https://dx.doi.org/10.22161/ijaers.4.2.5 *ISSN: 2349-6495(P) | 2456-1908(O)*

A Survey on Data control from sender using cloud computing

I.Subhashree, S.Swetha, S.Vanmathi, Muthukumarasamy.S

Department of computer science and engineering, S.A Engineering College, Chennai, India

Abstract*—To store data more efficiently in cloud security must also be taken into considerations. When certain information is stored in Cloud, it actually means that it resides outside an organization's structure bounds. This results in loss of data and information which leads to low cost security issues that, reduces adoption of Cloud computing techniques. This paper surveys mainly on data-centric access control with enriched role-based quality focusing security as a target, protecting user information despite the Cloud service provider that holds it. It also deals with identity based encryption and proxy re-encryption techniques to protect the authorization model.*

Keywords—authorization, cloud computing, data centric access control, role based access control systems.

I. INTRODUCTION

Cloud computing is widely preferred by all the users since it provides remote access to data or information that is stored in it. When a data gets stored into cloud storage it usually depends on the cloud service provider to strengthen the security of that data. Generally, the service level agreement takes up these responsibilities where the cloud service provider could retrieve the data or can even provide it to the other third party services that are unauthorized. This problem could be practically detected in the inter cloud scenarios where data may flow from one service to another service provider where it becomes a complex one. Hence instead of securing the networks or an application it would be better to improve security to the data itself by following a data centric approach. Also to enhance security, role based access control approach is used which guarantees restrictions for unauthorized user access. An enterprise comprising a large number of workers prefers this methodology. In order to protect the functions of authorization model identity based encryption and proxy re-encryption techniques can be widely adopted.

II. REALTED WORKS

G. Ateniese et.al. [1] Proposed an approach that was used to enhance confidentiality which converts a cipher text for a user without the knowledge about the plaintext involved in that process. In practice this work showed that it can process effectively. This kind of re-encryption scheme also can provide secure file systems that enhances security. They had proposed works with proxy re-encryption, double decryption, key translation, bilinear maps. This method supports various applications like, e-mail forwarding, and content distribution. When the proxy possesses both the keys simultaneously it makes the approach to a weaker re-encryption scheme. Here one key decrypts a plaintext and the other encrypts it. The main advantage of this method is that, it does not reveal either of the keys. Cryptographically improvements were made on access control server models with the help of proxy where the encryption keys are provided by the master keys. Significant advantages where bought up in access control levels of the system involved.

R. Bobba et.al. [2] proposed an encryption algorithm which itself specializes in all the policies which helps it to work with in real time environments. Works were proposed based on cipher text policy attribute based encryption. They mainly work on growing the flexibility. Though challenges were quite hard to overcome in constructing the cipher text policy attribute set based encryption, changes were also made to the cipher text policy attribute based encryption from a monolithic set into a recursive set based structure. This system mainly supports many practical situations and the main advantage is its versatility. Here in order to improve the efficiency and performance, two level cipher text policies are implemented which optimizes the decrypting function. Performance overheads are also evaluated here with the help of prototypic implementation. Future research can be made by extending the study of this scheme.

E. Coyne et.al. [3] discusses about the role based access control and attribute based access control.Anyway both the approaches deals with roles and attributes. Under role based access control approach gives group permission only if all the permissions were given through RBAC systems. This makes it a simple way to provide groups of user by assigning roles. Attribute based access control systems are

https://dx.doi.org/10.22161/ijaers.4.2.5 *ISSN: 2349-6495(P) | 2456-1908(O)*

also implemented to enhance other attributes like time and user location. This method also offers an attachment to Role based systems. Role based systems has been widely used for its administrative advantages and security purposes. But it's outmoded and it may not deal with real-time implementations. When compared attribute based access control is newer and provides wide range of support to real-time implementations. RBAC and ABAC can be combined to work efficiently. RBAC and ABAC are similar it is up to the property of each model that supports its behavior.

