ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

Intrusion Tolerance: Enhancement of Safety in Cloud Computing

Geethu Thomas Janardhanan P S

ABSTRACT — **Cloud computing is a recent computing model; provides consistent access to wide area distributed resources facing many problems as its usage increases. Enormous loss to both cloud clients as well as cloud service providers happen even with small intrusions. The protection and defense of cloud infrastructure against malicious attacks can be solved by designing 'intrusion tolerance'. We prove the renewal and confidentiality property of sensitive data by utilizing secret sharing and adding a proxy server. Proxy server acts as an intermediate server between the client system and cloud servers; blocks the intruders by sending the dummy dataset and by analysing their behaviours in the networks.**

Keywords*—*cloud computing, IDS, DoS, intrusion tolerance, proxy server

I. INTRODUCTION

Cloud computing is a recent technological achievement that connects the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and corporate business clients to use applications without installation and access their personal files and corporate data at any computer with internet access. This technology enhances more efficient computing by centralizing storage, memory, processing and bandwidth which in turn allows saving of storage space and energy.

Cloud computing can offer a variety of services including hosted services over the internet. With the increasing demand and applications, even number of security issues are also associated with cloud computing. Cloud computing platform is vulnerable to intrusions in sensitive data of data center and in the system. Intrusion tolerance in cloud computing is system security approach to safeguard cloud infrastructure against malicious attacks from unauthorized servers and hackers.

II. RELATED WORK

With the promising achievements and increased popularity of cloud computing, concerns are being voiced about the security issues introduced through adoption of this new model. The efficiency and effectiveness of conventional protection mechanisms are being redesigned and rebuild as the characteristics of this novel deployment model can differ widely from those of traditional architectural platforms [7]. Identity Management (IDM) is a mechanism to prevent unauthorized entry; authenticate users and provide services to them based on credentials and characteristics which are previously registered. Such a system should be able to protect private and sensitive information related to users and processes. Every business and corporate enterprises will have its own identity management system for control, access, information collection and computing resources usage. Since the cloud computing offers various clients to share, save and access the data in the same platform across the cloud; the individual client data must be properly segregated and portable across various locations [9].

In cloud computing environments, the clients are dependent on cloud service providers for various services and maintenance. In many services, the clients have to store their confidential data on the cloud platform. A trust framework should be developed that allows efficient capturing of generic set parameters required for establishing trust and managing interaction/sharing requirements[10].

Recent attention is being paid on Intrusion Detection (ID) which is an integral part of computer network security and the system defense. According to the recent development trends and advancement of intrusion detection, detecting all kinds of intrusions across the platform effectively requires a holistic view of the monitored network. Intrusion detection system sets off warning alerts about detected intrusions hackers so that a system administrator or the system itself may take appropriate and timely actions to prevent the incoming attacks. In nutshell, IDS collects and analyzes network traffics, and makes response or alerts the network to the system administrator if there is an unauthorized traffic is taking place. Thus, the aim of the IDS is to alert or notify the system that some malicious activities have taken place and ensuring suitable preventive measures to eliminate it and preserving the integrity of the cloud platform [5].

III. ISSUES

In general, security issues have been categorised into broad categories including sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. Cloud security management solutions and issues can vary, from cryptography; particularly public key infrastructure (PKI), to use of multiple cloud providers, standardisation of APIs, and improving virtual machine support and legal support [7].

Majority of the threats in the existing system arises from Service Oriented Architecture (SOA) ie combination of SOA and cloud computing which may expose security threats, and make controlling access to information potentially difficult. Low level of understanding can also generate threats. The performance of intrusion tolerance technologies is poorly adapted to the new environment, unless the issues are well understood. The new features and capabilities of intrusion tolerances may have shorter time to market, but information systems of the future will become more and more vulnerable, and do a little against intruders and hackers. Another issue is with host based authentication which is intrusion tolerant via threshold cryptography; the cloud coordinator can execute the cloud request only when the hosts running inside the datacenter are legitimate. In this case preferences are given only the hosts, not the data [6]. Key management is currently the responsibility of the cloud clients. Key provisioning and storage is usually an off-cloud parameter. Management interface usually make the availability of credential recovery. Copies of Virtual Machine may also contain keys that are not well managed. One key-pair per machine doesn't scale to multiple account holders. Key storage and provisioning are almost impossible to do on-cloud with current technologies including public key cryptographic system where revocation is even more complicated.

