and at the same time the unauthorized persons cannot access the data from cloud computing. Only the authenticate person i.e. Data owner can manage the group. So, without the knowledge of data owner no one can access any information from the cloud.

The proposal system contain the two main encryption such as identity based and proxy re-encryption and these technology is mainly used to cover the information and authorization model under cloud computing. This process can by divide into four type as owner, cloud services provider (CSP), data user and evaluator. While, the process contains data owner can upload an information, document and on. They can store in cloud services provider (CSP). Due the gathering information by authorized person either document or files by only the authentication services provider can access data evaluator. The key can be directly send to data user but only authorized persons.

II. METHODS AND MATERIAL

A. Literature Survey

2.1 Overview:

CSEIT172225 | Received: 05 March 2017 | Accepted: 17 March 2017 | March-April-2017 [(2)2: 163-167]

A literature review is an account of what has been published on a topic by accredited scholars and researchers. Occasionally you will be asked to write one as a separate assignment, but more often it is part of the introduction to an essay, research report, or thesis. In writing the literature review, your purpose is to convey to your reader what knowledge and ideas have been established on a topic, and what their strengths and weaknesses are. As a piece of writing, the literature review must be defined by a guiding concept (e.g., your research objective, the problem or issue you are discussing or your argumentative thesis). It is not just a descriptive list of the material available, or a set of summaries

Besides enlarging your knowledge about the topic, writing a literature review lets you gain and demonstrate skills in two areas

1. **INFORMATION SEEKING:** the ability to scan the literature efficiently, using manual or computerized methods, to identify a set of useful articles and books
2. **CRITICAL APPRAISAL:** the ability to apply principles of analysis to identify unbiased and valid studies.

RANDOMIZABLE PROOFS AND DELEGATABLE ANONYMOUS CREDENTIALS
AUTHOUR: Mira Belenkiy, Jan Camenisch, Melissa Chase, MarkulfKohlweiss

We construct an efficient delegable anonymous credentials system. Users can anonymously and unlikable obtain credentials from any authority, delegate their credentials to other users, and prove possession of a credential L levels away from a given authority. The size of the proof (and time to compute it) is O(Lk), where k is the security parameter. The only other construction of delegable anonymous credentials (Chase and Lysyanskaya, Crypto 2006) relies on general non-interactive proofs for NP-complete languages of size kΩ(2L). We revise the entire approach to constructing anonymous credentials and identify randomizable zero-knowledge proof of knowledge systems as the key building block. We formally define the notion of randomizable non-interactive zero-knowledge proofs, and give the first instance of controlled randomization of non-interactive zero-knowledge proofs by a third-party

FLEXIBLE AND SCALABLE ACCESS CONTROL IN CLOUD COMPUTING
AUTHOUR : Thamayanthi.M, Dhiveha.S

Cloud computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose Hierarchical Attribute Set-Based Encryption (HASBE) by extending cipher text-policy Attribute-Set-Based Encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme.

CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION: AN EXPRESSIVE, EFFICIENT, AND PROVABLY SECURE REALIZATION
AUTHOUR:B. Waters

We present new techniques for realizing Cipher text-Policy Attribute Encryption (CP-ABE) under concrete and no interactive cryptographic assumptions. Our solutions allow any encryption to specify access control in terms of an LSSS matrix, M, over the attributes in the system. We present three different constructions that allow different tradeoffs between the systems efficiency and the complexity of the assumptions used. All three constructions use a common methodology of “directly” solving the CP-ABE problem that enables us to get much better efficiency than prior approaches. Public-Key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device. While this is useful for applications where the data provider knows specifically which user he wants to share with, in many applications the provider will want to share data according to some policy based on the receiving user’s credentials.

B. RELATED WORK

Different approaches can be found in the literature to retain control over authorization in Cloud computing. In authors propose to keep the authorization decisions taken by the data owner. The access model is not published to the Cloud but kept secure on the data owner premises. However, in this approach the CSP becomes a mere storage system and the data owner should be online to process access requests from users. Another approach from deals with this issue by enabling a plug-in mechanism in the CSP that allows data owners to deploy their own security modules.

