IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Adaptive Secure Document Access Mechanism in Cloud

Dr. M. Priyadharshini[1], P. Anitha[2], C. Janani[3]

Associate Professor, CSE Department, KPR Institute of Engineering and Technology, Coimbatore, India[1]

UG Student, CSE Department, KPR Institute of Engineering and Technology, Coimbatore, India[2, 3]

Abstract: Cloud data storage has provided massive benefits by allowing users to store huge amount of data in cost-effective manner. To protect the privacy of data stored in the cloud, cryptographic role-based access control (RBAC) scheme combined with context information have been proposed and developed ensuring the restricted access of the documents. The system holds role and context information that enables the upload and download of documents by legitimate users. The security mapper component filters the user information so as to perform adaptive secure document access in cloud.

Keywords: Role-based access control, Context-based access, cryptographic RBAC, secure cloud data storage.

I. INTRODUCTION

In recent days there is a rapid growth in the development of online services. The major benefit of using online services is that users can store their data online and access it from anywhere. Cloud storage services are providing solutions to store and manage increasing amount of users' data stored online. This has raised several security issues such as how to control and prevent unauthorized access to data stored in the cloud. The privacy of the data stored in the cloud is enabled using access controls mechanisms. Many access control models for securing document access have been proposed over the years in the literature. RBAC is a well-known access control model that helps simplification of security provisioning especially in large-scale systems. In RBAC, roles are used to associate users with permissions on accessing resources. Instead of individual users, permissions are allocated to users based on the roles they hold. In traditional systems, access control policies are usually specified and enforced by a central authority.

However in a distributed system such as a cloud, there may not exist such a central authority as the data may be stored in distributed data centers which cannot be under the control of a single authority. In order to enforce the security policies for encryption and decryption of outsourced data we used the cryptographic algorithm combined with the access control. In pervasive environment, there may exist interaction between any devices or entities without the same owner and no prior knowledge of the entities are available. It is very difficult to define the boundaries for security measures. To overcome this we are including context as one of the important parameter to find the trustworthiness of the entities which will participate in accessing the services. More mobile devices are utilized in accessing the services anywhere, anytime all around the world in this electronic universe. Access Control Polices includes user identity, time of interaction, and location from where the request arises. XML is used to define these access control information of a user with corresponding role and context information. This scheme is more flexible since the access depends on the roles as well as the location and time of accessing the requested documents.

II. ADAPTIVE SECURE DOCUMENT ACCESS MECHANISM

In the proposed system, an adaptive secure access mechanism for access of cloud data remotely is enabled. The approach utilizes the access control information in form of XML or database. The proposed system is designed so as to facilitate the project development environment where, the project related files are accessed from anywhere through the remote devices like Laptop, Personal PC, Mobile etc.., Each individual is assigned the role and context information on ensuring which the document access is permitted for the users. The adaptive secure access mechanism proposed is implemented using ASP.NET and access information storage in form of XML or SQLSERVER database. The primary components involved in the Adaptive secure document access mechanism are Adaptive Security Mapper (ASMapper), ASDA Validation Handler that parses and provides secure access information to the ASMapper. The other components include encryption and decryption modules, user interface and login module at one end and the cloud server at the other end.

The proposed architecture shown in the Fig.1 clearly depicts the various components of Adaptive secure document access mechanism among which the ASM Mapper and Validation handler are very important in arriving the conclusion of document access with the access information available.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