DDoS: it is an attack where multiple compromised systems infected with a Trojans are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack with a high impact on the service provider than the clients. These hazardous infections seriously affect the company reputation, client trust and interest [5]. Standardization of the cloud platform allows the maintenance of security and evolution with competing market. Standards should allow clouds to interoperate and communicate with each other no matter which vendor provides cloud services. The Service Level Agreement (SLA) is the only legal agreement between the service provider and client. The only means the provider can gain trust of client is through the SLA.

IV. INTRUSION TOLERANCE

A. Motivation

One of the existing solution deals with the protection of data with cryptographic key. Cloud computing environment should be secure enough in maintaining cloud clients trust level, as small intrusion can cause a huge loss to both cloud users as well as cloud service executives. Introduce a new method of intrusion tolerance in cloud using threshold cryptography and proxy server can surely protect cloud platform.

B .Method of implementation

Provision of reliable and secure services in cloud computing environment is an important issue. The main security issue is to reduce the impact of denial-of-service (DoS) attack or distributed denial-of-service (DDoS) in the cloud platform. To counter these kinds of attacks, a framework of cooperative intrusion detection system (IDS) is proposed. Intrusion Tolerance have to be achieved with the help of cryptographic method and proxy server (Fig.1). Proxy servers can analyze the behaviors of the client request and also the behaviors of the intruders. If the intruders are found in the proxy servers their request will not be transferred to the main servers. The proxy server blocks the intruders, ie. the proxy server will analyze the user as well as the data. *CloudSim* tool kit is used to launch the cloud platform. It monitors the cloud process and stores the data periodically. The efficiency is being achieved by authenticating the proxy and the original data is being encrypted using data encryption standard. Proper authentication will only allow the real data to be viewable reducing the risk of intruders. It also ensures the security and the intrusion attacked is detected and separated during the process (Fig.2). These methods enable the process reliable and secure; fulfills the client expectation and serves them in better manner .

