ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.4. No.10, Pages : 01-06 (2016)
Special Issue of ICACSSE 2016 - Held on September 30, 2016 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2016sp01.pdf

Role Based Access Control using Advanced Data Centric Security Technique in cloud computing

BHARATHKUMAR CHEBROLU **Dr P Harini [2]**

[1] M.Tech Student, Dept. of CSE, St.Ann's College of Engineering & Technology, Chirala,

Andhra Pradesh - 523187, INDIA

[2] Professor and Head, Dept. of CSE, St.Ann's College of Engineering & Technology, Chirala,

Andhra Pradesh - 523187, INDIA

ABSTRACT:

Most present security arrangements depend on edge security. Nonetheless, Cloud processing breaks the association edges. At the point when information lives in the Cloud, they dwell outside the hierarchical limits. This leads clients to a loos of control over their information and raises sensible security worries that moderate down the appropriation of Cloud processing. Is the Cloud administration supplier getting to the information? Is it honest to goodness applying the entrance control arrangement characterized by the client? This paper displays information driven access control arrangement with advanced part based expressiveness in which security is centered on ensuring client information notwithstanding the Cloud administration supplier that holds it. Novel personality based and intermediary re-encryption strategies are utilized to ensure the approval model. Information is scrambled and approval principles are cryptographically ensured to protect client information against the administration supplier access or bad conduct. The approval model furnishes high expressiveness with part order and asset pecking order support. The arrangement exploits the rationale formalism gave by Semantic Web advances, which empowers propelled standard administration like semantic clash discovery. A proof of idea execution has been produced and a working prototypical sending of the proposition has been coordinated inside Google administrations.

INTRODUCTION

SECURITY is one of the principle client attentiveness toward the selection of Cloud processing. Moving information to the Cloud typically suggests depending on the Cloud Service Provider (CSP) for information insurance. Despite the fact that this is typically overseen based on legitimate or Service Level Agreements (SLA), the CSP could conceivably get to the information or even give it to outsiders. Also, one ought to believe the CSP to authentically apply the entrance control rules characterized by the information proprietor for other clients. The issue turns out to be significantly more perplexing in intercloud situations where information may spill out of one CSP to another. Clients may misfortune control on their information. Indeed, even the trust on the united CSPs is outside the control of the information proprietor. This circumstance prompts reexamine about information security approaches and to move to an information driven methodology where information are self-secured at whatever point they live.

Encryption is the most generally utilized strategy to secure information as a part of the Cloud. Truth be told, the Cloud Security Alliance security direction prescribes information to be ensured very still, in movement and being used [1]. Scrambling information stays away from undesired gets to.

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.4. No.10, Pages : 01-06 (2016)
Special Issue of ICACSSE 2016 - Held on September 30, 2016 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2016sp01.pdf

Nonetheless, it involves new issues identified with access control administration. A standard based methodology would be alluring to give expressiveness. Be that as it may, this assumes a major test for an information driven methodology since information has no calculation capacities independent from anyone else. It is not ready to authorize then again register any entrance control tenet or approach. This raises the issue of strategy choice for a self-secured information bundle: who ought to assess the tenets upon an entrance demand? The principal decision would be to have them assessed by the CSP, yet it could possibly sidestep the standards. Another alternative would be to have rules assessed by the information proprietor, yet this infers either information couldn't be shared or the proprietor should be online to take a choice for every entrance demand.

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. This approach can help to control and manage security and to deal with the complexity of managing access control in Cloud computing. Role and resource. A data-centric approach is used for data self-protection, where novel cryptographic techniques such as Proxy Re-EncryptionEncryption (PRE) [10], Identity-Based Encryption (IBE) [11] and Identity-Based Proxy Re-Encryption (IBPRE) [12] are used. They allow to re-encrypt data from one key to another without getting access and to use identities in cryptographic operations. 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 rulebased 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.

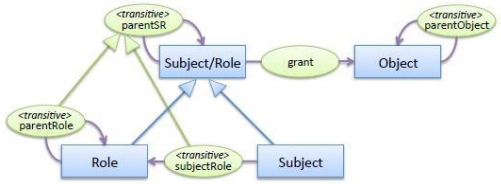

Fig. Ontology representing the authorization model

Attribute-based encryption

Attribute Based Encryption (ABE) was in this way proposed to have adaptable access control of encoded information using access arrangements and credited traits connected with private keys and figure messages individually. Trait based encryption, a large portion of ABE frameworks are developed with pairings while the calculation cost in the decoding stage develops alongside the measure of the entrance approach. ABEs are normally excessively costly for asset compelled front-end clients, which enormously ruins its useful fame. Encryption requires the information sender to scramble an additional irregular message and register a checksum esteem identified with two messages; unscrambling requires the outsider administration to execute the hidden decoding calculation twice and the information collector to confirm the outsourced calculation as for the encoded messages.

