IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-5, Issue-6 E-ISSN: 2347-2693

Data Security in Public Cloud for Authorization

P.B.Gajeli[1*] and P.S.Yalagi[2]

[1*]Department of CSE, Walchand Institute of Technology, Solapur University, Solapur,India
[2]Department of CSE, Walchand Institute of Technology, Solapur University, Solapur,India

[*]*Corresponding Author: pbgajeli@gmail.com*

Available online at: www.ijcseonline.org

Received: 25/May/2017, Revised: 02/Jun/2017, Accepted: 20/Jun/2017, Published: 30/Jun/2017

Abstract— Most of the security solutions use routers, firewalls, and intrusion detection systems implemented to tightly control, access to networks from outside authors. Cloud computing breaks these organizational bounds. When the data is present in the cloud, it resides outside the organizational bounds. Hence, a user loses control over their data. Another problem is, most of the time users are anxious about uploading private and confidential files for online backup due to concern that the service provider might use it inappropriately. So, providing security at the required level is a major concern. The existing solution is data-centric access control solution with an enriched role-based approach in which security is focused on protecting user data regardless the cloud service provider that holds it. In this, Novel rule-based and proxy re-encryption technique are used to protect the authorization model and increase the performance. The authorization model is rule-based file access control, i.e. permissions granted based on authority rules provided by the data owner. In this existing solution, the authorization model contains limited privileges which restrict modification and deletion. The proposed systems consist of two types of data viz. Normal data and Sensitive data. The user can upload the file and select the type of data. Protecting normal data by using proxy re-encryption technique and sensitive data by using rummage technique. The rummage technique which encrypts the original data into meaningful (readable) format, hence attacker gets confused to identify encrypted data. The authorization model is rule-based file access control that contains privileges like access, modify, delete, etc.

Keywords— Encryption technique, Data-centric security, Cloud computing, Role-based access control, Authorization

I. INTRODUCTION

Maintaining the security and the levels of security is a vital part in cloud computing. Most of the cloud service providers prefer basic security that is a firewall, router, and intrusion detection system for security purposes. Now when data is uploaded by data owner on a cloud by different organizations, cloud service providers apply their perimeter security mechanisms on that data. In such case, a user may lose the control on their data. To avoid such complications, the following few solutions are provided by Juan M. Mar´ın P´ erez et.al. 1] Among which one is data-centric access control solution with role-based expressiveness in which security is focused on protecting the authorization model. 2] Novel identity-based and proxy re-encryption technique are used for protecting authorization model.

The importance of access control is to authenticate the user to perform actions and operations. To restrict the subject or the group from accessing, a Discretionary Access Control (DAC) model is used [4]. This model restricts part of the session's elements because it uses access control matrix for setting the policy. But this type of model support does not security level restriction and multi-policy. Mandatory Access Control (MAC) model is same like the DAC model, but a difference is that MAC support, security level restriction due to MAC sets a secret class on the target and the subject [6]. An RBAC (Role-Based Access Control) approach, it is a role-centric model. In that, roles can be well accepted by their names, and they decide the permissions be granted to users. An ABAC (Attribute-Based Access Control) approach, It is an attribute-centric model. In this model, the permissions are granted to the user depends on their attributes and that attributes must select by expert staff or personnel [2].

An RBAC m may require the large definition of roles for fine-grain authorization and ABAC is easier to set up without making an effort to determine the role as an RBAC model. On the other hand, In ABAC model, ABAC may result in a huge number of rules that is a system with n attributes then it would have possible rule combinations up to 2^n. An ABAC splits authorization rules from user attributes, making it difficult to decide permissions available to a particular user, while RBAC is role-centric and user privileges can be easily decided by the data owner. A rule-based approach following the RBAC scheme is to propose for authorization solution, where roles are used to assign the privileges to the user for data access. This approach can help to control and manage security based on the cloud access that is access data from a cloud by authorized users.

We will propose authorization solution which provides a rule-based approach containing RBAC (Role-Based Access Control) scheme. A data-centric access control solution that is SecRBAC, for self-protected data that can run with untrusted CSPs (Cloud service provider) and thus provides extended Role-Based Access Control expressiveness on data. In existing paper, the proposed system does not provide more privileges, for example, they are providing only data access to the users [1]. Suppose a data owner wants to modify the data or delete the file and he is unable to do so, then he will provide privileges to the authorized user to modify or delete the file. Hence, to extend privileges to the users and save the time for data owner this paper provides such a system which will solve the problem of both the data owner and the users.

