ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 5, May 2013

Privacy Preserving and Intrusion Detection For Securing Data In Cloud

Manisha G. Vaidya
Computer Sciences And Engineering
G. H. Raisoni College Of Engineering
Nagpur, Maharashtra

Asst. Prof.A.V.Sakhare
Department of Computer Science &Engg.
G. H. Raisoni College Of Engineering
Nagpur, Maharashtra

Abstract— ***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. 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 but cloud does not know user's identity. User should need to authenticate before storing the data 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. this paper also introduce the Cloud Intrusion Detection Service (CIDS), which detect the different attack and fire the alert to other cloud user. CIDS used various component to summarize the alerts and inform about the attack fired information to the cloud administrator. CIDS architecture is scalable and elastic. CIDS approach detects the masquerade and host based attack and informs to cloud administrator to take proper action.***

Keywords: Access control, Authentication, Attribute-based signatures, Attribute-based encryption, Cloud storage. Cloud computing, security, intrusion detection, attacks, masque

I. INTRODUCTION

In cloud computing, users can outsource their computation and data through the Internet. Sensitive data should be encrypted before uploading to cloud servers and a secure user enforced data access control mechanism must be provided before cloud users have the liberty to outsource sensitive data to the cloud for storage. This issue can be resolve using a cryptographic-based data access control mechanism There are need to address challenge issues such as fine-grained access control with scalability, user dynamics, scalability and flexibility. Enable users to delegate most data decryption operations to cloud servers and reduce the computation load on users to a constant complexity and also greatly reduce the computation load on cloud servers. Cloud computing has three basic abstraction layers i.e. system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications).Cloud computing also has three service models namely Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models

Cloud Computing is a promising next-generation IT architecture which provides unlimited resources, such as storage as services to cloud users. cloud users and cloud service providers are almost certain to be from different trust domains and ensure that the sensitive data should be encrypted before uploading to cloud servers in cloud computing . Another main challenge in Cloud Computing is system efficiency. In Cloud Computing, Cloud users could access the system via various low-end devices such as mobile. Therefore, the proposed access control mechanism should be efficient enough in the sense that the computation load addressed on both the data owner and data consumers should be affordable to these low-end devices.

The main objectives of this project is to provide the facility to the data owner enforce fine-grained access control over data in large-scale data centers outsourced to Cloud Servers.The key challenge in cloud is a Fine-grained access control. In paper [1] fine-grained access control enable the data owner to enforce a unique access structure on each user Cloud computing is internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customer as a service on pay-as you-use basis. Securing the data or access data in cloud is issue but parallel there are need to detect the attack on cloud. So to detect the attack on cloud intrusion detection system is used.As paper [2] IDSs can detect intrusion patterns by critically inspecting the network packets, applying Rule and generating alarms for system administrators. Intrusion detection system plays an important role in the security and perseverance of active defense system against intruder. Intrusion Detection System (IDS) is known as strong defensive mechanism. IDSs are host-based, network-based and distributed IDSs. IDSs[3] produce alerts for the

Manuscript received April, 2013.

First Author name*, Computer science and Enggineering G.H. Raisoni College of Engg , nagpur , Maharashtra 8275396732*
Second Author name*, , Computer science and Enggineering, G.H. Raisoni College of Engg ,* Nagpur, Maharashtra

administrators which are based on true positives or true alarms when actually intrusion takes place and false positive or false alarms in case of a wrong detection by the system. Since services are outsourced to a remote server, security and privacy are of immense concern in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified.

II.RELATED WORK

Researches on data privacy in cloud computing are still in its early stages. Security and privacy is another concern for scientific cloud computing users. Data in cloud can be protected through giving valid access control to valid user.
Access control is the policy which guarantees that requests coming by authorized user are accepted and those coming by unauthorized user are rejected. Access control refers to security features that control who can access resources or data from cloud. Sahai and Waters [4] introducing the concept of Attributed-Based Encryption (ABE) to solve the data privacy problem. In an ABE system, a user's keys and cipher texts are labelled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. Sahai and Waters [19], [6] first introduced attribute based encryption (ABE) for encrypted access control. In an ABE system, both the user secret key and the cipher text are associated with a set of attributes. The ABE technique can be apply in two ways. In Key Policy ABE (KP-ABE) the secret keys are associated with an access structure; while the cipher text is labeled with a set of attributes [6] In[5] Cipher text-Policy ABE (CP-ABE the cipher text is associated with an access structure, while the secret keys are labeled with a set of attributes