RELATED WORK

Different approaches can be found in the literature to retaincontrol over authorization in Cloud computing. In [13]authors propose to keep the authorization decisions takenby the

data owner. The access model is not published tothe Cloud but kept secure on the data owner premises.However, in this approach the CSP becomes a mere storagesystem and the data owner should be online to process accessrequests from users. Another approach from [14] dealswith this issue by enabling a plug-in mechanism in the CSPthat allows data owners to deploy their own security modules.This permits to control the authorization mechanismsused within a CSP. However, it does not establish how theauthorization model should be protected, so the CSP couldpotentially infer information and access the data. Moreover,this approach does not cover Inter-cloud scenarios, sincethe plug-in module should be deployed to different CSPs.Additionally, these approaches do not protect data withencryption methods. In the proposed SecRBAC solution,data encryption is used to prevent the CSP to access the dataor to release it bypassing the authorization mechanism.

However, applying data encryption implies additionalchallenges related to authorization expressiveness. Followinga straightforward approach, one can include data in apackage encrypted for the intended users. This is usuallydone when sending a file or document to a specific receiverand ensures that only the receiver with the appropriate keyis able to decrypt it. From an authorization point of view,this can be seen as a simple rule where only the user withprivilege to access the data will be able to decrypt it (i.e. theone owning the key). However, no access control expressivenessis provided by this approach. Only that simple rule canbe enforced and just one single rule can apply to each datapackage. Thus, multiple encrypted copies should be createdin order to deliver the same data to different receivers.To cope with these issues, SecRBAC follows a data-centricapproach that is able to cryptographically protect the datawhile providing access control capabilities.

Several data-centric approaches, mostly based on Attribute-based Encryption (ABE) [5], have arisen for data protectionin the Cloud [4]. In ABE, the encrypted ciphertext islabeled with a set of attributes by the data owner. Users alsohave a set of attributes defined in their private keys. Theywould be able to access data (i.e. decrypt it) or not dependingon the match between ciphertext and key attributes. Theset of attributes needed by a user to decrypt the data isdefined by an access structure, which is specified as a treewith AND and OR nodes. There are two main approachesfor ABE depending on where the access structure resides:Key-Policy ABE (KP-ABE) [5] and Ciphertext-Policy ABE(CP-ABE) [3]. In KP-ABE the access structure or policy isdefined within the private keys of users. This allows encrypting data labeled with attributes and then controlling theaccess to such data by delivering the appropriate keys tousers. However, in this case the policy is really defined bythe key issuer instead of the encrypt or of data, i.e. the dataowner. So, the data owner should trust the key issuer forthis to properly generate an adequate access policy. To solvethis issue, CP-ABE proposes to include the access structurewithin the ciperthext, which is under control of the dataowner. Then, the key issuer just asserts the attributes ofusers by including them in private keys. However, either inKP-ABE or CP-ABE, the expressiveness of the access controlpolicy is limited to combinations of AND-ed or OR-edattributes. The data-centric solution presented in this papergoes a step forward in terms of expressiveness, providing arule-based approach following the RBAC scheme that is nottied to the limitations of current ABE approaches.

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.4. No.10, Pages : 01-06 (2016)
Special Issue of ICACSSE 2016 - Held on September 30, 2016 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2016sp01.pdf

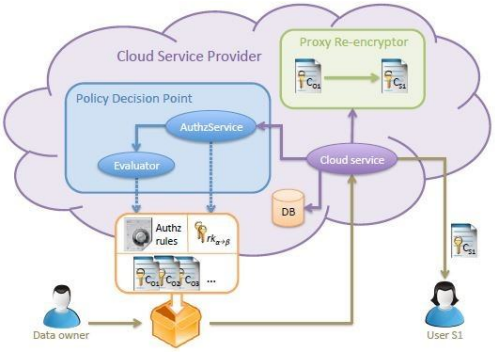

Fig. Architecture for deployment in a CSP

Objective:

The application of these functions makes the re-encryptionscheme to lose the Multi-use feature, which isrequired as described in this paper. That is, oncea Re-encryption Key generated by rkgen pke() is used tore-encrypt, no further re-encryptions can be done to thatencrypted object. However, for the purposes of authorizationin this paper, this kind of re-encryption only needsto be done to re-encrypt the protected object under therequesting user public key. And this is done in the last reencryption,which is the one that results in the data beingencrypted under the user public key. Thus, re-encryptionkeys generated with the original rkgen () function shouldstill be applied for re-encryptions along the authorizationpath, except the one affecting the user, which is the last reencryption.

With this approach, the data owner uses the public keyof the user when defining rules in the authorization model.Upon a request, the data object is re-encrypted under therequesting user public key. This user can then decrypt thedata by using the corresponding private key. Hence, keymanagement results in managing public and private keypairs of PKE, which can be done by means of commonlyused and standard PKI solutions.

Problem Definition:

In the Existing system current security solutions are based on perimeter security. However, Cloud computing breaks the organization perimeters. When data resides in the Cloud, they reside outside the organizational bounds. This leads users control over their data and raises reasonable security concerns that slow down the adoption of Cloud computing. Is the Cloud service provider accessing the data? Is it legitimately applying the access control policy defined by the user? 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.