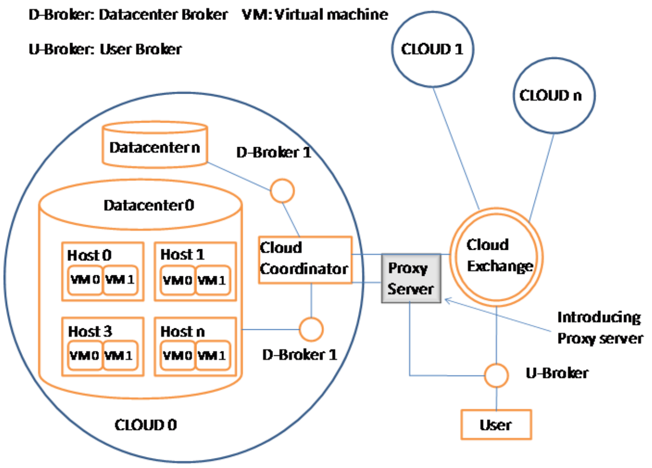

Fig.1 Cloud Computing Simulation environment

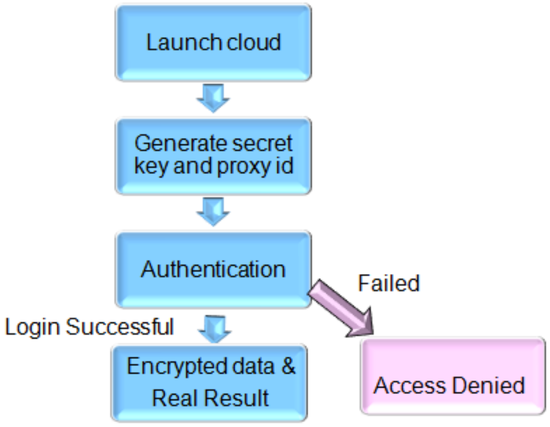

Fig.2 Designed dataflow diagram for intrusion tolerance

V. CONCLUSION

Cloud computing is clearly one of today's most enticing technology areas due, at least in part, to its cost-efficiency and flexibility. The clouds have different architecture based on the services they provide.. To provide secure and reliable services in cloud computing environment is an important issue. One of the security issues is how to reduce the impact of denial-of-service (DoS) attack or distributed denial-of-service (DDoS) in this environment. To counter these kinds of attacks, a framework of cooperative intrusion detection system (IDS) is proposed. The attacks may never be completely prevented, and some attacks may not be detected accurately and on time. For this instance *CloudSim* Tool kit is implemented. It monitors the cloud process and stores the data. The efficient thing is that, it can be authenticated by the proxy and the original data is encrypted. If the authenticated is success means the real data will be viewable. It ensures the security and the intrusion attacked is detected and separated during the process. As a result it fulfills the client expectation which enable the process reliable and secure.

ACKNOWLEDGMENT

I would like to express my gratitude to all those who helped me during the writing of this paper. I gratefully acknowledge the help of my guide, Professor Janardhanan P S, who has offered me valuable suggestions in the academic activities and technical support. Special thanks should go to my friends who have put considerable time and effort into their comments on the draft.

REFERENCES

[1] A. Shamir "How to share a secret", Comm. of the ACM, Vol.22, 1979, pp.612,613.

[2] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr: "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE Trans, Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33 (Jan. 2004)

[3] Ayda Saidane, Vincent Nicomette, and Yves Deswarte: "The Design of a Generic Intrusion-Tolerant Architecture for Web Servers", IEEE Trans. vol. 6 , pp. 45-58 (Jan-Mar 2009)

[4] Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros, " Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit Challenges and Opportunities.", University of Melbourne, Australia. (Jul.2009)

[5] Sebastian Roschke, Feng Cheng, Christoph Meinel: "Intrusion Detection in the Cloud", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[6] Popovic, Kresimir, Hocenski, Zeljko: "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of

the 33rd International Convention pp. 344 - 349 (May 2010)
[7] Zissis, Dimitrios; Lekkas (2010). "Addressing cloud computing security issues". Future Generation Computer Systems

[8] Vishal M. Karande and Alwyn R. Pais: "A Framework for Intrusion Tolerance in Cloud Computing", First International Conference on Advances in Computing and Communications (ACC 2011)

[9] Ngamsuriyaroj, S.Rattidham, P Rassameeroj, Wongbuchasin, P.Aramkul, N.Rungmano, " Performance Evaluation of Load Balanced Web Proxies",IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), 2011

[10] Amandeep Verma1, Sakshi Kaushal: "Cloud Computing Security Issues and Challenges: A Survey", First International Conference on Advances in Computing and Communications (ACC 2011)

[11] Wasim ari, Vinicius V. Cogo, Alysson Bessani Marcelo Pasin, Hans P.Reiser : " Fault Intrusion Tolerance for cloud computing",2012

[12] http://www.enisa.europa.eu/act/rm/_les/deliverables/cloud .../fullReport,2012

[13] "Intrusion Tolerance via Threshold Cryptography", http://crypto.stanford.edu/ dabo/ITTC/

[14] http://netbeans.org/about/ ,2012-06-09

[15]http://www.terena.org/activities/tf-csirt/.../hogbencloudcomputing.pdf ,2012

[16] O. Sami Saydjari "Intrusion-Tolerant Middleware" published by the IEEE computer society