International Journal of Engineering Research and Management (IJERM) – Volume-4, Issue-1, March 2018

Enterprise Security and Authorization in the Clouds using RBAC

Miss. Suvarna S. Jondhale[#1], Prof. Shrinivas K. Sonkar[*2]

[1,2]Computer Engineering Department, AVCOE , Sangamner, India

[1]suvarnajondhale1694@gmail.com

[2]sonkar83@gmail.com

Abstract *— Cloud computing now offers organizations more choices regarding how to run infrastructures, save costs, and delegate liabilities to third-party providers. It has become an integral part of technology and business models, and has forced businesses to adapt to new technology strategies. Data security is by far the most challenging barrier to cloud adoption. Data is the most precious corporate asset, and companies want to know that their data is safe. Companies feel confident when they store data internally because they have full control over it. Load Balancing is one of the responses to these issues. RBAC approach manages such issue. The proposed strategy includes the FCFS with RBAC procedure. RBAC will allocate roles to the customers and customers with a specific role can just access the specific data. Subsequently identity administration and access management are implemented and utilizing this system.*

Keywords — *Role-based access control, cloud computing, role-based encryption, role-based encryption system architecture*

I. INTRODUCTION

Cloud gives numerous favourable circumstances as putting data on the cloud also gives relatively boundless capacity limit. Simple access to data gives authorization to information on cloud from anyplace if client is registered to it. On opposite side, cloud got numerous issues in regards to security particularly on Data burglary, Data loss and Privacy. Securing cloud from unauthorized users[2] and threats is a critical assignment for security suppliers who are responsible for the cloud as secure cloud is constantly solid wellspring of data. A Cloud is said to be great just when it is dependable and gives better security to clients. Regardless of whether cloud provider is giving secure cloud, he should ensure who can get to the information and who maintains the server.

Regularly, role based access control technique has three basic structures; clients, authorizations and roles. A role is a more elevated amount portrayal of access control. Client relate to certifiable clients of the registering framework. Client authentication can be refined independently; appointing clients to existing roles and relegating access benefits for articles to roles. Authorizations gives a portrayal of the entrance clients can need to objects in the framework and roles gives a depiction of the elements of clients inside system. In RBAC, there is hierarchical structure; a role can acquire get to authorization from another role. Following chart indicates connection between clients, roles and authorizations or permissions.

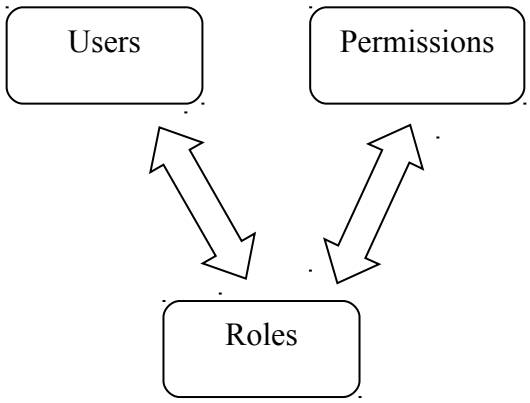

Fig. 1 Relation between users, permissions and roles

Data owner utilizes cryptographic methods to shield information from unapproved access for giving assurance to the security of their information and just those clients can get to information who approach authorization. Clients need to fulfil get to strategies to get to information. On the off chance that client fulfil the entrance strategies, client can decrypt data by utilizing his private key. The role based access policies are reinforced by utilizing role based encryption strategy (RBE).

The solution enables a rule based approach for authorization in Cloud systems where rules are under control of the dataowner and access control computation is appointed to the CSP, yet making it unable to grant access to unauthorized parties.

The main contributions of the proposed solution are:

- Data-centric solution within formation protection for the Cloud Service Provider to be not able 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 assigned to the CSP, yet being notable give access to unauthorized parties.
- Secure key distribution mechanism and PKI compatibility for utilizing standard X.509 certificates and keys.

Various feature of RBAC involves: first one, it provides the security of the data by limiting the roles to the users and another features of RBAC is, it reduces the transaction time of the data by limiting the users. Last one is backup of data can be taken.

II. Related Work

Reliably examined the security and protection issues in cloud computing in based on attribute-driven methodology. The authors ordered the security/protection qualities (e.g., confidentiality, integrity, availability, accountability, and privacy-serviceability) and in addition talked about the vulnerabilities, which might be abused by the aggressors to perform different assaults. Safeguard techniques and their methodologies were talked about too. The authors trust that this examination will be useful to shape the future research in the territories of cloud security and protection. All through the investigation, the creators got a shared objective to give a broad report of the current security and protection issues in cloud environments [1].

The fundamental issues emerging in the cloud while getting to the information and the security related issues and countermeasures to handle the issue. Issues like Unwanted Access, data segregation, vendor lock in, data romance, etc are covered in this paper [2].

Over viewed different distributed computing conditions and administrations created by different activities, for example, Google, force.com, Amazon, open source. The studied outcomes are utilized to recognize the comparable and diverse composition methodologies of distributed computing. Based on proposed taxonomy and technical studies, the author has assessed the distinctive cloud computing frameworks to give vital data that can help in future for the new advancements and change in existing frameworks. The proposed scientific categorization gives specialist and engineers the thoughts on the present cloud frameworks, build-up and challenges [3].

