IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 2 (Jan. - Feb. 2013), PP 28-31
www.iosrjournals.org

Intrusion Detection of Masquerading Attacks & Secure Authentication in Cloud

[1]Swati P. Ramteke, [2]Priya S. Karemore, [3]S.S. Golait
[1]swatiofficial01@gmail.com, [2]priya.karemore@gmail.com, [3]snehal.golait@gmail.com
[1,2,3]Priyadarshini College of Engineering,Nagpur

Abstract : *This paper proposed for a new authenticated access control scheme for securing data in cloud system. In this scheme cloud system verifies the authenticity of user and provides access control only to applicable user to decrypt the stored data. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. By impersonating legal users, intruders can use the copious resources of cloud computing environments. CIDS also provides a component to summarize the alerts and inform the cloud administrator. CIDS architecture is scalable and elastic with no central coordinator. This paper also describes the components, architecture, detection models, and advantages of CIDS.*

Keywords - *Authentication, Attribute-based signatures, Attribute-based encryption, intrusion detection, and masquerade attacks*

I. INTRODUCTION

Research in cloud computing is receiving a lot of attention from both academic and industrial worlds. The trend of using cloud environments is growing for storage and data processing needs. Cloud computing is an Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand. It is very costly and cumbersome to manage database systems in-house especially for small or medium organizations. Data-as-a-Service (DaaS) hosted in the cloud provides an attractive solution, which is flexible, reliable, easy and economical to operate, for such organizations. However security and privacy issues concerning the storage of the data in the cloud and access via the Internet have been major concerns for many organizations. However, a major barrier for cloud adoption is real and perceived lack of security. Hence, they should be strongly protected.

The idea is to construct a new privacy preserving access control scheme for securing data in clouds. The cloud verifies the authenticity of the user without knowing the user's identity before storing information. It has the added feature of access control in which only valid users are able to decrypt the stored information. This is also prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches. Organizations enjoy all the benefits of data in the cloud while at the same time organization used a framework for "CIDS" a cloud based intrusion detection system, to solve the deficiencies of current IDSs. CIDS also provides a component to summarize the alerts and inform the cloud administrator. CIDS architecture is scalable and elastic with no central coordinator. This describes the components, architecture, detection models, and advantages of CIDS.

Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking).

There are broadly three types of access control:
1.User Based Access Control (UBAC),
In UBAC, the access control list (ACL) contains the list of users who are authorized to access data. This is not feasible in clouds where there are many users
2.Role Based Access Control (RBAC),
In RBAC users are classified based on their individual roles. Data can be accessed by users who have matching roles. The roles are defined by the system. For example, only faculty members and senior secretaries might have access to data but not the junior secretaries.
3.Attribute Based Access Control (ABAC).

The ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data. For instance, in the above example certain records might be accessible by faculty members with more than 10 years of research experience or by senior secretaries with more than 8 years experience.

II. Cloud Intrusion Detection System

Cloud computing has a broad appeal because it enables IT managers to provision services to users faster and in a cost-effective way. However, it does raise some concerns and chief among them is securing data in the cloud because of their operational models, the enabling technologies, and their distributed nature, clouds are easy targets for intruders. While intrusions can be handled by an Intrusion Detection System (IDS) , current IDSs have many deficiencies which hinder their adoption in a cloud environment. This paper describes CIDS, a framework for a Cloud based Intrusion Detection System to deal with attacks like:

(1) Masquerade attacks: where threats impersonate legitimate users,

- This is a PaaS attack tht includes any attack that impersonates a legitimate user to use service resources maliciously.
- This is by far the most critical attack, as its exploitation is rather easy.
- An intruder masquerades as a legal user by obtaining the user’s password and this leaves some trails left at the service location.
- CIDS detects this attack through HSGAA.

(2) Host-based attacks: these can be a consequence of masquerade attacks and generally result in an observable user behavior anomaly and

(3) Network-based attacks. CIDS also summarizes the intensive network based IDS alerts according to the attack signature and target.

III. SECURITY PROVIDED TECHNIQUES

By using encryption, the cloud server is prevented data stored in cloud from malicious user

All these work use a cryptographic primitive known as Attribute Based Encryption (ABE).and Attribute Based Signature (ABS).

1 .Attribute Based Encryption

Standard encryption is inefficient when selectively sharing data with many people, since the data needs to be encrypted using every user's public key. ABE can be implemented by

a. Key-policy ABE:-

1 .KP-ABE the sender has an access policy to encrypt data.