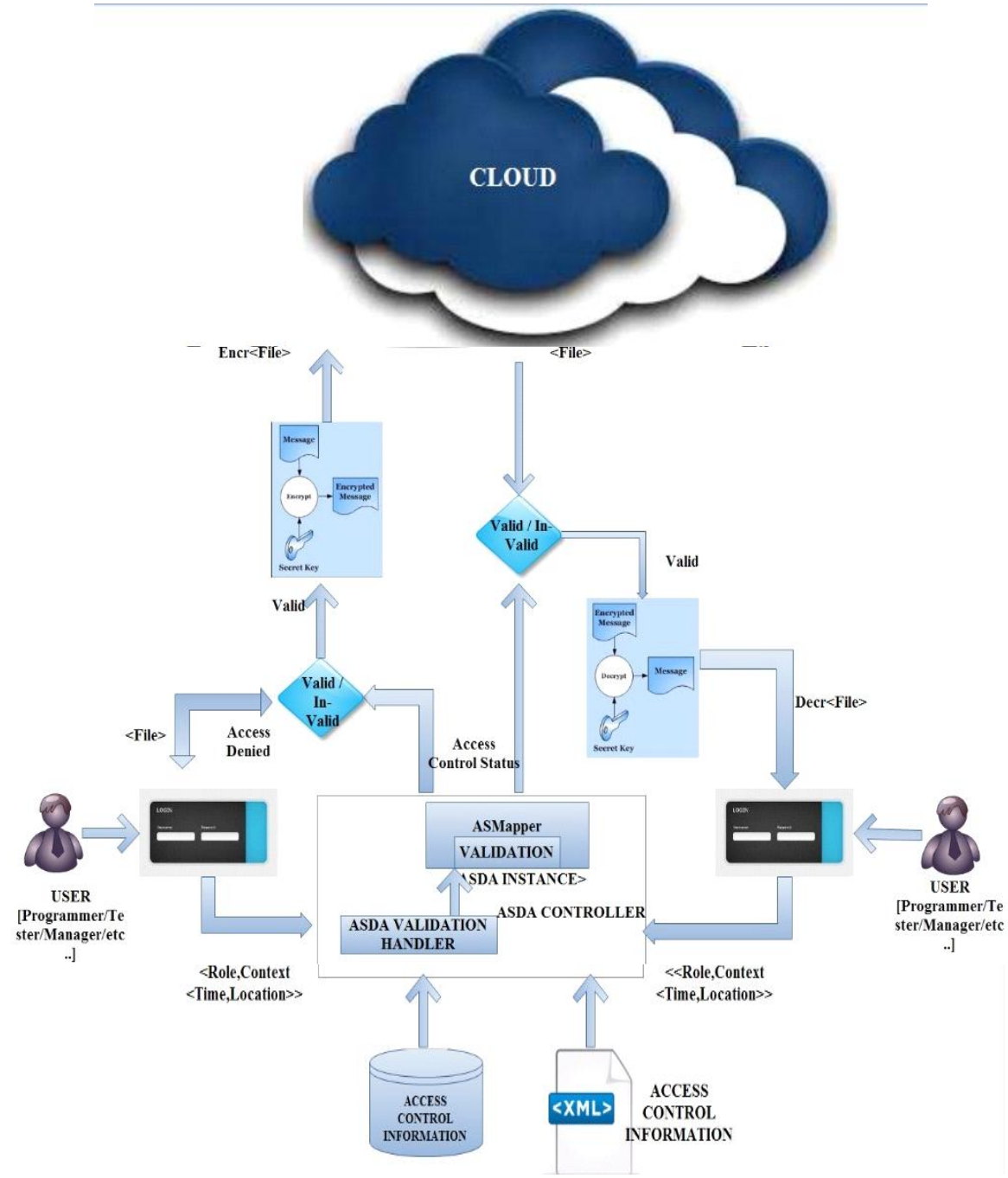

Fig.1 Adaptive Secure document access mechanism

III. ADAPTIVE SECURITY MAPPER

ASMapper takes XML or database of Access Control Information from the cloud server, when there is a request from user on login. ASMapper filters the role and context information of the user who has logged in and validates his access using validate( ) method of ASDA validation handler.

validate( ) does a sequence of action as follows:

BEGIN
Verify <ASDA Instance> with <Request>
If <Access Control Status> = = Valid
Encr<File/Document>/ Decr<File/Document>
Else
<Upload/Download Failure> status
to User
END

The User in the system refers to the Programmer, Tester, Manager etc., involved in the Development of Software. The Login of same user with different roles yields different responses on request even considering the context of login and access.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