We will propose a system to extend the privileges of the authorization model with more action like modification and deletion that are not present in the existing authorization model. The authorization model is a rule-based file access control, i.e. Permissions granted based on authority rules that are assigned by data owner like, access, modification and deletion mode. Novel rule-based and proxy re-encryption technique will be used to protect the authorization model and increase the performance. The proposed system will consist of normal data and sensitive data. The data owners will upload normal data, and then apply proxy re-encryption technique and for uploading sensitive data rummage technique will be applied.

In a proxy re-encryption (PRE) scheme, a proxy can convert an encryption, computed with Bob's public key into an encryption intended for Alice. In PRE schemes, the fundamental property is that the proxy is semi-trusted, i.e., it does not know the secret keys of Bob or Alice and does not learn the plaintext during the conversion process. The proxy and Alice, however, are not allowed to connive, thus it is usually assumed that at least one of the two is honest or that their collusion is preventable or detectable via other means. An Identity-Based Encryption (IBE) is a type of asymmetric cryptography schemes that is public key cryptography; in which senders encrypt messages by using the public key as the recipient's identity (a string). For instance, Bob could encrypt a message for Alice by only using her email address [10]. The IB-PRE (Identity-based Proxy re-encryption) scheme produced with the combination of PRE and IBE schemes and this scheme is helpful for cloud storage system [8]. Next concept is rummage technique, i.e. used for sensitive data. Rummage technique is one of the encryption technique, it will encrypt the data into the meaningful format that is a readable format, but it cannot extract the meaning of that data or sentences. So, the attacker gets confused in that stage.

This paper is organized in six sections with introduction preceding the literature review in section II. In section IV, we propose our approach for data protection in cloud that is problems are exists is section III. In section V, we are discussed expected result and last section VI is conclusion.

II. LITURATURE REVIEW

A. RBAC and ABAC: Flexible,Scalable and Auditable Access Management

This system has introduced novel access control models used for authorization. In RBAC, this type of access control model works based on roles and role can be understood by their names and they decide the sets of permission to be granted to the users. This type of model is useful when given permission to the user; RBAC is a role-centric model for the role can be represented as an attribute. It is easy to implement and RBAC has been extensively adopted and provides security and administrative advantages. RBAC must be restricted to handle dynamically changing attributes. With ABAC, there is no need to manage roles and role names aren't used as attributes because it is an attribute centric model. This type of access control model allows dynamically changing attributes such as location and time of day can be adapted in access control decisions. ABAC is simpler to implement and adapts real-time environmental states as an access control parameters. Both RBAC and ABAC can be used by considering the roles as user attributes [2].

B. PBAC: Policy Based Access Control

In this, a policy-based access control model (PBAC) because the existing access control models cannot support multi-policy and not flexible [3]. The different types of traditional models are which restrict session only with subject authorization, such as DAC (Discretionary Access Control), RBAC (Role-based Access Control), MAC (Mandatory Access Control), and ERBAC (Extended Role-based Access Control) which are restricted session with subject authorization and also integrated with application logic [4, 5, 6, 7]. PBAC recognizes policy based access control by specifying attributes to describe a session property, performing a new policy management method that is advocating an independent access control decision mechanism and free from application logic. As a consequence, PBAC makes great progress on multi-policy supporting and more flexible on restricting session. In this paper, their analysis indicates that PBAC is best to the current access models used by considering the roles as user attributes.

C. Identity-Based Proxy Re-encryption (IB-PRE)

This paper addresses the problem of Identity-Based proxy re-encryption (IB-PRE), where the encrypted text i.e. ciphertexts are transformed from one identity to another. Their schemes are compatible with current IBE deployments and avoiding extra work from the IBE trusted-party key generator. In addition, one of them permits multiple re-encryptions and they are non-interactive. In this paper work, they introduced different constructions enabling non-interactive, unidirectional proxy re-encryption in the IBE setting. Those schemes are very efficient and can be deployed within standard IBE frameworks. New compelling applications can be realized thanks to their schemes, most notably access control and attribute-based delegation [8].