2. The receiver receives attributes and secret keys from the attribute authority

3. decrypted data if matching occur

2. Attribute Based Signature

In the case of attribute-based signatures (ABS), users obtain from an authority their secret keys as a function of the attributes they hold, with which they can later sign messages for any predicate satisfied by their attributes. A verifier will be convinced of the fact that the signer’s attributes satisfy the signing predicate while remaining completely ignorant of the identity of the user. Some feature of ABS are given below

- Users have a claim predicate associated with a message.
- The claim predicate helps to identify the user as an authorized user
- Other users or the cloud can verify the user and the validity of the message stored.

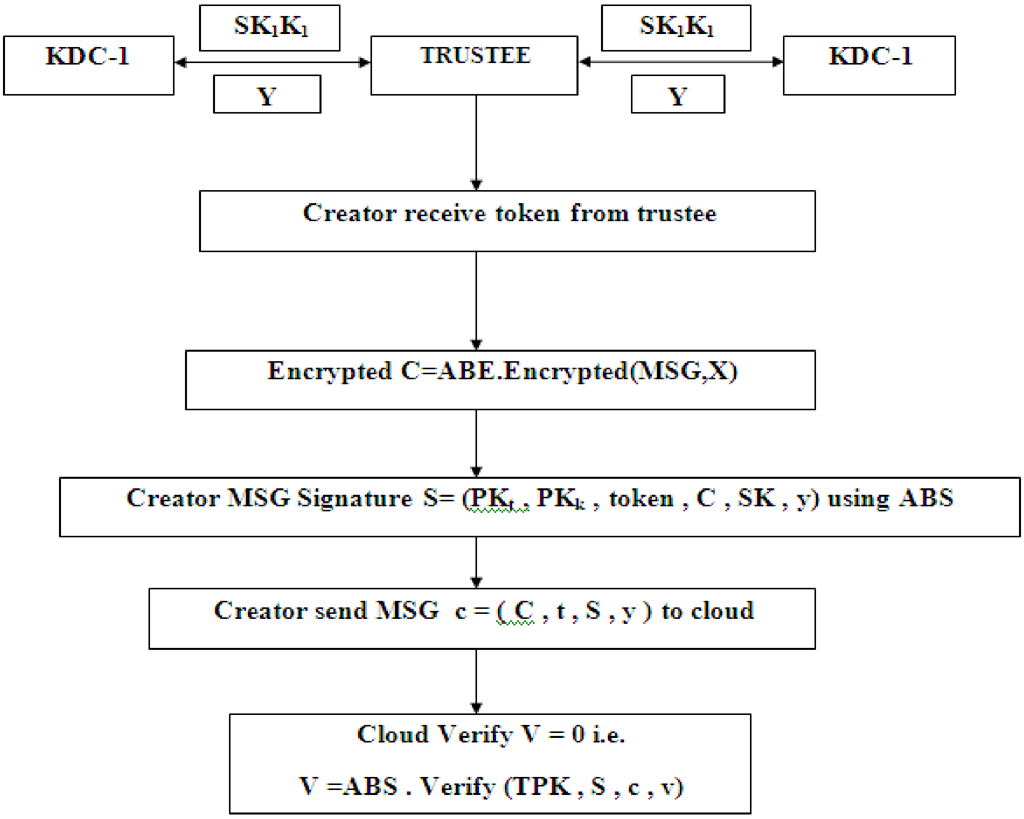
KDC-1
SK_1K_1
Y
TRUSTEE
SK_1K_1
Y
KDC-1
Creator receive token from trustee
Encrypted C=ABE.Encrypted(MSG,X)
Creator MSG Signature S= (PK_t, PK_k, token , C , SK , y) using ABS
Creator send MSG c = (C , t , S , y) to cloud
Cloud Verify V = 0 i.e.
V =ABS . Verify (TPK , S , c , v)

Figure 1: Flowchart for ABE & ABS

IV. INTRUSION DETECTION OF MASQUERADING ATTACKS

Audit exchange model

In this model nodes exchange their audit data among each others for current data. The detection phase depends on two parameters:

(1) The alignment score computed

(2) Alerts fired by the HIDS component.

In this way, the detection overhead is balanced among nodes with no single point of failure.

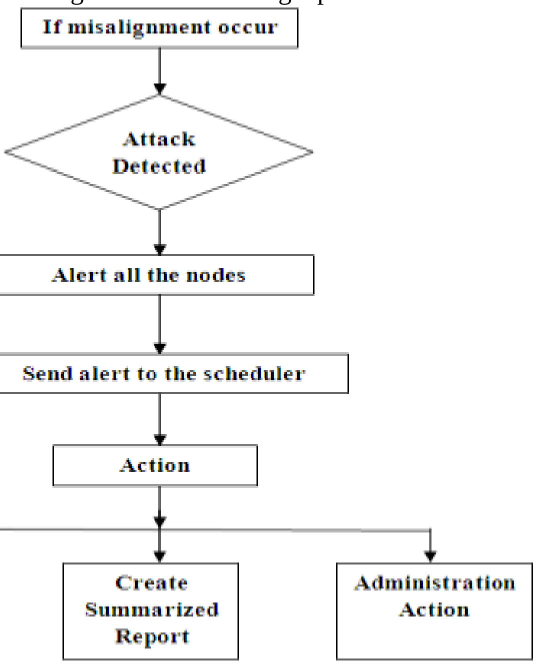

Figure 2: Audit Exchange Model

V. CONCLUSION

This paper presents the secure authentication to access policies of cloud. Our scheme not only provides fine-grained access control but also authenticates users who store information in the cloud. Under such conditions, the authenticity of the data must be verified by the users. Also, it may be very important to hide the identity of the users and owners, at the same time provide their authentication. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data & applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required.

