Enhancement of Safety in Cloud Computing Based on Intrusion Tolerance

Shrikant A. Deshmukh
Student of Master of Engineering in (CSE)
G.H. Raisoni college of Engineering and Management
Amravati, India
shrik240@gmail.com

Prof. Vinit Kakade
Assistant professor Department of (CSE)
G.H. Raisoni college of Engineering and Management
Amravati, India
vinit.kakade@raisoni.net

Abstract- As we uses a computer and access our personal information and business information and also store the data on web servers. This arises the new security challenges with new computing and communication paradigms. Encryption have failed in preventing data theft attacksin existing data protection mechanisms. One of the emerging technologies in the present world is Cloud computing. Many of the individual users and organizations have profound usage of cloud computing as they can access data base resources through internet from anywhere. This computing model is beneficiary as far as the terms cost reduction and data accessibility are concerned. But there is a need to consider the security concept in cloud computing as the users store the sensitive data on the cloud storage providers which cannot trusted always. By designing 'intrusion tolerance', the protection against malicious attacks of cloud infrastructure can be solved. In this paper we provide method about security in cloud computing. This paper is mainly aims at the Enhancement of Safety based on Intrusion Tolerancein Cloud Computing.

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

*****

I. INTRODUCTION

Cloud computing is a technology which allows to connects the internet and central remote servers to maintain all data and related applications. The use of cloud computing has increased rapidly in many organizations. From small companies to medium companies use cloud computing services for their organization, because services by cloud computing provide fast access to their applications and reduce their infrastructure costs. Cloud providers should maintain privacy and security issues on high and urgent priority. By the Cloud computing user and business clients are able to use the applications by any computer over the internet without installation and accessing personal information and corporate data at any computer with internet access. By centralizing storage, memory, processing and bandwidth which in turn allows saving of storage space and energy, cloud computing enhances more efficient computing. Cloud computing can dealwith a diversity of services including hosted services over the internet. With the accumulative demand and applications, large number of security issues are also accompanying with cloud computing. Cloud computing is exposed to intrusions in sensitive data of web server 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 amplified attractiveness of cloud computing, concerns are being worried about the security issues acquaint with embracing of this new model. The efficiency and effectiveness of conventional protection mechanisms can differ widely from those of traditional architectural platforms [5]. Identity Management (IDM) is a mechanism to restrict the unauthorized entry; authenticate users and provide them various services based on credentials and characteristics are registered previously. To protect private and sensitive information related to users and processes, such a system should be used. Every business and corporate enterprises, for control, access, information collection and computing resources usage, will have its own identity management system. The individual client data must be properly segregated and portable across various locations, where clients are able to share, save and access the data in the same platform across the cloud. This is due to the cloud computing power [6]. In cloud computing environments, the services, application and maintenance required by the clients for their use is depends on the cloud computing service provider. The many of services and application from cloud server needs the client's confidential data on the cloud server. For this, a secured framework should be developed for establishing trust and managing interaction/sharing requirements that facilitate efficient parameters required [7].Intrusion Detection (ID) research area is being developed as an integral part of computer network security and the system defense. Detection of all kinds of intrusions across the platform effectively requires a holistic view of the monitored network. To prevent the incoming attacks system administrator or the system it may take appropriate and timely actions. In nutshell, if there is an unauthorized traffic taking place IDS collects and analyzes network traffics, and makes response or alerts the network to the system administrator. The Basic aim is to aware system about the attack that are going to be taken placed and ensuring suitable preventive measures to eliminate it and preserving the integrity of the cloud platform [3].

III. SECURITY RISKS IN CLOUD COMPUTING

Cloud service providers have offered benefits tousers, security is the main component in the cloud computing environment. Online data sharing or network facilities of the user are aware of the various loss of privacy [9]. The top challenge for74% of CIOs in relation to cloud computing is security. Protecting private and important information from various attackers such as creditcard details or patients' medical records is of critical importance. The Shifting of databases to a big data center may include many security issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. Subashini and Kavitha proposed basic security challenges, that are data storage security and management, application security, data transmission , and protection that are related to third-party resources. The security responsibilities are kept separated between users and providers in various cloud services models.