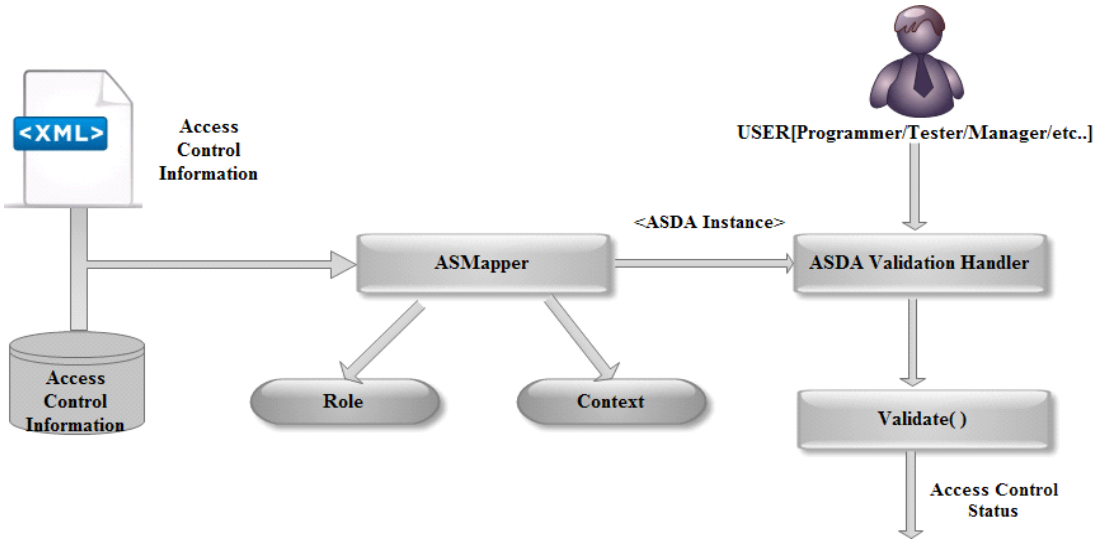

Fig.2 Adaptive Security mapper

IV. LITERATURE

RBAC mechanism to overcome issue in MAC and DAC has been proposed [1] in which access control is based on the functions; a user is allowed to perform within an organization. Transaction to roles and membership in roles are allocated by system administrator. There is no common accepted definition and standards encompassing RBAC. Evaluation and testing programs for this system have not been established. It addresses security for application not for OS. Vimercati et.al, [2] proposed approaches for enforcing authorization policies and support dynamic authorization and data updates at limited cost in terms of bandwidth and computational power; BEL and SEL were used for data encryption. Major issue includes integration with web paradigm and efficient execution of queries. Collusion risk occurs during two layer encryption. A crucial problem to be addressed in data outsourcing is the enforcement of selective authorization policies and support of policy updates in dynamic scenarios. "Selective encryption" with two layers of encryption BEL and SEL is proposed. It is based on indexing information stored together with encrypted data. Current solutions suffer from limitations requiring the involvement of owner every time. It also has collusion risk. The access policies based on data attributes has been defined [4] that allow data owner to face difficulty to provide fine grain access control to untrusted cloud servers. ABE, re_encryption, key policy attribute based encryption is used. Confidentiality of user access privilege and user secret key accountability need to be improved. "RBE scheme with revocation mechanism" [5] based on key hierarchy structure allows sender to directly specify a role for encrypting data which can be decrypted by all senior roles and revoke by any subgroup of users and roles. More comprehensive role based cryptosystem to support various secure mechanisms need to be implemented along with the performance. RBE mechanism uses broadcast encryption algorithm which improves security against attacks and the cloud providers are not supposed to decrypt the data. The method is best suited for large scale systems. Here, authorizations are granted to roles instead of to single users. Authorizations granted to a role are strictly related to the data objects and resources that are needed by a user in order to exercise the functions of the role. The role definitions could also be reused. Separation of Duties[SOD] aims at reducing the risk of fraud by not allowing any individual to have sufficient authority within the system to perpetrate a fraud on his/her own. Power and complexity of RBAC models still need to be addressed. There are still relevant application requirements not addressed by current RBAC models and mechanisms [6]. RBAC [7] provides a powerful mechanism for reducing complexity, cost, and potential for error in assigning user permissions within the enterprise. RBAC that were chosen to be included represent stable and well accepted set of features described in RBAC included in commercial implementations. A scheme [8] based on cryptography is proposed for access control in a system where hierarchy is represented by a partially ordered set. Authorized users are allowed to retrieve independently as soon as it is stored or broadcast by central authority. But anyone with the proper receiving equipment can intercept the message but has access to the information it contains only if in possession of the right key. Different relevant types of trust are identified and classified [9]. Formalism for expressing trust relations is presented along with an algorithm for deriving trust relations from recommendations. Examining execution paths[10] and in particular their relationship to trust paths is difficult. Specifying and developing protocols to reflect the cases in which it is not necessarily known a-priori who each of the players trusts in what respect. Different strategies would correspond to different assumptions about the likely trust relation structures. Using these cryptographic schemes, the owner of data can encrypt the data in such a way that only the users with appropriate roles as specified by a role-based access control policy can