This permits to control the authorization mechanisms used within a CSP. However, it does not establish how the authorization model should be protected, so the CSP could potentially infer information and access the data. Moreover, this approach does not cover Inter-cloud scenarios, since the plug-in module should be deployed to different CSPs. Additionally, these approaches do not protect data with encryption methods. In the proposed SecRBAC solution, data encryption is used to prevent the CSP to access the data or to release it bypassing the authorization mechanism. However, applying data encryption implies additional challenges related to authorization expressiveness. Following a straightforward approach, one can include data in a package encrypted for the intended users.

This is usually done when sending a file or document to a specific receiver and ensures that only the receiver with the appropriate key is able to decrypt it. 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. To cope with these issues, SecRBAC follows a data-centric approach that is able to cryptographically protect the data while providing access control capabilities.

C. SYSTEM ANALYSIS

In this phase a detailed appraisal of the existing system is explained. This appraisal includes how the system works and what it does. It also includes finding out in more detail- what are the problems with the system and what user requires from the new system or any new change in system. The output of this phase results in the detail model of the system. The model describes the system functions and data and system information flow. The phase also contains the detail set of user requirements and these requirements are used to set objectives for the new system.

D . EXISTING SYSTEM

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: who should evaluate the rules upon an access request? The first choice would be to have them evaluated by the CSP, but it could potentially bypass the rules. Another option would be to have rules evaluated by the data owner, but this implies that either data could not be shared or the owner should be online to take a decision for each access request.

III. RESULTS AND DISCUSSION

A. LIMITATIONS

- Users may loss control on their data.
- A big challenge for a data-centric approach since data has no computation capabilities by itself.

B. PROPOSED WORK

These techniques are used to protect both the data and the 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. The solution enables a rule based approach for authorization in Cloud systems where rules are under control of the data owner and access control computation is delegated to the CSP, but making it unable to grant access to unauthorized parties. 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.
- Secure key distribution mechanism and PKI compatibility for using standard X.509 certificates and keys.

C. ADVANTAGES

- Secure protection of data in the Cloud.
- Advanced cryptographic techniques have been applied to protect the authorization model.

D. SYSTEM ARCHITECTURE:

System architecture is a conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system

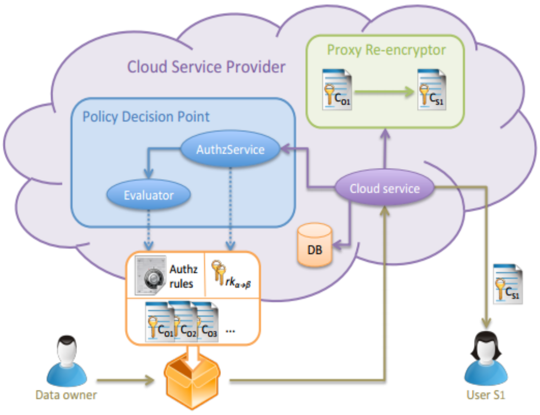

Figure 1. System Architecture

When moving data to the cloud, a self-protected package is generated by the data owner. This package contains: the encrypted data objects, the authorization rules and the corresponding re-encryption keys. Data objects are encrypted before uploading them to the Cloud in order to prevent the CSP to access them. This is done by data owners by using the encrypt() function. According to Def. 8, data should be encrypted using the identity ido1 of the object being uploaded o1. A digital envelope approach can be applied to protect data objects instead of direct encryption. This would enhance cryptographic operations like re-encryptions for large data objects. This approach consists in using a symmetric encryption algorithm (e.g. AES) to protect the data object itself. The encryption of data is done with a random symmetric key generated for the purpose of a single encryption. Then, this key is encrypted with the encrypt () function. With this procedure, potentially big objects (e.g. large documents) are encrypted using symmetric cryptography, whose algorithms are more efficient. In turn, more costly operations are only applied to the keys used for the symmetric encryption, which are usually small pieces of data of some bytes length.

IV. CONCLUSION

A secure role base access control have contains a data-centric have proposal system for protect the cloud Computing. The process provides two encryption algorithms for secure all data, files and so on. They includes evaluator as a key generating function for data user to access the encryption key to convert cipher text to plaintext otherwise unknown language to known language.

The concrete scheme contains feasible solution and high secure data. The techniques contribute such as collision detection determination methods. The cloud service provider including an hybrid approach with cryptography usage of public key infrastructures. The proposal contain prototype implementation can discovered and advanced paper. Thus the expected result can obtained.

V. 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, "Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public KeyCryptography - 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]. International Committee for Information Technology Standards, "INCITS 494-2012 - information technology - role based access control - policy enhanced," INCITS, Standard, Jul. 2012.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.