According to Amazon, EC2 addresses security controlling relation to physical, environmental, and virtualization security, in which the users remain accountable for addressing security control of the IT system that incorporate the operating systems, applications and data.

Cloud Security is a part of the internet and any upcoming issues on internet will also disturb the services of the cloud. Through the Internet cloud services resources are accessed for efficient use. Accordingly the cloud providers always focus on security in the cloud infrastructure, the data that are sent to the users with the help of networks may be insecure. So internet security problems will hamper the working of the cloud, with greater risks due to important resources that are stored within the cloud. The technology used in the cloud is similar to the technology used in the Internet. Various Encryption techniques and secure protocols will be not enough to protect data transmission in the cloud. Data intrusion of the cloud needs to be addressed and the cloud environment needs to be secure from hackers and cybercriminals and more security should be provided to clients.

A. Data Intrusion

According to Garfinkel[10], Hacked password or data intrusion is the security risk that are arising with the cloud provider. If Amazon account password is hacked, the account's instances and resources will be easily accessible .and it will result in erasing all the information inside any virtual machine instance can easily change services and information. There is a possibility for the user's email (Amazon user name) to be and since Amazon allows a lost password to be reset by email, the hacker may still beable to log in to the account after receiving the new reset password.

As cloud computing provides service that can provide a large amount of information and the computing services to each individual or an organization. The cloud computing systems as service providers provide many services to so many customers or organizations that are not trustworthy because there might chances of occurrence of threats by various cyber-attacks. So there is a need of Intrusion Detection Systems (IDSs) for the protection of virtual machines against threats and that system provides a stronger security service by using many of the rules.

B. INTRUSION DETECTIONSYSTEMS

This is an important component which can be implemented for protecting computer systems and network against security attacks. The main aim of IDS is to detect the attacks and provide the proper response and it is a technique that detects and responds to intrusion activities from malicious host. There are two types of IDSs, They are Host level and another is Network level.

Host based intrusion detection system involves software or agent components, which is run on the server, router, switch or network appliance in detecting and responding to long term attacks such as data thieving. Network based intrusion detection systems captures network traffic packets such as TCP, UDP and IPX/SPX and analyzes the content against a set of rules, signatures to determine if a possible event took place.

Majority of the threats in the existing system arises from Service Oriented Architecture (SOA) is 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 [4].

IV. INTRUSION TOLERANCE

A. Motivation

One of the existing solution cryptographic key provides a protection to data. Cloud computing environment should be efficient in maintaining cloud clients trust level, as small intrusion can cause a big loss to both cloud services as well as users. Intrusion tolerance a new approach in cloud using threshold cryptography and proxy server can surely protect cloud platform.

B .Method of implementation

In cloud computing environment reliable and secure services is an important issue. To reduce the impact of denial-of-service (DoS) attack or distributed denial-of-service (DDoS) in the cloud platform is an important issue in cloud. To overcome these kinds of attacks, an efficient framework of cooperative intrusion detection system (IDS) is proposed. Intrusion Tolerance has is achieved by cryptographic approach and proxy server (Fig.1). Behaviors of the client request and also the behaviors of the intruders are analyzed by the Proxy Servers. 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.