Acknowledgements

The making of the paper needed co-operation and guidance of a number of people. We therefore consider it our prime duty to thank all those who had helped us for making it successful. It is our immense pleasure to express our gratitude to prof. Priya S. Karemore & Prof S. S. Golait (Priyadarshini College of Engineering)as a guide who provided us constructive and positive feedback during the preparation of this paper. Last but not least, We are thankful to our friends and library staff members whose encouragement and suggestion helped us to complete our seminar. We are also thankful to our parents.

REFERENCES

[1] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy keyword search over encrypted data in cloud computing,” in *IEEE INFOCOM.* 2010, pp. 441–445.

[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in *Financial Cryptography Workshops*, ser. Lecture Notes in Computer Science, vol. 6054. Springer, 2010, pp. 136–149.

[3] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-based authentication for cloud computing,” in *CloudCom*, ser. Lecture Notes in Computer Science, vol. 5931. Springer, 2009, pp. 157–166.

[4] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.

[5] A.-R. Sadeghi, T. Schneider, and M. Winandy, “Token-based cloud comput-ing,” in *TRUST*, ser. Lecture Notes in Computer Science, vol. 6101. Springer, 2010, pp. 417–429.

[6] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, “Trustcloud: A framework for accountability and trust in cloud computing,” HP Technical Report HPL-2011-38. Available at http://www. hpl. hp. com/ techreports /2011/HPL-2011-38.html.

[7] D. F. Ferraiolo and D. R. Kuhn, “Role-based access controls,” in *15th National Computer Security Conference*, 1992.

[8] D. R. Kuhn, E. J. Coyne, and T. R. Weil, “Adding attributes to role-based access control,” *IEEE Computer*, vol. 43, no. 6, pp. 79–81, 2010.

[9] M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings,” in *SecureComm*, 2010, pp. 89–106.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in *ACM ASIACCS*, 2010, pp. 261–270.

[11] G. Wang, Q. Liu, and J. Wu, “Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,” in *ACM CCS*, 2010,735–737.

[12] F. Zhao, T. Nishide, and K. Sakurai, “Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems,” in *ISPEC*, ser. Lecture Notes in Computer Science, vol. 6672. Springer, 2011, 83–97.

[13] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed access control in clouds,” in *IEEE TrustCom*, 2011.

[14] S. Jahid, P. Mittal, and N. Borisov, “EASiER: Encryption-based access control in social networks with efficient revocation,” in *ACM ASIACCS*, 2011.

[15] R. L. Rivest, A. Shamir, and Y. Tauman, “How to leak a secret,” in *ASIACRYPT*, ser. Lecture Notes in Computer Science, vol. 2248. Springer, 2001, pp. 552–565.

[16] Boyen, “Mesh signatures,” in *EUROCRYPT*, ser. Lecture Notes in Com-puter Science, vol. 4515. Springer, 2007, pp. 210–227

[17] Karen Scarfone and Peter Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS)”, National Institute of Standards and Technology(NIST), Special Publication 800-94, Feb. 2007.

[18] Top Threats to Cloud Computing”, Cloud Security Alliance, http://www.cloudsecurityalliance.org/csaguide.pdf, V. 1.0 (2010) Foster, I.; Yong Zhao; Raicu, I.; Lu, S., "Cloud Computing and Grid Computing 360-Degree Compared", Grid Computing Environments Workshop, GCE '08, vol., no., pp.1-10, Nov. 2008

[19] J. Brodkin. “Gartner: Seven cloud-computing security risks”, http://www.networkworld.com/news/2008/070208-cloud.html.

[20] Jansen W., Karygiannis, T. 1999, “Mobile agents and security”. Special Publication 800-19, NIST.

[21] W Jansen, P Mell, T Karygiannis, Marks, "Applying Mobile Agents to Intrusion Detection and Response (1999)", National Institute of Standards and Technology Interim Report - 6416

[22] O. Choon and A. Samsudin, “Grid-based intrusion detection system,” in Proc. 9th Asia-Pacific Conference on Communications, vol. 3, pp. 1028-1032, September 21-24,2003.