Now in current generation most of people used a cloud for accessing and storing data so the most of known and unknown attack found on cloud. To detect the attack IDS system is used IDS usually monitor, collect and analyze logs, network traffic and user action in a process to identifying suspicious behaviour. IDSs may be classified according to the source of data into: (1) Host-based IDS (HIDS) (2) Network-based IDS (NIDS) (3) Distributed IDS (DIDS) which integrates both types of sensors The analysis of previous work confirms that, a proper defence strategy for cloud systems needs to Be distributed and scalable to adapt the cloud characteristics and also need to Protect the IDS by isolating it from vulnerabilities in the host machine. The defence strategy should Have a flexible architecture to be applied to several cloud architecture and to Integrate both behaviour and knowledge based techniques scheme propose the deployment of IDS on each layer of the Cloud to gather and correlate the alerts from different sensors.As paper[6]Virtualization as one of the key technologies for Cloud Computing because virtualization provide the better output for attack detection overview. the sequence alignment technique with a focus on the Semi-Global alignment technique (SGA) [7] used for integrating VM management and IDS management The most important advantages of this technique are its ability of exploiting distinct sequences of audit data and its low false positive and missing alarms rates [7] Scheme developed a log analyzer and correlator system to parse and analyze the host based log files and network packets. CIDD [8] has different audits from different environments; to increase its usability in different systems and thus simplify the support of distinct detection techniques in Communication between multiple virtual machines with the outside world must be monitored. The information which is available in VMM (Virtual Machine Monitor) level can be used by the IDS to detect intrusion correctly. This type of host-based intrusion detection is called VMM-Based IDS[6], where the IDS reside on physical host machine Organizer stored a data in cloud and accesses the data when they required. Data owners can send their important data to many other users at a time through the cloud. The individual users might want to only retrieve certain specific data files they are interested in during a given session.

Fuzzy keyword search [9]
The most common technique is to selectively retrieve files through keyword-based search.. K.Ren[1]Encrypted data files stored in the cloud server, a set of distinct keywords with predefined edit distance d. To decrypt file in cloud user send a keyword as searching input with edit distance and if the user's searching input exactly matches the pre-set keyword, then cloud server return the files that containing the searching keyword .. Chang et al. [10] and Curtmola et al. [11] both proposed index approaches, where only one index table is used i.e., single encrypted hash table index is created for the entire file collection. In this paper, the searching is performed through a keyword, which is containing in data file. Each entry consists of the trapdoor of a keyword and an encrypted set of file identifiers whose corresponding data files However; this approach has serious efficiency disadvantages. This approach required a large storage. In this approach, cloud give a decrypted data but cloud does not know the actual data stored in cloud.

Role Based Access Control [12]
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 or sensitive information is being stored in the cloud so cloud ensures access control of this sensitive information through providing a particular role to each user. Role includes the specification of duties this is an approach to restricting system access to authorized users. A role name is just one of many attributes. Main drawback of this approaches is that when more attribute are added the it will loss of RBAC's administrative simplicity.In UBAC, the access control list (ACL) contains the list of users who are authorized to access data and only listed user have privilege to decrypted the data from cloud. This approach is not suitable for many cloud servicers. This is not feasible in clouds where there are many users.

Attribute Based Access Control [13]

The ABAC 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. cloud assign a set of attribute to the user then if cloud user want to access the data from cloud then user need to provided a set of attribute to cloud and if attribute matches then only user can decrypted the data from cloud. Attribute revocation technique as paper[14] need a proxy server to revoke the key which are distributed to cloud user. This technique increase the storage and communication overhead and required huge computation

Distributed Access Control in Clouds [15]
Ruj, and Stojmenovic**[15]** Distributed Access Control in Clouds, a new access control mechanism, where owners decide on attributes that users should have to decrypt the data and users receive decryption keys which enable them to access records which they are authorized to access. The cloud stores only encrypted data. Owners encrypt their information using the public keys belonging to the attributes in the policy and stores this encrypted information in the cloud. The selection of KDCs(key distributed centre) depends on the application.This technique does not provided the authentication and also does not hide the access structure information.

EASiER Overview [16]
EASiER, proposed an architecture that enables users to set fine-grained access control policies even for dynamic groups. EASiER algorithm is capable to protect accidental or intentional information leak in online social network (OSN) through encryption unlike traditional OSNs, which generally support one type of relationship such as friend, EASiER users define relationships by assigning attributes and keys to each other. To protect information, users encrypt different pieces of data such as profile information, wall posts, etc.with attribute policies. Only the contacts with keys having enough attributes to satisfy a policy can decrypt the data.