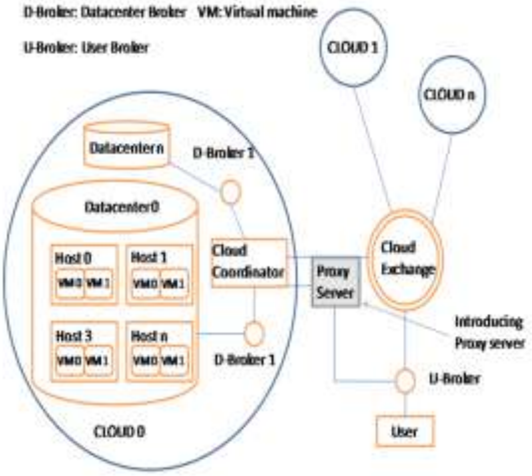

Figure 1 : Cloud Computing simulation environment

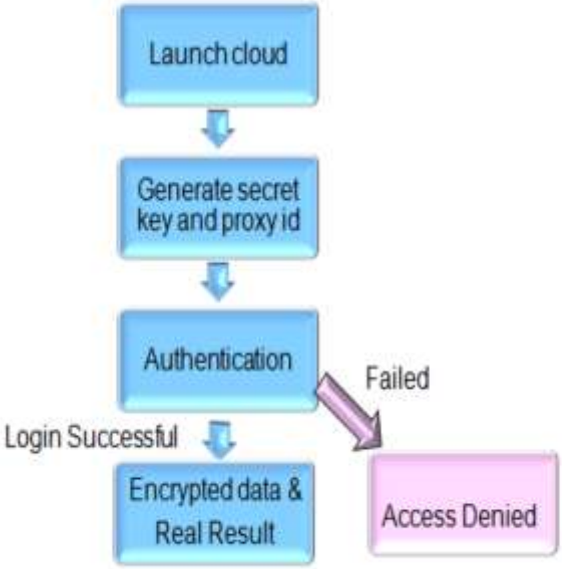

Figure 2: Designed Data Flow Diagram of Intrusion Detection System

V. Conclusion

Cost-efficiency and flexibility have made the Cloud computing the emerging technology areas. It has variable architecture that is based on the services. Cloud computing environment provide the secure and reliable services that is consider as an important issue today. The one drawbacks in security issues is to reduce the impact of denial-of-service (DoS) attack and as well as the distributed denial-of-service (DDoS) in this environment. To solve this problem a framework of cooperative intrusion detection system (IDS) is proposed. The attack is not completely prevented, and many of these attacks may not be detected accurately in specific duration of time. To solve this problem CloudSimTool kit is used. The work of the CloudSim is to monitor the various cloud process efficiently and also to stores the information accurately. The best thing is that the original data is encrypted and detected by this system. The authentication steps make it more efficient and by this the user can see view data. Security is guaranteed and the detection of intrusion attack during the process. The client expectation is fulfilled that enable the process more reliable and more secure.

As the usage of cloud computing has been increasing rapidly there is need of considering the security concepts in cloud computing service providers as many of the users or customers or the organization's store sensitive data on cloud. If the cloud service provider works only with a single provider then there are many security challenges has to be encountered and the customer has be worried more if there occurs some attacks on the data they have stored on the cloud. Data integrity, data corruption, or the unavailability of the data from the cloud service provider could arise many problems for the customers. The main aim of this paper is to ensure a work of the recent research on single cloud storage and multi cloud storage and has to overcome the security issues that are raised during the usage of single cloud storage. It could be more beneficial if the cloud computing has migrated from single cloud to multi clouds in which the DEPSKY system can overcome the limitations of the individual clouds.

REFERENCES

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

[2] Ravi Jhawar, Vincenzo Piuri and Marco Santambrogio, “Fault Tolerance Management in Cloud Computing: A System-Level Perspective”, in IEEE Transaction, ISSN: 1932-8184,doi: 10.1109/JSYST.2012.2221934,2012.

[3] Sebastian Roschke, Feng Cheng, ChristophMeinel:"Intrusion Detection in the Cloud", 2009 Eighth IEEE International Conference on Dependable, Autonomic andSecure Computing.

[4] Popovic, Kresimir, Hocenski, Zeljko: "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings ofthe 33rd International Convention pp. 344 - 349 (May 2010)

[5] Zissis, Dimitrios; Lekkas (2010). "Addressing cloudcomputing security issues". Future Generation Computer Systems

[6] 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

[7] Amandeep Verma1, SakshiKaushal: "Cloud ComputingSecurity Issues and Challenges: A Survey", First InternationalConference on Advances in Computing and Communications(ACC 2011)

[8] Intrusion Detection System for Cloud Computing Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande , International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012

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

[10] Hans P. Reiser, “Byzantine Fault Tolerance for the Cloud”, in University of Lisbon Faculty of Science, Portugal, at http://cloudfit.di.fc.ul.pt

[11] Shivam Nagpal and Parveen Kumar , “A Study on Adaptive Fault Tolerance in Real Time Cloud Computing”, in International Journal of Advanced Research in Computer Science and Software Engineering (IJarcsse), ISSN: 2277 128X, Volume 3, Issue 3, March 2013.