ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 2, Ver. 2 (April - June 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Secure the Cloud Computing Environment from Attackers using Intrusion Detection System

[I]T.V.S.Jeganathan, [II]T.Arun Prakasam
[I,II]Assistant Professor, Dept. of Computer Science, Siri PSG Arts & Science College for Women, Salem, Tamilnadu, India.

Abstract
Cloud computing is a method of novel internet infrastructure and demand industrial feature that IT offers today. It provides a framework for end users easily attaching powerful services and many enterprise applications through Cloud platforms. The wide utilize of cloud computing, security issues came out on a growing scale. It is most important to solve many security issues to support the wider applications of cloud computing. So, a Cloud computing system requires some Intrusion Detection Systems (IDSs) for protecting each machine against threats. The IDS provide security services using many convention or patterns, another issue in Cloud Computing is difficult to analyze large amount of logs by system administrators. Most IDSs are facing specific types of attacks through appropriate technique can guarantee protection against future attacks. It can provide robust protection, highly flexible, portable and fully controlled against an entire field of threats. In this paper, it is aimed to define different attack types, which will affect integrity of resources and services in cloud computing environment. Additionally, the paper also introduces intrusion detection models to recognize and prevent many attacks.

Keywords
Cloud Computing, Intrusion Detection System, Attacks, Services and Security

I. Introduction

Cloud computing organizations have to give an elevated excellence service and protect the users' sensitive data. To prevent these attackers, many production techniques are used such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Passwords, SSL and Data Encryption, Standard Scanning Programs, Code Implementation and so on. The Intrusion Detection System (IDS) are effective solutions to resist them. The monitoring of cloud resources are from different locations. Sometimes, it will be different countries. So that, intrusion detection installation (sensors placement, collecting intrusion data, analyzing by detection engines) are not easy [1]. In Cloud computing, where massive amount of data is generated due to high network access rate, IDS must be robust against noise data & false positives. Since Cloud infrastructure has enormous network traffic the traditional IDSs are not efficient enough to handle such a large data flow [2].

In a usual network, IDS monitors, detects and alert the administrative user for network traffic by deploying IDS on key network block points on user site. But in Cloud network IDS has to be placed at Cloud server site and entirely administered and managed by the service provider. In this scenario, if an attacker manages to penetrate and damage or steal user's data, the cloud user will not be notified directly. The intrusion data would only be communicated through the service provider and user has to rely on him. The cloud service provider may not like to inform the user about the loss and can hide the information for the sake of his image and repute. In such a case, a neutral third party monitoring service can ensure adequate monitoring and alerting for cloud user. In this paper, we have proposed an efficient cloud IDS, administered and monitored by a third party ID monitoring service, who can provide alert reports to cloud user and expert advice for cloud service provider[3].

The remaining part of the paper is organized as follows. The section II discusses the service models of Cloud computing. Section III deals with the installation types of clouds. In section IV, we carried out different way of attacks in clouds. In section V describe about Intrusion detection System types. The Section VI, trace out the techniques of IDS. In the next section, the proposed model is described to show in diagrammatic. Finally, we give conclusion in sections VII.

II. Service Models Of Cloud Computing

Cloud Computing served over internet systems based on Anything as a Service (XaaS). This services are like; Communication as a Service (CaaS), Network as a Service (NaaS) or Monitoring as a Service (MaaS). However, the three main cloud service delivery models are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [4]. These three cloud service models are shown in Figure 1 and detailed as follows.

