IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
ISSN : 2348 - 6090
www.IJCAT.org

Two Ways Security on Cloud Computing using Cryptography and Intrusion Detection: A Review

[1]Tony Durgadas Jagyasi, [2]Jagdish Pimple

[1] Dept. of Computer Science and Engineering,Nagpur Institute of Technology
Nagpur, India

[2]Dept. of Computer Science and Engineering, Nagpur Institute of Technology
Nagpur, India

Abstract - Cloud Computing gives various benefits to the customers, for instance, agreeability and approachability. As the data is receptive over the cloud, it could be entered by dissimilar customers. There may be delicate data of various organizations stores over the cloud. This is the one issue to offer access to authorized customers only. However the data could be available to the owner of the cloud. So to avoid getting into the data, the user is being redirected to the different security layers where the authentication of the user is done by the cloud security servers.

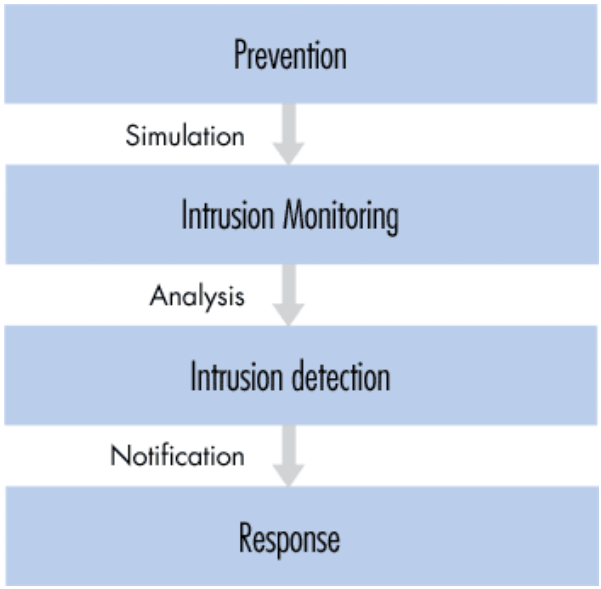
***Keywords* - Cloud Computing, Cloud Security, Triple DES, Encryption Algorithm. Intrusion Detection, Unusual Activity of the user, IDS, IDPS**.

1. Introduction

The utilization of cloud computing is expanding vastly. Cloud computing gives numerous profits to the clients, for example, openness and accessibility. As the information is accessible over the cloud which is gained entrance to by number of diverse clients, so there are some security issues related to the information over the cloud. There may be delicate information of association which is archived over the cloud which might be gained entrance to by any client. The issue is to give validation of the client to gain access to the information if the cloud where the information is saved. So the same information has to be stored in different clouds as the backup of the main cloud.

An intrusion detection system (IDS) is a tool or computer application that detects network or program behavior for hazardous activities or policy violations as well as generates reports to a managing condition. Several devices will probably make an effort to prevent an intrusion attempt but yet this is neither necessary nor predicted of a tracking program. Intrusion detection and prevention system (IDPS) are mainly dedicated to diagnosing likely situations, logging details about these, and tracking effort. As well as, companies make use of IDPS for additional purposes, like determining issues with security policies, documenting threats as well as removing persons from violating privacy policies. IDPS have grown to be an essential security infrastructure of almost every internet business.

The working of the Intrusion Detection and Prevention can be seen in the figure below. IDPS normally gives information in regard to noticed events, informs security professionals of important identified occasions and also give reports. A lot of IDPS also have the option to give response to an identified warning by trying to stop it from being successful. They use various reaction strategies, which include the IDPS stopping the attack by itself, altering the security measure.



2. Literature Survey

Cloud computing is used as a tool to discover solution as well as type of software. This solution dynamically comes with requirements, configures, reconfigures, in addition to servers as required by the cloud. Servers in the cloud could in fact be actual devices or maybe virtual equipment. Modern clouds commonly include additional computing options like storage area networks (SANs), network equipment, firewall or other security measure.

Cloud computing furthermore explains programs which can be expanded to be available using the internet. A lot of these cloud programs make use of huge data facilities and even highly effective servers that host Web programs or Internet programs. Any individual with an appropriate On-line connection in addition to a regular navigator will gain access to cloud software. Reliability in cloud is truly one of the primary aspects of research.

An Intrusion Detection System (IDS) is a system monitoring solutions actually designed for detecting vulnerability exploits against a specific software or computer as can be seen in the figure below. Intrusion Prevention Methods (IPS) developed IDS techniques by increasing the capability to prevent threats together with detecting all of them and became the main deployment solution for IDS/IPS technologies.

Figure 1Accessing Cloud Securely

An IDS requires to only discover threats and also as such is placed out-of-band on the network infrastructure, and therefore it is not necessarily in the real-time interaction path between the sender and receiver of information

IDS was firstly formulated this way simply because during the time the range of analysis necessary for intrusion detection could hardly be achieved at a speed which could keep pace with elements on the direct communications path of the network infrastructure .

As described, the IDS are also a listen-only device. The IDS detects web traffic and reviews the results to an administrator, yet find it difficult to automatically do something to stop a detected exploit from taking over the program. Attackers are equipped for exploiting vulnerabilities quickly after they get into the system, making the IDS an insufficient deployment for preventing device.

