IJCSN International Journal of Computer Science and Network, Volume 4, Issue 4, August 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Two-Level Security in Cloud using Cryptographic Techniques, RBA, Network Intrusion and Detection System

[1] Sharvari Pawar, [2] Suresh Rathod , [3] Mandar Mahadeokar

[1,2,3] Computer Department, Pune University
Pune, Maharashtra, India

Abstract - Security is one of the most concerned areas in the cloud computing. Achieving security in cloud environment is not a straight forward task as it requires different level approach. Security in Cloud Environment consists of data level and system level security. Data level security deals with the unauthorized access to the data over cloud while system level security deals with unauthorized intrusion into the cloud environment by an external entity. Data level security sees to it that the users of the cloud should be provided with the access to the data based on individual's role while System level security ensures that no external or third party user accesses the cloud system to pose threat to the functioning of the system. We have proposed the two level approaches by implementing two modules that take care of each level of security. The data level system is tackled with a module that performs encryption and decryption of the data as well as role based access approach. The system level security is achieved using a module that performs network intrusion detection and countermeasure selection for the cloud environment.

Keywords - *Cloud Computing, Cloud Security, Cryptographic Techniques, Role-Based Access.*

1. Introduction

Cloud computing is internet-based computing which allows large groups of remote servers sharing of data-processing tasks, centralized data storage, and online access to computer services or resources. Cloud computing is not a programming language it is just a way to use old services very effectively. In computer security we protect the data by using some encryption/decryption algorithm. Same approach also can be used to protect the data which travel across the cloud. Cloud services are the services made available to users on demand via Internet from cloud servers. Main motive to design cloud services are to provide easy and scalable access to applications, services and resources. There are 3 types of cloud services which are explained in detail below. First service is IaaS (Infrastructure as a service) [3]. Here, Infrastructure is provided as a service. Infrastructure may include resources such as hypervisor, such as Xen, Oracle Virtual Box, KVM, VMware ESX/ESXi, or Hyper-V runs the virtual machines as guests. Second is SaaS (Software as a Service) [4]. Here, provider allows multiple clients to access software which is centrally build in cloud by the cloud providers. It provides Software as a kind of service. Third is PaaS (Platform as a Service) [5]. Here provider provides platform to its legitimate users. Platform may include resources like operating system, programming-language execution environment, database, and web server.

There are 4 types of cloud namely, Public cloud, Private cloud, Hybrid cloud and Community cloud. Public cloud as the name suggests, it is publically open to all. Public cloud is maintained by cloud providers. It can be access via a thin browser. But here data security comes in threat, as it can be accessed by anyone. To overcome this fear, private cloud term came in picture. Private cloud is private to a single organization. It is maintained by the organization itself. Hybrid cloud is a combination of Public and Private cloud. This cloud takes the advantages of both public and private cloud. Community cloud is built when the organizations of same community come together and share a single cloud. All involved in this type of cloud trust each other. Hybrid and community cloud are maintained by third party. Cloud is spreading like fire in the world of technology but also carrying some concerns along. Few issues of cloud computing are Data security, Charging model, SLA, migration Costing model and Cloud Interoperability issues. In computer security, a Network Intrusion Detection System (NIDS) is a system

that tries to discover unauthorized access to a computer network by analysing traffic on the network for signs of malicious activity. A recent CSA (Cloud Survey Alliance) survey reports that among all Security issues, exploitation and despicable use of cloud computing is considered as the main security threat. In traditional data centers, where system administrators have full control over the host machine(s), vulnerabilities can be detected and controlled by the system administrator. However, controlling this is patching security holes in cloud data centers, where legitimate cloud users normally have the privilege to control software installed on their managed VMs, it may not work effectively and can violate the Service Level Agreement (SLA).