D. Full secure IBE scheme with short public key size over lattices in the standard model

In this approach an efficient Identity-based encryption (IBE) scheme in the standard model over the lattice [9, 10, 11]. Under the strictness of the learning with errors (LWE) problem, the proposed scheme is semantic secure against chosen plaintext attack and adaptive chosen identity in the standard model [12]. To improve the efficiency of the lattice-based IBE scheme, they prove that the proposed scheme is semantic secure against the chosen plaintext attack and adaptive chosen identities if the LWE problem is difficult to solve. They use to encode the identity information into a vector by using l + 1 vectors, then after, the private key can be extracted at the same lattice. Hence matrix one n × m and l + 1 n-dimensional vectors are the public-key of the proposed scheme. As a result, their proposed scheme is the public key size is shorter than that of the known constructions of the lattice-based IBE scheme.

E. Different Obfuscation Techniques for Code Protection

This approach has provided different types of obfuscation technique for code protection [13, 14]. With the improvements in digital technology, the threat of unbelievable level of illegal and duplicating reproducing of software also increases. Therefore the plagiarism (piracy) rate is increasing proportionally. The various software protection techniques have been developed in that, this paper proposed one of such software protection techniques is code obfuscation [15]. The obfuscation code is a technique for hiding the data structures or the logic of the code, original algorithm or to harden or protect from the attacker and unauthorized reverse engineering process. Some obfuscation methods are proposed, which can help to protect original code and given some example in assembly language [16, 17].

III. EXISTING SYSTEM

In the traditional approach, most security solutions are based on boundary security like a firewall, router, and intrusion detection system. However, Cloud computing breaks the organization perimeters that are security-related devices. When data present in the Cloud, they present outside the organizational bounds where users can't access their own data due to the boundary security provided by own CSP rules. So, the existing solution is a data-centric access control solution in which security is focused on protecting the user data regardless cloud service provider that holds it. A novel cryptographic technique that is identity-based and proxy re-encryption techniques are used to protect the authorization model.

In the existing system, the Authorization model contains limited privileges, that is, it contains only accessing the data. The authorized users are only accessing the data depends on authorization rules and that rule contains limited privileges, unlike modification or deletion. Suppose a data owner wants to modify the data and they have less time to modify the data. Hence, the data owner extends the privileges like modification and deletion. When data owner has less time and modify privilege giving to the trusted user and that user modifies the data. The data owner providing some tasks to the authorized users and save his/her time based on extending the privileges. The following points represent two problems of the existing system and those problems are attempted to be solved in the proposed system:

- Extending privileges in the authorization model like to modify and delete etc. that are not provided in existing authorization model.
- Applying a cryptographic technique to user data for data access against CSP or unauthorized users. Hence, Identity-Based Proxy Re-Encryption scheme applies for normal data. Rummage technique applies for sensitive data.

IV. PROPOSED SYSTEM

The proposed system consists of two types of data one is normal data and another one is sensitive data. In that, we are presenting a data-centric access control solution with improved role-based expressiveness in which security is focused on protecting user data regardless the cloud service provider (CSP) that holds it. The figure 4.1 shows that, when data move to the cloud, data owner generates a self-protected package. This contains the authorization rules, the encrypted data objects, and the corresponding re-encryption keys.

In the *IBPRE scheme* for normal data, before uploading the data object first it will encrypt it, then after uploading them in order to prevent the CSP to access them. When a user want to access the data which is uploaded by data owner then it generates re-encryption key with the combination of a secret key and public key. To apply this key for re-encryption and it will decrypt by authorized user’s own secret key. In Rummage technique for sensitive data, before uploading the data first it will encrypt in that level attacker should get confused that is the encrypted file is encrypted or not. When a user wants to access that file uploaded by data owner then user enter her/him secret key for file decryption.

PDP (Point Decision Point) which can manage the proxy re-encryptor and also manage the authorization model that performs cryptographic operations. An AuthzService that is Authorization service module act as starting point to the PDP for cloud services allowing to query it for authorization decisions. This module can take decisions upon when a user u1 request to accessing the data d1 managed by the service.

This module usually returns a statement that is the access granted or denied. This module makes use of evaluator module in control of making the computations over the authorization model.