A. Infrastructure as a Service (IaaS)

The IaaS provides the organizations with hardware resources that can be used for anything. The advantage is that instead of buying servers, software, and having to pay for the datacenter space for them, the service provider rents those resources. And by renting resources we mean any resources than a person can think of, including Server Space, Network Equipment, Memory, CPU Cycles, Storage Space, etc The cloud has provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host. Amazon's Elastic Compute Cloud (EC2) is a good example of IaaS. At the cloud infrastructure level, Service Provider can enforce network security with intrusion-detection systems (IDS), firewalls, antivirus programs, distributed denial-of-service (DDoS), and so on.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Fig.1: Cloud Service Models

B. Platform as a Service (PaaS)

PaaS supplies all the resources required to build applications and services completely from the Internet, without having to download or install any kind of software. The services provided in PaaS model include application design, development, testing, deployment, hosting, team collaboration, web service &database integration, and versioning. Such platforms let users deploy user-built software applications onto the cloud infrastructure using provider-supported programming languages and software tools (such as Java,.NET and etc). Virtual machines must be protected against malicious attacks such as cloud malware. Therefore maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental. Google App Engine, Microsoft Windows Azure, ADP Payroll processing, and US Postal Service offerings is an example of PaaS.

C. Software as a Service

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over the Internet. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. It SaaS is most often implemented to provide business software functionality to enterprise customers. It associated with complexity of installation, management, support, licensing, and high initial cost. Web Services security, Extendable Markup Language encryption, Secure Socket Layer and available options which are used in enforcing data protection transmitted over the Internet. Highest-profile examples are Salesforce.com, Google's Gmail and Apps, instant messaging from AOL, Yahoo and Google, and VoIP from Vonage and Skype [5].

III. Cloud Installation Types

A. Private cloud

Vendors are Install the cloud computing on private networks. Enterprises are implementing a private cloud within areas of their infrastructure in which a cloud model makes the most sense. Enterprise Level organizations are implementing a private cloud within areas of their infrastructure in which a cloud model makes the most sense.

B. Public cloud

Public cloud applications, storage and other resources are made available to the general public by service providers. End users without actually possessing these resources can gain access to them easily on demand via a Web browser from a simple laptop or terminal, wherever they are needed and with minimal management or service provider effort. Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them.

C. Hybrid cloud

This infrastructure is a combination of the Public and Private Cloud, often adopted by organizations that require greater control over come of the data they hold, yet still wish to run certain workloads on public cloud infrastructure as required. For example, a company may employ an internal cloud to share physical and virtual resources over a network, but extend these capabilities when needed such as at peak processing times. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet [6].

IV. Way Of Attacks In Cloud

A. Flooding Attack

These kinds of attacks are mostly realized over unauthorized network connections. Because of cloud computing paradigms' nature, connections to the virtual machines are established over Internet. When an adversary has achieved the authorization to make a request to the cloud, then he/she can easily create fake data and pose these requests to the cloud server. When processing these requests, the server first checks the authenticity of the requested jobs. Because non-legitimate requests must be checked to determine their authenticity, checking consumes CPU utilization, memory and engages the IaaS to a great extent. While processing these requests, legitimate services can starve, and as a result the server will offload its services to another server. Again, the same thing will occur and the adversary is successful in engaging the whole cloud system just by interrupting the usual processing of one server, in essence flooding the system[7].

B. Insider Attack

Insider attacks done by Employee, entrepreneur and associates. This are individuals to harm or temper knowledge about consumers or providers and include every kind of attacks which can be executed from inside.

C. User to Root Attacks

In this type of attack, an intruder seizes the account and password information of an authorized user, and he can acquire limitless access to the whole system. An attacker who owned the account and password information of an authorized user can hold the access privilege to servers and also to virtual machines.

D. Wrapping Attack Problem

In web server, messages are contains the structural information

that will be exchanged between the browser and server during the message passing. Before message passing occurs, the XML document needs to be signed and appended with the document. the body of the message is duplicated and sent to the server as a legitimate user. The server checks the authentication by the Sign Value (which is also duplicated) and integrity checking for the message is done. As a result, the adversary is able to intrude in the cloud and can run malicious code to interrupt the usual functioning of the cloud servers [8].

E. Port Scanning

An attack that identifies open, closed and filtered ports on a system .In port scanning, attacker can seize information with the help of open ports like services that run on a system, IP and MAC addresses which belong to a connection, and router, gateway and firewall rules. TCP, UDP, SYN/FIN/ACK and Window scanning are the most common scanning attacks. Port scanning is not used by its own, an intruder realize the actual attack after getting information about open ports and running services.