Furthermore, legitimate cloud users can install vulnerable software or untrusted software on their VMs, which is responsible for creating loopholes in cloud security. The important challenge is nothing but to establish an effective vulnerability/attack detection and response system which is used for accurately identifying attacks and minimize the impact of security breach to cloud users. In a cloud system where the infrastructure is shared by potentially millions of users that is in IaaS, abuse and nefarious use of the shared infrastructure benefits attackers to identify vulnerabilities of the cloud and use its resource to deploy attacks in more efficient ways. Such attacks are more effective in the cloud environment since cloud users usually share computing resources that are connected through the same switch, sharing with the same data storage and file systems. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, etc., attracts attackers to compromise multiple VMs.

In this paper, we propose a system having Two-Level of security. First is Data Level Security and second is System Level Security. Whenever an unauthorized individual tries to obtain highly confidential data here we are going to use Data Security module which consist of cryptographic techniques along with Role-Based Access. Because of this, unauthorized individual (attacker) will not be able to obtain data in plaintext form but what if attacker changes his mind, instead of obtaining data, what if he thinks of putting the system down by performing DOS, DDOS attack. In such situation our second module i.e. System Security module comes in picture. We must note that the design of System does not intend to improve any of the existing intrusion detection algorithms; indeed, it only provides software framework which is useful for attack detection, appropriate counter measure election and finally system also provides security policies which will help in securing the overall cloud environment.

2. Literature Survey

Depot [6] is a two level architecture that assures security of data stored in cloud. Architecture is fault tolerant and provides confidentiality. But it can't be used in our system as; it is unable to compute on encrypted data. For security of data, some cloud providers divide the data/database of the single user in several parts and store each part onto different clouds [7]. By this the cloud providers is unable to access the entire data as a whole. But loophole here is, if all the cloud providers get together they can get entire data of the user. So this technique can hamper security. In [8][9] architecture uses intermediate proxy server which contains the entire logic of encryption and decryption. The architecture can perform SQL operations on encrypted data. In [9] the data to be encrypted is divided into blocks and then encrypted and stored. When clients demand for certain data item, the proxy processes the entire data block, decrypts it and takes the wanted data item and discards the remaining. For this, modifications are required in the original SQL operation. This results in heavy overheads on DBMS server as well as the intermediate servers. Over reliance on trusted proxies hinders the outsourcing of this service. Alongside this, easy access of trusted proxies can't be assured. Thus have limitations. In Homomorphic encryption, operations are directly performed on encrypted data without decrypting it. Client who perform operations are unaware of the private key, Maha TEBBA et al [11] proposed an architecture which uses Homomorphic encryption, helps strengthens the data confidentiality as it improves the complexity of Homomorphic encryption. The review of research is provided in table 1.

Chun-Jen Chung [12] proposed a NICE framework which having advantage of attack detection and detection accuracy. But the disadvantage is that they do not provide any prevention mechanism. This architecture only finds out an attack and takes appropriate counter measure. H. Takabi [13] gives brief description of Cloud computing include on-demand self-service, broader network access, location independent resource pooling, rapid elasticity and measured service. This paper also focuses on disadvantages of cloud computing such as Authentication and Identity Management, Access control and Accounting, Privacy and Data protection, Secure Service Management. Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker paper [14] focuses on effective spam zombie detection system named SPOT which is useful for monitoring outgoing messages of network. SPOT is designed which is based on Statistical tool called as Sequential Probability Ratio Test, which has bounded false positive and false negative error rates. G. Gu, P.

Table 1: Review Table

Sr. No	*Title*	*Implementation Method*	*Description*
1	Distributed, Concurrent and Independent Access to Encrypted Cloud Databases.	Encryption applied on database and metadata.	Encrypting database at client side. Firing SQL queries onto cloud for database retrieval.
2	Achieving Secure Role-Based Access Control on Encrypted data in Cloud Storage.	RBAC	Hybrid Cloud architecture is used. Using role parameters the access policies are controlled.
3	Depot: Cloud Storage with minimal trust.	Depot	Provides data security, fault tolerance, preserve confidentiality. Doesn't support computation on the encrypted data.
4	Distributing data for Secure Database Services	Dividing the database and storing on multiple providers.	Database is divided and kept onto multiple cloud provides. Query fired is divided and fired.
5	NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems	NICE	System has advantage of attack detection and detection accuracy. But disadvantage is they do not provide any prevention mechanism.
6	Detecting spam zombies by monitoring outgoing messages	SPOT	Focuses on effective spam zombie detection system, which is useful for monitoring outgoing messages of network.