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

decrypt and view the data. The proposed trust model takes into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. [11] TCAC extends the traditional RBAC model with the notion of trust and context. It model is flexible, scalable, and well suitable for the dynamic and distributed systems. It integrates the trustworthiness and context information into the traditional RBAC. Important issue is how to prevent the privacy such as location information from disclosure when capturing the context information. A domain space has been created, where the user identification is already available and the initial trust value for every service is initiated [12]. Also the access rights and their roles are stored in server database. The identity of user may be UID or IP address. The domain categorization with respect to the level of security for the services is not available. It is not possible to add some user profile to act as an identity to avoid malicious nodes or anonymous user.

V. CONCLUSION

In this paper, we have addressed role and context issues in cryptographic ADSA systems for securing data storage in a cloud environment. The system assists the development environment to create flexible access policies, and cryptographic algorithms to ensure that these policies are enforced in the storage of data in the cloud. In future the system could be aimed at extending the access of data over multiple peer organizations with trust information.

REFERENCES

[1] D. F. Ferraiolo and D. R. Kuhn, Role-based access controls, Proc. 15th NIST-NCSC Nat. Comput. Secur. Conf., 1992, 554–563.
[2] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi,and P. Samarati, A data outsourcing architecture combining cryptography and access control, Proc. CSAW, 2007, 63–69.
[3] S. D. C. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P.Samarati, Over-encryption: Management of access control evolutionon outsourced data, Proc. VLDB, 2007, 123–134.
[4] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving secure, scalable, and fine-grained data access control in cloud computing,, Proc. IEEE INFOCOM, 2010, 1–9.
[5] Y. Zhu, H.-X. Hu, G.-J. Ahn, H.-X. Wang, and S.-B. Wang, Provably secure role-based encryption with revocation mechanism, J. Comput. Sci. Technol., 26(4), 2011,. 697–710.
[6] L. Zhou, V. Varadharajan, and M. Hitchens, "Enforcing role-based access control for secure data storage in the cloud," Comput. J., vol. 54,no. 10, pp. 1675–1687, Oct. 2011.
[7] S.Chakraborty and I. Ray, TrustBAC: Integrating trust relationships into the RBAC model for access control in open systems, Proc. SACMAT, 2006, 49–58.
[8] F. Feng, C. Lin, D. Peng, and J. Li, A trust and context based access control model for distributed systems, Proc. HPCC, 2008, 629–634.
[9] M. Toahchoodee, R. Abdunabi, I. Ray, and I. Ray, A trust-based access control model for pervasive computing applications, Proc. DBSec, 2009, 307–314.
[10] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, Role-based access control models, IEEE Comput., 29(2), 1996, 38–47.
[11] R. Sandhu, D. Ferraiolo, and D. Kuhn, The NIST model for role based access control: Towards a unified standard, Proc. RBAC, 2000, 47–63.
[12] S. G. Akl and P. D. Taylor, Cryptographic solution to a problem of access control in a hierarchy,ACM Trans. Comput. Syst., 1(3), 1983, 239–248.
[13] M. Blaze, J. Feigenbaum, and J. Lacy, Decentralized trust management, Proc. IEEE Symp. Secur. Privacy,1996,164–173.