Existing disadvantages:

- Because of the decryption from the client sidealleviate ABE expressiveness limitation.
- ABAC may result in a large number of rules since a system with n attributes
- When the third party is introduced in between it set a great increase in the cost of maintenance.

Proposed Solution:

This paper presents a data-centric access control solution with enriched role-based expressiveness in which security is focused on protecting user data regardless the Cloud service provider that holds it. Novel identity-based and proxy re-encryption techniques are used to protect the authorization model.Data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider access or misbehavior. The authorization model provides high expressiveness with role hierarchy and resource hierarchy support. The solution takes advantage of the logic formalism provided by Semantic Web technologies, which enables advanced rule management like semantic conflict detection. A proof of concept implementation has been developed and a working prototypical

deployment of theproposal has been integrated within Google services.

Advantages:

- Data-centric solution with data protection for the Cloud Service Provider to be unable to access it.
- ABE with algorithmic specification reduces the overhead of decryption mechanisms that are mostly felt by the resource constrained systems.
- Since the algorithmic specification is to be specified by the destination itself here the need of the third party because the use of third party may sometimes lead to data leakage.

CONCLUSION

Information driven approval arrangement has been proposed for the safe security of information in the Cloud. SecRBAC permits overseeing approval taking after a principle based approach and gives enhanced part based expressiveness including part and protest progressions. Access controlcalculations are assigned to the CSP, being this not able to get to the information, as well as not able to discharge it to unapproved parties. Progressed cryptographic methods have been connected to ensure the approval model. A re-encryption key supplements every approval guideline as cryptographic token to secure information against CSP bad conduct. The arrangement is free of any PRE plan or usage to the extent three particular components is upheld. A solid IBPRE plan has been utilized as a part of this paper with a specific end goal to give a far reaching and possible arrangement.

A proposition taking into account Semantic Web advancements has been uncovered for the representation and assessment of the approval model. It makes utilization of the semantic components of ontology's and the computational abilities of reasoners to determine and assess the model. This likewise empowers the utilization of cutting edge strategies, for example, struggle identification and determination techniques. Rules for organization in a Cloud Service Provider have been likewise given, including a half and half approach good with Public Key Cryptography that empowers the use of standard PKI for key administration and dissemination. A prototypical execution of the proposition has been additionally created and uncovered in this paper, together with some trial comes about.

FEATURE ENHANCEMENT

Future lines of research include the analysis of novelcryptographic techniques that could enable the secure modificationand deletion of data in the Cloud. This would allowextending the privileges of the authorization model withmore actions like modify and delete. Another interesting pointis the obfuscation of the authorization model for privacy reasons.Although the usage of pseudonyms is proposed, butmore advanced obfuscation techniques can be researched toachieve a higher level of privacy.

REFERENCES

[1] Cloud Security Alliance, "Security guidance for critical areas offocus in cloud computing v3.0," CSA, Tech. Rep., 2003.

[2] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhou, "Feacs: Aflexible 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 KeyCryptography - PKC 2011, 2011, vol. 6571, pp. 53–70.

[4] B. B and V. P, "Extensive survey on usage of attribute basedencryption 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-basedencryption for fine-grained access control of encrypted data," inProceedings of the 13th ACM Conference on Computer and CommunicationsSecurity, 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 accesscontrol - policy enhanced," INCITS, Standard, Jul. 2012.

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

[8] Empower ID, "Best practices in enterprise authorization: TheRBAC/ABAC hybrid approach," Empower ID, White paper, 2013.

[9] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to rolebasedaccess control," Computer, vol. 43, no. 6, pp. 79–81, 2010.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "ImprovedProxy Re-encryption schemes with applications to secure distributedstorage," ACM Transactions on Information and SystemSecurity, vol. 9, no. 1, pp. 1–30, 2006.

[11] F. Wang, Z. Liu, and C. Wang, "Full secure identity-based encryptionscheme with short public key size over lattices in the standardmodel," 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 Cryptographyand Network Security, ser. ACNS '07. Berlin, Heidelberg:Springer-Verlag, 2007, pp. 288–306.

[13] A. Lawall, D. Reichelt, and T. Schaller, "Resource management andauthorization for cloud services," in Proceedings of the 7th InternationalConference 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 computingplatform 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 BerlinHeidelberg, 2009, vol. 5789, pp. 587–604.

AUTHORS

Mr.Bharathkumar Chebrolu Studying M.Tech (CSE) In St.Ann's College of Engineering & Technology, Chirala. He completed B.tech.(IT) in 2011 in chirala engineering college, Chirala

Dr.P.Harini is presently working as professor & Head, Department Of Computer Science & Engineering in St.Ann's College Of Engineering & Technology, Chirala. She completed Ph.D. in Distributed and Mobile Computing from JNTUA. She guided many U.G & P.G projects. She has more than 19 years of teaching and 2 years of Industry Experience. She published more than 20 International Journals and 25 research Oriented papers in various areas. She was awarded certificated of Merit by JNTUK, Kakinada on the University Formation day, 21st August 2012.