Porras, V.Yegneswaran, M. Fong, and W. Lee [15] give detail information about BotHunter. It is an application designed to track the two-way communication flows between internal assets and external entities, it is also helpful to monitor system for real-time detection of internet malware infections.

3. Proposed System

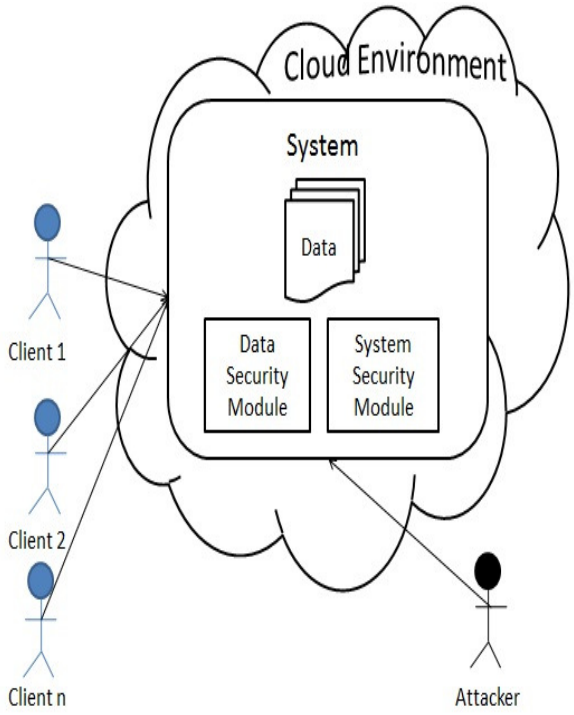

Fig. 1 Basic Architecture

3.1 Basic Architecture

The basic architecture is shown in Fig.1. It is a two level security architecture. First level deals with Data security and second with system security. In data security module, cryptographic techniques along with Role-based access is used so as to strengthen the data security and in system security module, if any attacker in the face of client tries to make the system down by sending flood of packets, this module will monitor the packets and block the IP address of the respective client and take action against it.

3.2 Data Security Module

This module is outlined to allow n number of authenticated clients to access the cloud database in simultaneous and independent manner [1]. Each client here has limited access to the Cloud database as per its

role (designation) [2] in that organization. Let us discuss the module in detail. Many organizations are moving to cloud for data/database storage. Let us consider such organization, here each tenant installs this module in every machine .Each client is allowed to access the organizations database stored onto cloud using this data security module. Each client can upload the data/database onto cloud and can download or update the database but depending upon its designation in that organization.

The system overview [10] is shown in Fig.2.