F. Attacks on Virtualization

After compromising hypervisor, control of the virtual machines in the virtual environment will be captured. Zero day attacks are one of the methods that attack virtual machines and use hypervisor or other virtual machines to attack other virtual machines. Zero day attacks use known vulnerabilities before system or software developers apply patches or updates..

G. Backdoor Channel Attacks

A passive attack type in which intruders compromise a node in the cloud and use this compromised node as a zombie resource to execute a attack. After compromising system become a zombie and also data can be reachable on the system [8].

H. Storage allocation and multi tenancy:

There are some issues to be defined about the data that are processed on cloud. Owner and control of the data, maintaining audit records, how and how much of the audit records will be shared with the consumer. To ensure consumers' data privacy, provider has to realize isolation of data and guarantee in service level agreement.

I. Data Modification, Forgery and Integrity

Untrusted providers and system administrators can manipulate users' and consumers' data among to their own benefits. Cloud users will be fall into a particularly bad position after such a manipulation or forgery occurs. With a combination of techniques like encryption and hash, this kind of integrity attacks can be prevented [9].

J. Network and host based attacks on remote Server

Host and network intrusion attacks on remote hypervisors are a major security concern, as cloud vendors use virtual machine technology. DOS and DDOS attacks are launched to deny service availability to end users.

Cloud security auditing Cloud auditing is a difficult task to check compliance of all the security policies by the vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is another concern of cloud security

Lack of data interoperability standards It results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be able to do so, as cloud user.s data and application may not be compatible with other vendor.s data storage format or platform. Security and confidentiality of data would be in the hands of cloud service provider and cloud user would be dependent on a single service provider.

K. Non-availability of cloud services

Non-availability of services due to Cloud outages can cause monetary loss to cloud user organization. A deliberate and comprehensive Service Level Agreement (SLA) must be written among user and provider covering all the relevant legal and service provisioning issues and details.

Flash Crowds: Sudden increase in the number of (legitimate) clients. Cloud computing systems are used by many people, therefore, they generates huge amount of logs. Huge amount of log makes IDS hard to analyze them and also time consuming. This in turn reduces system effectiveness. Intrusions in cloud distributed systems are potentially greater in speed, consequences, and damages.

L. Malware-Injection Attack Problem

In a malware injection attack, an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping. Here the attacker takes his first step by implementing his malicious service in such a way that it will run in Iaas or SaaS of the cloud servers. This type of attack is also known as a meta-data spoofing attack .When an instance of a legitimate user is ready to run in the cloud server, and then the respective service accepts the instance for computation in the cloud. The only checking done is to determine if the instance matches a legitimate existing service. However, the integrity of the instance is not checked. By penetrating the instance and duplicating it as if it is a valid service, the malware activity succeeds in the cloud[10].

M. Accountability Check Problem:

The payment method in a cloud System is "pay per use". When a customer launches an instance, the duration of the instance, the amount of data transfer in the network and the number of CPU cycles per user are all recorded. Based on this recorded information, the customer is charged. So, when an attacker has engaged the cloud with a malicious service or runs malicious code, which consumes a lot of computational power and storage from the cloud server, then the legitimate account holder is charged for this kind of computation. As a result, a dispute arises and business reputations are hampered. The focus for charging is based on the recorded parameters.

V. Intrusion Detection System

Intrusion detection systems (IDS) are an important role in the cloud computing environment for defensive measures protecting the systems and network against harm abuse [11,12]. Intrusion Detection System is software that automates the process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. The

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

basic types of IDS are Host based and Network based Intrusion Detecting System.