Apply Mobile Agent based intrusion detection system [17**]**
In this paper a Mobile Agent based intrusion detection system (IDS) [17] which can be applied by Cloud clients, The advantages of the proposed approach for Cloud. Computing include achieving higher scalability, overcoming network latency, reducing network load and consequently lower operational cost. This approach follows a hierarchical structure[18] therefore, if any part of the internal nodes is disabled, the functioning of that of branch of IDS will be disqualified. Therefore, those architectures are not flexible, not completely distributed and are not able to respond to attacks **against intrusion detection system itself.**

Intrusions detection in computational grid [19]
Grid intrusion detection is a process that involves the gathering of information available at its networks and nodes based on the collection and correlation of the gathered data. GIDS architectures are designed to properly detect user behaviour anomalies, but this are unable to detecting host attacks, network attacks and grid-specific attacks GIDS uses the audit data shared by the lower-level IDSs to identify grid attacks and to compare the behaviour of grid users with their previously built historical profiles. when intrusion is detected by GIDS then the grid security manager send alert by the lower-level IDS. This solution is not complete, as it provides protection against host and network-specific intrusions but not against unauthorized access, misuse, grid attack grid-specific intrusions. The available GIDS architectures also lack protection against grid attacks and typical computer host and network attacks.

Intrusion Detection in the Cloud [20]
In this paper, which consists of several sensors and a central management unit Different types of sensors can be easily integrated into the extensible architecture. The IDMEF standard is used to represent and exchange the alarm information. A standardized interface is designed to provide a unified view of result reports for users. IDMEF standard to support the storage and exchange of alert information within the management system. The limitations of this system are signature pool that required constant updates to keep up with every malicious packet.

II. Conclusion

All the approaches take a centralized approach and allow only one key distribution centre (KDC). All existing approaches are not providing authentication and also not able to protect the user identity. Existing Ids system is not able to detect HIDS and masquerade attack in efficient way and all takes large time to detect the attack. So there is a need to overcome all these problems. For that it requires a system to help the data owner achieve fine-grained access control on files stored and allow a multiple write on cloud by Cloud Servers but also authenticates users who store information in the cloud. The cloud however does not know the identity of the user, who stores information, but only verify the user's attribute and access policy. And it must me necessary that the Key distribution is done in a decentralized way.

REFERENCES

[1] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS, 2010, pp. 735–737.
[2] Fang-Yie L., Jia-Chun L., Ming-Chang L., and Chao-Tung Y., "A Performance-Based Grid Intrusion Detection System," in Proc. 29th Annual IEEE International Computer Software and Applications Conference (COMPSAC), pp.525-530, July, 2005

[3] Jansen W., Karygiannis, T. 1999, "Mobile agents and security". Special Publication 800-19, NIST.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*. 2007, pp. 321– 334

[6] F. Azmandian, M. Moffie, M. Alshawabkeh, J.G. Dy, J.A. Aslam, D.R. Kaeli, "Virtual Machine Monitor-Based Lightweight Intrusion Detection", Operating Systems Review, Vol. 45(2), pp.38-53, 2011
[7]Scott E. Coull, Joel W. Branch, Boleslaw K. Szymanski, Eric A.Breimer. 2008. "Sequence alignment for masquerade detection". Journal of Computational Statistics & DataAnalysis. 52, 8(April2008), 41164131 http://dx.doi.org/10.1016/j.csda.2008.0122

[8] CIDD: A Cloud Intrusion Detection Dataset For Cloud Computing and Masquerade Attacks 2012

[9] 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

[10] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS'05, 2005.

[11] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS'06, 2006.

[12] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.

[13] 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

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

[15] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011

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

[17] 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

[18] Amir Vahid Dastjerdi, Kamalrulnizam Abu Bakar, Sayed Gholam Hassan Tabatabaei, "Distributed Instrusion Detection in Clouds Using Mobile Agents", Third International Conference on Advanced Engineering Computing and Application in Sciences, October 11-16, 2009 - Sliema, Malta

[19] Schulter, A.; Navarro, F.; Koch, F.; Westphall, C.B., "Intrusion Detection for Computational Grids", Proc. 2nd Int'l Conf. New Technologies, Mobility, and Security, IEEE Press, November, 2008, pp. 1–5.

[20] 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.

[21] Roschke, S., Cheng, F., Meinel, "Intrusion Detection in the Cloud", The 8th International Conference on Dependable, Autonomic and Secure Computing (DASC-09) China, Dec. 2009

First Author Manisha G.Vaidya B.E from Y.C.C.E in computer technology and M.tech persuing from Raisoni college (Autonomus Univecity) in CSE Nagpur ,Maharashtra

Second Author Asst. Prof.A.V.Sakhare Department of Computer Science &Engg.G. H. Raisoni College Of Engineering Nagpur, Maharashtra M.tech from Embedded system