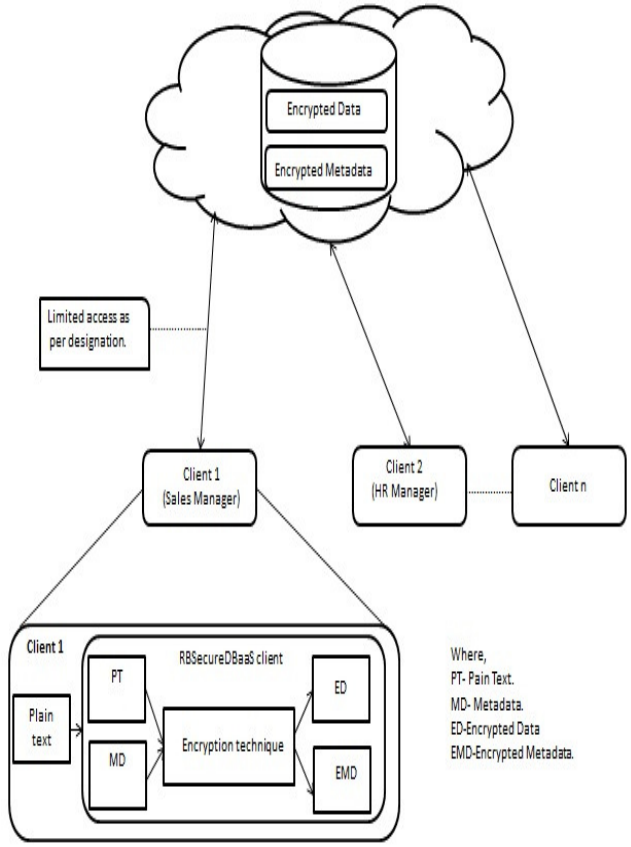

Fig. 2 Data Security Module.

Entities involved in the module are as follows:-

1. Plaintext data-This is the vital and confidential data of the organization that is to be kept secure in Cloud environment.
2. Metadata- It is a data of data of an organization's data which plays cardinal role while encrypting and decrypting data.
3. Encrypted data- The data security module converts the plaintext database into encrypted database. It contains the cryptographic techniques which are used for encryption or decryption of database. In this paper, we are using AES-128 algorithm for encrypting.
4. Encrypted Metadata- It encrypts the above discussed metadata and converts it into encrypted metadata and stores it onto Cloud database.

If a certain client wants to upload a database onto organizations cloud database, the RBSecureDBaaS client extracts the metadata from the database file. Then the file and the metadata is converted into encrypted form i.e encrypted metadata and encrypted database and then uploaded onto cloud. As the data/database is in encrypted form, nor the cloud provider neither the attacker can access the data/database. If a certain client wants to access a certain database, he sends a request to the cloud database. The client's role is checked and its permissions are checked. If that client has permission to access the file demanded, he is given access or else he is not given access of the demanded file.

3.3 System Security Module

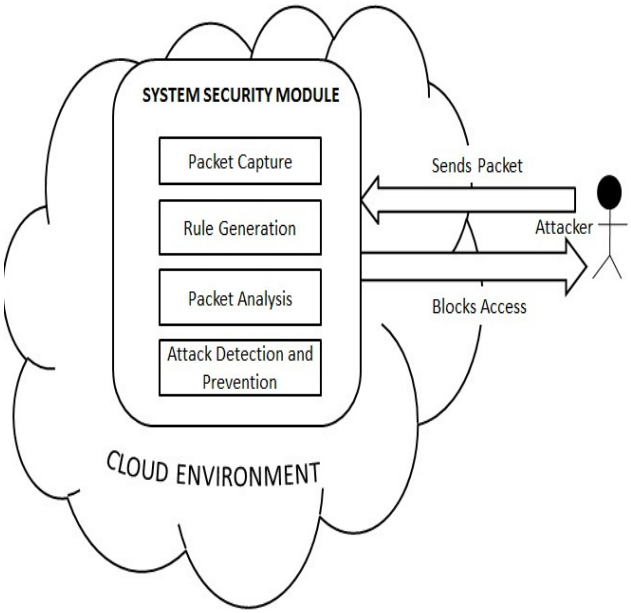

Fig. 3 System Security Module.

The final scenario is that attacker attacks on data which resides in cloud .But because of encryption and decryption algorithms he could not get that confidential data. Then Attacker tries to access the cloud illegally or try to down cloud services by performing DOS and DDOS attack. So this service is not available for legitimate cloud users. Here our Second Level of security comes into picture. This System Security Module is responsible for attack detection and prevention .So when attacker attack on

cloud, the Cloud service provider detects the attacker. After that the system finds out events those are carried out by an attacker. This module analysis and determines the severity of attacks. Depending on this Counter measure selection process is carried out. Finally by using the built-in policies or security mechanism which are pre-defined, the system blocks the attacker forever so that the attacker will never access the cloud services illegally. Countermeasure is nothing but simply blocking the IP address of the attacker and dealing with it so that attacker can't perform any malicious activity in future.