V. Goyal et.al. [4] focuses on key policy attribute based encryption. For security concerns the data being shared over the internet is being encrypted but anyway there also lies a disadvantage in it which is found when the keys are shared at the fine grained coarse level. In order to avoid this problem they have implemented a new cryptosystems where cipher texts were provided with set of attributes and private keys where both are provided with access structures. A new technique was also adopted to work with fine grained access control systems where only encrypted data gets stored in the server. Though different information lies in the server, different users can decrypt the data under the security policy that has been followed. It also focuses on hierarchical identity based encryption to deal with more complex process. This implementation mainly benefits complex policies.

Lawall et.al. [5] mainly emphasized to work on the problem of managing the access rights the resources, of a virtual organization located at cloud providers. So work has been implemented for the automatic deployment of resources where works regarding the resource and authorization management were handled under hybrid cloud environment. The separation of resources was not directly given to the cloud provider. This increases security concerns. This implementation makes the intrusion more complex since the attackers cannot have direct access since the authorization model is not located in same location. This model contains system resources that are made independent of whether they are in-house or leased from a provider. Here conflict arises between the infrastructure and elements of an organization which can be dealt by assigning permissions between all the systems involved. This implementation differs from one organization to other since each organization prefers a different practice.

J. Liu et.al. [6] focuses on the cipher text policy attribute set based encryption which was mainly implemented to increases security and scalability. By this technique an authorized user can access the data without any constraints. Considerations were also made on hierarchical attribute set based encryption which resulted in a high level of security for user data. Data owner manages the encrypted data which would be easy to eliminate data replication in the cloud environment. Under this process, data consumer can have access to the resources directly from the data owners. Attribute authority is used to verify the level of the data consumer and provides a packet with the level and key structure encrypted by a notification key. This work is far more secure and scalable because of the implementation of both the cipher text policy and hierarchical attribute set based encryption schemes. The main advantage of this method is that the cost of computation is reduced.

G. Wang et.al. [7] proposed hierarchical attribute based encryption in order to focus on achieving high performance and full delegation. Since all functions are performed through networks, it there arises a need to secure the data. This access control method allows exceptional access over the encrypted data. Under the key policy extract discussed here, the primitive enables senders to encrypt messages. New security feature for various organizations are achieved with the help of hierarchical attribute based implementation. Cipher text policy manages control over the encryption and decryption of the data. Data is securely controlled by the domain authorities. This process also enhances the fine grained access control. This system follows hierarchical structure agreement with access control permissions. With the help of the algorithm preferred here, the proposed scheme can be implemented to promote its level of efficiency over existing systems**.**

F. Wang et.al.[8]proposed a method called as efficient identity based encryption scheme to achieve security at the lattice based systems, which can be made fully secure without random oracles. First presented identity based encryption was on constructions of hierarchical identity based encryption which was not able to deal with the practical implementations as it was concerned with certain limitations. Later, reduced the security of this scheme to decisional bilinear diffiehellman problem. In future this technique can be adopted to build a new signature scheme which could be more secure under the computational Diffie-Hellman assumption.

B. waters [9] proposed a new methodology for representing the cipher text policy attribute based encryption approach. But the construction process resulted in some limitations in the implementations of that new methodology. Hence three constraints were preferred within the framework; the first system was decisional parallel bilinear diffiehellman exponent assumption which was selectively secure.

https://dx.doi.org/10.22161/ijaers.4.2.5 *ISSN: 2349-6495(P) | 2456-1908(O)*

Following two construction models provided performance tradeoffs to attain security assumptions. One main disadvantage with this approach is that it has only one threshold gate at the earlier stages of constructions with limited capabilities. This lack of satisfaction resulted in the cipher text policy attribute based encryption technique which achieves all the advantages as expected.

Y. Zhang et.al. [10] focused on flexible and efficient access control system that could bring out important features like scalable, flexible, and fine-grained access control in cloud computing. So a hierarchical attribute set based encryption had been proposed by extending the cipher text policy attribute set based encryption which follows a hierarchical structure of implementation. This scheme was mainly focused to make secure data sharing in cloud environment with the help of adaptive access control schemes to achieve scalability and flexibility by also following key policy attribute based encryption. The security of hierarchical attribute set-based encryption is concerned on the security of the cipher text policy attribute based encryption scheme. Main security concerns deals with privacy and data security in cloud.