3. Problem Statement

As the use of cloud networks has increased, the security has also become more important accordingly. Historical events show that prevention alone, i.e., cryptography and authentication are not enough; therefore, the intrusion detection systems are brought into consideration. Since most of the current techniques were originally designed for wired networks, many researchers are engaged in improving old techniques or finding and developing new techniques that are suitable. With the nature of cloud networks, almost all of the intrusion detection systems (IDSs) are structured to be distributed. The number of new attacks is likely to increase quickly and those attacks should be detected before they can do any harm to the systems or data.

A network behavior analysis (NBA) system examines network traffic or statistics on network traffic to identify unusual traffic flows. NBA solutions usually have sensors and consoles, with some products also offering management servers. Some sensors are similar to network-based IDPS sensors in that they sniff packets to monitor network activity on one or a few network segments.

4. Methodology

The user will get the verification code while the user registers itself over the cloud. The user needs to remember the code all the time when it needs to gain access of the cloud storage where the user file are available to authenticate the validation of the user. The user will have to pass different security logics which are made available for the purpose of security of the data available over the cloud. If the user will try to get inside the cloud storage of the other user, it will need to pass different security

measures or the security codes of that user and if the unauthenticated user tries it for number of times, then serious action will be taken against that. The different layers of the intrusion detection can be as shown in the figure below.

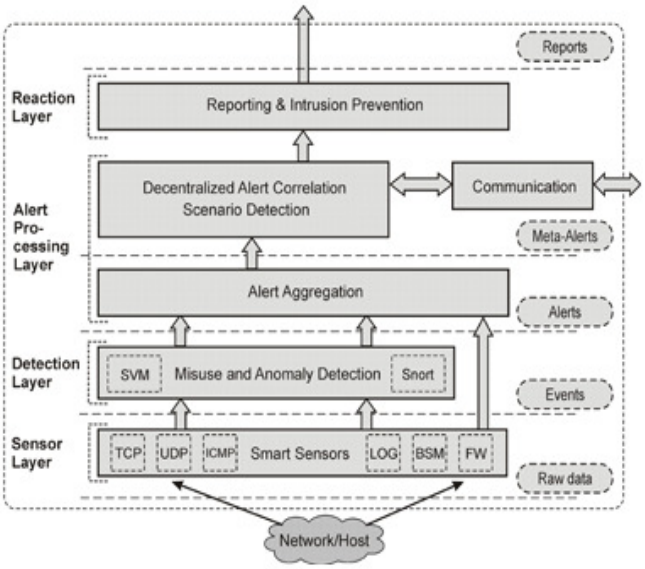


Fig 2 Intrusion Detection and Prevention at different Network Layers

5. Proposed Approach

When the user tries to login into the main portal where all the files and folders are available, the verification of the user is done, with different layers of the intrusion detection techniques. At the time of registration the user is given the verification code and the account is verified so that the main portal will be activated. After the activation of the main portal, the space is created to be utilized by the user. All the time the user enters the its cloud space, the user needs to remember the verification code to get inside its space.

6. Tools for Development and Verification of Result

- Hardware requirement: Personnel Computer, Pentium processor PIII and above, Ram 512 and above, Internet connection.
- Software requirement: VB.net, ASP.net.
- Operating system: Windows Azure
- Database Connectivity: SQL Azure
- Cloud connectivity

References

[1] http://en.wikipedia.org/wiki/Intrusion_detection_system

[2] Volume 3, Issue 4, April 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Intrusion Detection and Prevention in Wireless Adhoc Networks.

[3] International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011 ISSN 2229-5518 IJSER © 2010 Importance of Intrusion Detection System (IDS).

[4] ISCA Journal of Engineering Sciences Engineering Sci.Vol. 1(1), 51-56, July (2012) Intrusion Detection and Prevention System (IDPS) Technology- Network Behavior Analysis System (NBAS).

[5] International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009 INTELLIGENT INTRUSION DETECTION SYSTEM FRAMEWORK USING MOBILE AGENTS.

[6] Securing Cloud Computing Environment by means of Intrusion Detection and Prevention System (IDPS) International Journal of Computer Science and Management Research Vol 2 Issue 5 May 2013.

[7] http://www.microsoft.com/azure.

[8] http://www.google.com/apps/business.

[9] Amazon web services. http://aws.amazon.com.

First Author Tony Durgadas Jagyasi is a student of Master of Technology, Computer Science and Engineering in Nagpur Institute of Technology affiliated to RTM Nagpur University, Nagpur, Maharashtra, India. He is awarded B.E. in Computer Engineering from Mumbai University. He has experience in Computer Science and Engineering areas pertaining to academics and industry related real time projects. His area of research include Cloud computing, Network Security, Data Mining, Web Technologies and Emerging Technologies.

Second Author detail Prof. Jagdish Pimple: He is working as an Assistant Professor in Computer Science & Engineering Department, in Nagpur Institute of Technology, Affiliated to RTM Nagpur University & Approved by AICTE New Delhi. He is having more than 7 years of experience in academic and industry. His various research papers have been published in various international, national Journal and various international conferences. He has good grip in design, development and implementation of IT, Software tools. He has a good hand on various Programming languages. His main research interests include Android, Cryptography, Social Computing, wireless sensor network.