3.4 Merits and Demerits

Merits:

1. The proposed system provides higher security as compared to the existing systems. This is due to the 'two level security approach' that provides a stringent security to data as well as system.
2. Differentiating the problem of security in Cloud into two different levels allows the Cloud Providers to tackle each level security with specific techniques and more reliable methods.

Demerits:

1. Differentiating the problem of security in Cloud into two different levels makes the system more complex for the Cloud Developers as they need to consider each level with different assumptions.
2. Network based intrusion detection does not consider Host based approach which may leave a loophole for the attacker.

4. Conclusion

In this paper, we have proposed a two level architecture in which one level deals with data and second with system security. In data security level, two techniques are used so as to strengthen security, namely cryptographic algorithm and role-based access. In system security, if any attacker tries to down the system, the application traces the attacker and blocks its IP address.

Acknowledgments

We express sincere regards to all those who have contributed in successful accomplishment of this research work. I would like to take this opportunity to thanks all the staff members for their continuous support and assistance. Last but not the least thanks in advance to all the reviewers for their comments which will surely lead this research a successful and vital source of knowledge.

References

[1] Luca Ferretti, Michele Colajanni, and Mirco Marchetti "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", IEEE transactions on parallel and distributed systems, VOL. 25, No. 2, February 2014.

[2] Lan Zhou, Vijay Varadharajan, and Michael Hitchens , "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", IEEE transactions on information forensics and security, VOL. 8, No.12, December 2013.

[3] Amazon elastic compute cloud web services. http://aws.amazon.com/ec2.

[4] Netsuite saas portal. http://www.netsuite.com.

[5] Salesforceforce.com platform. http://developer.force.com.

[6] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot: Cloud Storage with Minimal Trust," ACM Trans. Computer Systems, vol. 29, no. 4, article 12, 2011.

[7] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R.Motwani, "Distributing Data for Secure Database Services," Proc.Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.

[8] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan,"CryptDB: Protecting Confidentiality with Encrypted Query Processing," Proc. 23rd ACM Symp. Operating Systems Principles,Oct. 2011.

[9] H. Hacigu¨mu¨ S, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model,"Proc. ACM SIGMOD Int'l Conf. Management Data, June 2002.

[10] Sharvari A. Pawar, Suresh B. Rathod "Accessing the Encrypted Cloud Data in a Simultaneous, Independent and role-based fashion," IJSR, VOL. 3, Issue 11, Nov 2014.

[11] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI "Homomorphic Encryption Applied to the Cloud Computing Security" Proceedings of the World Congress on Engineering, London, U.K., Vol 1, July 4 - 6, 2012.

[12] A. R Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee. "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems." IEEE Transaction on Dependable and Secure Computing VOL: 10 NO: 4 Year 2013

[13] H.Takabi, J.B.Joshi, and G.Ahn. "Security and privacy challenges in cloud computing environments." IEEE Security and Privacy, vol. 8, no. 6, pp. 2431, Dec. 2010. .

[14] Z.Duan, P.Chen, F.Sanchez, Y.Dong, M.Stephenson, and J.Barker. "Detecting spam zombies by monitoring outgoing messages." IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198210, Apr. 2012.

[15] G.Gu, P.Porras, V.Yegneswaran, M.Fong, W.Lee. "BotHunter: detecting malware infection through IDS-driven dialog correlation." Proc. of 16th USENIX Security Symp. (SS 07), pp. 12:112:16, Aug. 2007.

Sharvari A. Pawar received B.E degree in Information Technology from P.G.M.C.O.E, Pune, Maharashtra, India in 2012.M.E in Computer Engineering from S.A.O.E, Pune in 2015.

Suresh B.Rathod received the B.E. degree in Computer Engineering from T.COE, Tulajapur INDIA in 2007 and M.E. degree in Computer Engineering from S.C.O.E, Pune in 2012.He is currently working as an Assistant Professor in S.A.O.E, Pune.

Mandar M. Mahadeokar received the B.E. degree in Computer Engineering from A.I.S.S.M.S.COE, Pune, INDIA in 2013 and M.E. degree in Computer Engineering from S.A.O.E, Pune.