Novel rule-based and encryption technique is used to protect the authorization model and increase the performance. The encryption technique and authorization rules are cryptographically protected against the service provider access or misbehavior. The authorization model is rule-based file access control, i.e. Permissions granted based on authority rules like, access, modification, and deletion mode that is to increase the privileges of authorization model.

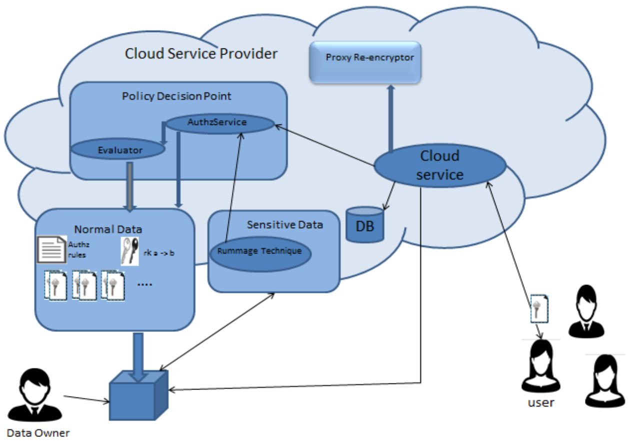

Figure1. Overview of the proposed system

The proposed system consists of two types of encryption techniques that are Identity-Based proxy Re-encryption technique (IB-PRE) and Rummage technique to protect the data. The IB-PRE scheme used for normal data and Rummage technique used for sensitive data.

A. Identity-Based proxy Re-encryption technique (IB-PRE)

Identity-Based Proxy Re-Encryption (IB-PRE) schemes allow a proxy to convert a ciphertext encrypted under Bob's identity into one computed under Alice's identity. To allow this translation, Bob generates delegation key i.e. re-encryption key and provisions the proxy with a re-encryption key that the proxy uses to do the re-encryption. The advantages of this scheme, the information about the secret key of Alice or Bob cannot be shared and the proxy also cannot read the underlying plaintext. Hence, this type of proxy re-encryption scheme is helpful for data sharing through a cloud and protects data from misbehaviors or cloud service provider.

B. Rummage technique

In Identity-based proxy re-encryption scheme, master secret key (MSK) is a secret key and data will encrypt with MSK. Proxy re-encryption generates ciphertext that is unreadable formatted. So, the attacker knows this is cipher text and they try to decrypt in original format. In this technique, MSK is a secret key. Hence this technique is securely based on MSK. But in Rummage technique, this is also an encryption technique that is, it will generate ciphertext. The difference between both techniques is that proxy generates ciphertext and that text is an unreadable format, but in Rummage technique generates ciphertext and that text is in a readable format. Hence attacker gets confused this text is encrypted or not. So, this concept is more secure in rummage technique.

Rummage comprises a number of advanced obfuscation techniques. The most of these algorithms produce by irreversibly removing information and structure which helps attackers. Rummage technique, i.e. used for sensitive data. Rummage technique is a technique which encrypts the data in a meaningful format. That format is a user readable format and this format to get confused to attacker based on encrypting on a meaningful format.

V. EXPECTED RESULTS

We propose a new cryptographic technique that is Rummage technique. In IBPRE scheme, which is generated cipher text that is an unreadable format that is not only IBPRE scheme, but also some others cryptographic techniques such as Symmetric and Asymmetric cryptographic techniques are created a cipher text that is an unreadable format for preventing unauthorized access. In this technique, at least attackers know that is, this is an encrypted file, then attacker tries to decrypt the file by using different methods and sometimes it may be successful or not. In Rummage technique, this level of encryption is that encrypted file is a readable format or meaningful format. Hence, the attacker gets fooled or confuse to identify the encrypted file is encrypted or not. So, that encrypted file to create like this the original file converts into a meaningful format to apply some techniques like grammar or dictionary words. This level of encryption, the attacker can read an encrypted file and get the meaning of that file, but that file content's meaning and original file content's meaning are different. Hence, we propose to this level of encryption is helpful to share sensitive data against CSP or unauthorized users and this technique is well suitable for data access or sharing from a cloud.