III. Techniques Used

The architecture of secure cloud storage system is presented in below figure

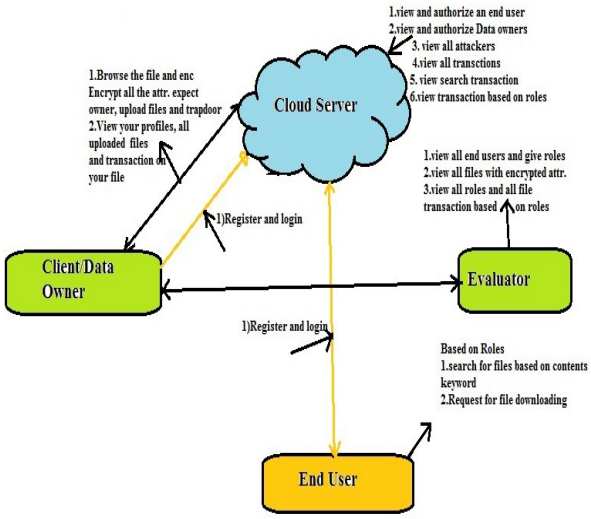

Fig. 2 System Architecture

The components of the system architecture are shown in Figure:

1. Cloud server: Cloud service providers offers its customers storage or software services available via a public network or private network. CSP is a company who is partially trusted. Whenever the user accesses the cloud service, the CSP validates the user and issues access attributes to users. The CSP also acts as the key distribution centre and also view and authorize the user. View all kinds of attackers, view all transactions, view transaction base on their roles, view all the data owners.
2. Data Owner (DO): Data owner is a cloud client who registers with the Cloud Service Provider. Data owner outsources data to cloud in encrypted form. Data Owner anonymously gets authenticated to cloud while getting duly authenticated. It is the duty of the Data Owner to prevent the admission of malicious Data Owner's to cloud.

Data owner browse the file and encrypt them and also encrypt owners, name uploads the files, view your profiles, view transaction on your file. This kind of operation is done with data owner.

3. Evaluator: In this component view all end users and given roles, also view all files with encrypted attributes, view all kinds of roles, view all transactions based on their roles.
4. End User (EU): End User is a cloud client who registers with the Cloud service Provider. Whenever a End user query for data to the CSP, the CSP provides a list of Data Owner who possesses the data. End User is also anonymous if they follow the rules of the Cloud Service Providers accordingly.

End user did the operation with the help of roles. It searches for files based on contents keywords, Request for file, and also request file for downloading with current sec key for the corresponding file from the cloud and decrypt, download.

Techniques used:

Encryption algorithms are mainly used to keep the data safe from any kind of attack. The best and the most efficient algorithms have to be used since the data is stored in a third party data centre and also large amounts of data transfer takes place during this process. Here, in this proposed solution, the Data Owner can choose any of the public-key encryption algorithms i.e. RSA to encrypt their data.

RSA algorithm is based on the difficulty of factoring large integers [6]. RSA user creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but only someone with knowledge of prime factors can possibly decode the message. The decryption of RSA cipher text is infeasible as there is no efficient algorithm for integer factorization.

There are two techniques are used that is-

1. PRE (Proxy Re-Encryption Encryption) – key pair α and β

-The proxy could re-encrypt a cipher text Cα encrypted under α public key to another cipher text Cβ that can be decrypted using β private key.

- A user uα can encrypt a piece of data m using his own public key pubα to obtain a cipher text cα a re-encryption key rkα->β then another user uβ can use his own private key priβ to decrypt cβ & obtain the plain text data m. and another technique is below.

2. Identity based Encryption:

-A piece of data m can be encrypted using the identity idα of user uα to obtain a cipher text Cα then user Uα can use his private key priα to decrypt Cα & obtain plain piece of data m. e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user.

In RBAC combine these two techniques to form IBE-PRE.

3. IBEPRE

-A user Uα can encrypt a piece of data m using his identity idα to obtain a cipher text Cidα encrypted under idα .

-A re-encryption key rkα -> β can be generated to re-encrypt from idα to idβ to obtain another cipher text Cidβ under the identity of another user Uβ.

-This can use his own secret key Skβ to obtain the plain piece of data m.

It allows an authorized proxy to convert a cipher text of an identity-based broadcast encryption (IBBE) scheme into a cipher text of an identity based encryption (IBE) scheme. This can use his own secret key to obtain the plain piece of data.

IV. Conclusion

The disadvantage towards the quickened development of cloud computing is information security and protection issues. Analysts have proposed various strategies for information insurance and to accomplish larger amounts of information security in the cloud. There are frameworks which enable verified clients to speak with each other in a encrypted form. Those frameworks offer solid encryption and secrecy through confirmed clients yet they don't focus around unknown authentication. There might be frameworks which gives unknown authentication to clients however doesn't focus on confidentiality. This work consolidates a mysterious confirmation for an enlisted client alongside RSA encryption methods and furthermore gives privacy and integrity where the cloud customers can send encrypted messages to each other.

For secure cloud environment, the following methods were proposed to protect user's privacy and security of data:(1) Proxy Re-Encryption Encryption (2) Identity based Encryption (3) IBEPRE. This solution provides a good secure and anonymous communication system for all users.

Acknowledgment

I would like to thank my project coordinator and Guide Prof. S.K. Sonkar for the valuable advice and support he has given me in writing of this paper. I would also like to thank my teachers for their encouragement, guidance, understanding and support.

References

[1] 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,

[2] B. B and V. P, "Extensive survey on usage of attribute based encryption in cloud," Journal of Emerging Technologies in Web Intelligence,

[3] InterNational Committee for Information Technology Standards,

[4] "INCITS 494-2012 - information technology - role based access control - policy enhanced," INCITS, Standard, Jul. 2012.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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

[11] 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.

[12] W3C OWL Working Group, "OWL 2 Web Ontology Language: Document overview (second edition)," World Wide Web Consortium(W3C), W3C Recommendation, Dec. 2012.