III. FIGURES

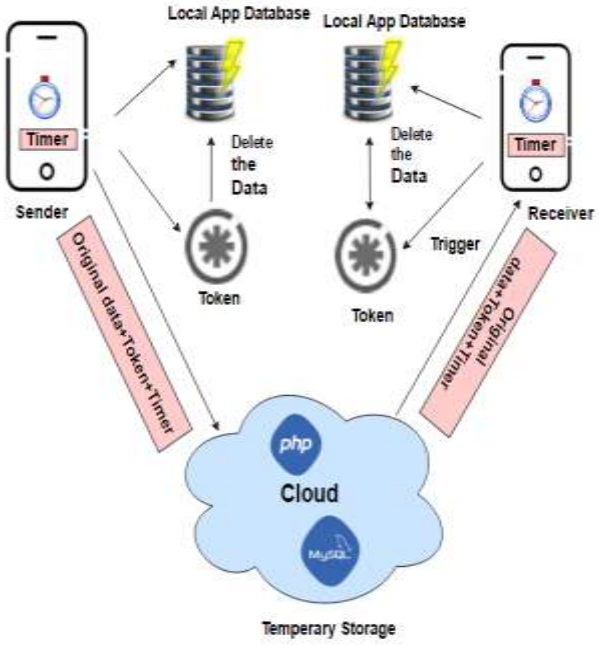

Fig. 1: architecture diagram

The above proposed diagram is based on the sender and the receiver interaction. Sender sends the data to the receiver where a token and timer is also generated along with the data that is being transferred. The token and the timer will permit the receiver to have access on the data for a specific period of time which also secures the data from the receiver without mishandling the information for security concerns. It gets stored in the cloud until it reaches the receiver. When the data is transferred over the cloud to the receiver, the token and the timer complementing the data will reside in the local application database of the receiver. Once when the receiver retrieves the data the timer and the token gets activated from the local app database of the receiver and will not be available after the specified period of time. This strengthens the security of the data.

IV. CONCLUSION

When a data centric access control solutions are preferred, it would be more helpful to provide secure protection of the data in the cloud. This helps to possibly manage authorization techniques with the use of role based access controls which manages access permissions of authorized users. Semantic web technologies are widely preferred to evaluate the performance of the authorization model. Once a cloud service provider is given access control privileges it can not only make direct access to the data but also cab retrieve the data to unauthorized or third party services. So when we prefer a timer and a token approach it would enhance the security of the data which prevents the data disclosure to unauthorized users. Hence advanced techniques can be implemented to protect the authorization model.

REFERENCES

[1] G. Ateniese et.al., "*Improved Proxy Re-encryption schemes with applications to secure distributed storage,"* ACM Transactions on Information and System, Security, vol. 9, no. 1, pp. 1–30, 2006.

[2] R. Bobbaet.al., "*Attribute-sets: A practically motivated enhancement to attribute-based encryption*," in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 587–604.

[3] E. Coyne et.al.,*"Abac and rbac: Scalable, flexible, and auditable access management*," IT Professional, vol. 15, no. 3, pp. 14–16, 2013.

[4] V. Goyalt.al., "*Attribute based encryption for fine-grained access control of encrypted data*," in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, New York, NY, USA, 2006, pp. 89–98.

[5] A. Lawall et.al., "*Resource management and authorization for cloud services*," in Proceedings of the 7th International Conference on Subject-Oriented Business Process

https://dx.doi.org/10.22161/ijaers.4.2.5 *ISSN: 2349-6495(P) | 2456-1908(O)*

Management, ser. S-BPM ONE '15, New York, NY, USA, 2015, pp. 18:1–18:8.

[6] J. Liu et.al., "*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.

[7] G. Wang et.al., "*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.

[8] F. Wang et.al.,"*Full secure identity-based encryption scheme with short public key size over lattices in the standard model*", posted online: 16 Mar 2015.Publishedonline: 09 Apr 2015.

[9] B. Waters, "*Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization*," in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp.

[10] Y. Zhang et.al., "*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.