IV. CONCLUSION

The main objective of this paper is belongs to protect data on cloud and prevent data access to unauthorized users. Hence, we propose a data-centric authorization solution for secure protection of data in the cloud and extend the privileges, which help both data owner and user and novel cryptographic technique to protect the authorization model. The rule-based approach that is access control models is useful for implementing authorization model, which help to provide more privileges to the users like file access, modify and delete. Another point is data encryption, which is protecting data from unauthorized users or attackers. Hence, the novel identity-based proxy re-encryption technique and Rummage technique are feasible to protect the authorization model. The rummage technique is one of the encryption technique to protect sensitive data, this encryption format is like the attacker can read the file, but they do not extract the meaning like the original file. These techniques are helpful to protect data from CSP or misbehavior and also unauthorized users.

ACKNOWLEDGEMENT

I am thankful to my guide Asst. Prof. P. S. Yalagi for her advice and encouragement for the paper work.

REFERENCES

[1] Juan M. Marin Perez; Gregorio Martinez Perez; Antonio F. Gomez-Skarmeta, ―SecRBAC:Secure data in the Clouds.IEEE Transactions on Services Computing, 2016.

[2] Coyne and T. R. Weil, "Abac and rbac: Scalable, flexible, and auditable access management," IT Professional, vol. 15, no. 3, pp.14–16, 2013.

[3] Lin Zhi, Wang Jing, Chen Xiao-su and Jia Lian-xing," Research on Policy-based Access Control Model", 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 978-0-7695-3610-1/09 $25.00 © 2009 IEEE ,DOI 10.1109/NSWCTC.2009.313

[4] R. S. Sandhu, P. Samarati. "Access control: principles and practice",IEEE Comrnunications, vol. 32(9), pp. 40~48, 1994.

[5] R S. Sandhu, E J. Coync, H L Fcinstcin et al. "Role-based access control models", IEEE Computer., vol. 29(2), pp.38~47, 1996.

[6] Ravi Sandhu. "Mandatory controls for database integrity" In Database Security ¬: Status and prospects. North-Holland,pp.143~150, 1990.

[7] Huang Yi-ming. "Design of an Extended Role-Based Access Control Model and Its Implementation", Journal of Computer Research and Development, vol. 40(10), pp.1521~1528, 2003.

[8] 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.

[9] Pooja B. Gajeli, Pratibha.S. Yalagi, "A Survey on Access control models and Encryption schemes" International Journal of Engineering Research and Management (IJERM) ISSN: 2349-2058, Volume-01, Issue-01, April 2014.

[10] 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.

[11] A.Shamir, Identity-based cryptosystems and signature schemes, Proceedings of Crypto 1984, LNCS 196, Springer,Berlin, 1984. pp. 47–53.

[12] O. Regev, On lattice, learning with errors, random linear codes, and cryptography, Proceedings of STOC 2005, Baltimore, 2005. pp. 84–93.

[13] Chandan Kumar Behera and D. Lalitha Bhaskari, "Different Obfuscation Techniques for Code Protection", 4thInternational Conference on Eco-friendly Computing and Communication Systems, Procedia Computer Science 70 (2015) 757 – 763.

[14] Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil Pairing. In: Advances in Cryptology (CRYPTO 2001). Volume 2139 of Lecture Notes in Computer Science., Springer (2001) 213–229

[15] Jean-Maries Borello and Ludovic Me, Code Obfuscation Techniques for Metamorphic Viruses, Springer, 2008.

[16] Wroblewski., General method of program code obfuscation. In Proc. International Conference on Software Engineering Research and Practice (SERP 02), pages 153–159, 2002.

[17] Giovanni Vigna, Static Disassembly and Code Analysis, Malware Detection. Advances in Information Security, Springer, Heidelberg, vol.35, pages. 19 – 42, 2007.

Authors Profile

Pooja Balaji Gajeli is pursuing her Master Degree of Computer Science & Engineering from Walchand Institute of Technology, Solapur University, Maharashtra, India. She has received Bachelor degree in Computer Science and Engineering from Nagesh Karajagi Orchid College of Engineering, Solapur University, Solapur. Her research interests include Cloud Computing, Computer Security.

Ms. Pratibha S. Yalagi is working as Assistant Professor in Computer Science and Engineering / Information Technology at Walchand Institute of Technology, Solapur, Maharashtra, India. She is pursuing Ph.D. in distributed and parallel computing. The Author has an experience of total 16 years in teaching. She has presented and published more than 25 papers in various national, international conferences and journals. Worked as a Member, Board of Studies, Information Technology, Solapur University, Solapur.