1. Host Based Intrusion Detection System (HIDS)

HIDS working within the software or agent components, it has run on the server and network devices (routers switch and so on). In fact, HIDSs are much better in detecting and responding to long term attacks such as data thieving .Host-based IDSs operate on information collected from within an individual computer system. A Host-based IDS monitors the inbound and outbound packets from the computer system only and would alert the user or administrator if suspicious activity is detected. The HIDS on the machine would be deployed, managed and monitored by the user. The HIDS on the hypervisor would be the responsibility of the provider. An HIDS is not just monitor network traffic, it can also trace more and settle with local settings of an OS and log records. Demerit of HIDS, it has harder to manage, as information must be configured and managed for every host monitored. Figure2 shows HIDS Model.

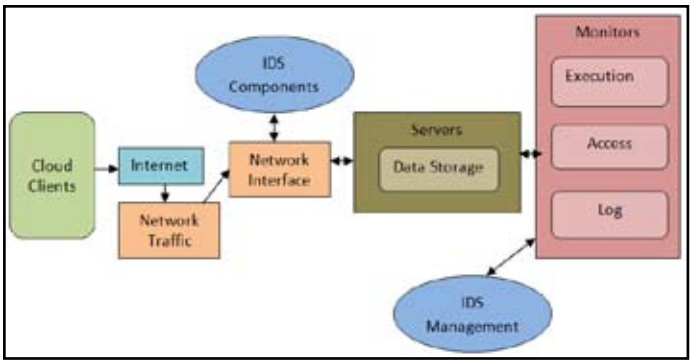

Fig. 2: HIDS Architecture

2. Network Based Intrusion Detection system (NIDS)

Network-based IDS can detect different situations based on specified points and generally located between the end point devices like routers, firewalls. A NIDS is an intrusion detection system that attempts to discover unauthorized access to a network by analyzing traffic on the network for signs of malicious activities and events. Network traffic stacks on different layers and every layer delivers the data coming from a layer to another layer. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting different hosts that are connected to the network segment, thereby protecting those hosts. Network-based IDSs often consist of a set of single purpose sensors placed at various points in a network. As the sensors are limited to running the IDS, they can be more easily secured against attacks, e.g. run the IDS sensors in stealth mode. Figure 3 shows NIDS Model.

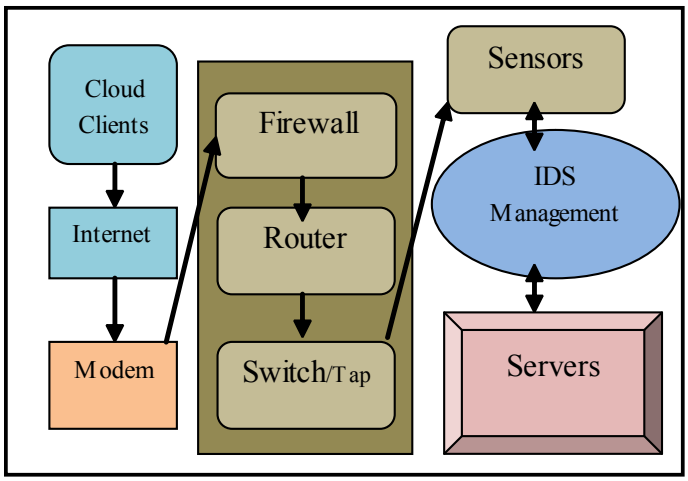

Fig. 3: NIDS Architecture

VI. Intrusion Detection Techniques

IDS using two kinds of techniques for analyzing events to detect attacks: Misuse Detection Approach and Anomaly Detection Approach [13].

Anomaly Detection Technique

Anomaly detectors identify abnormal unusual behavior on a host or network. Anomaly detectors construct profiles from historical data (behavior of users, hosts, or network connections) collected over a period of normal operation. The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the normal routine. A large number of false alarms, as normal patterns of user and system behavior can vary wildly. Anomaly detection includes; Threshold detection, Statistical measures, Rule-based measures, other measures, including neural networks, genetic algorithms, and immune system models.

Misuse Detection Technique

Misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called signature-based detection. The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. Misuse detectors are very effective at detecting attacks without generating an overwhelming number of false alarms. Misuse detector approach does not require extensive training in order to detect attacks.

VII. Proposed Work

Our proposed model is a resourceful Cloud IDS which can use much technique to pick up securities in IDS performance over the Cloud computing. In this IDS are uses sensors to check for malicious client data packets. Initially this system will reject unwanted users and then allowed to pattern checking in cloud. The IDS then sends intrusion alert to a monitoring service, which can provide instant reporting to cloud user organization management system with an advisory report for cloud service provider. Cloud computing provide submission and storage space services on remote servers. The clients do not have to worry about its preservation and software or hardware up-gradations.

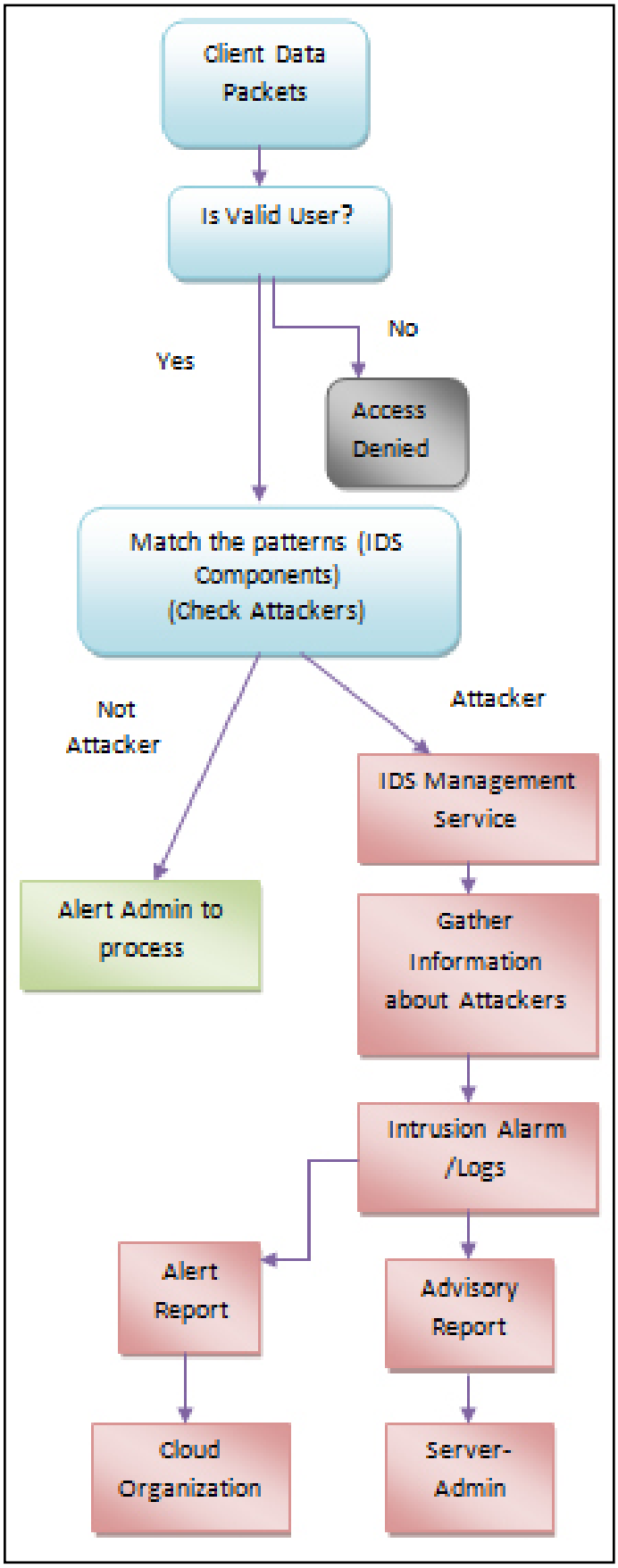

Fig. 4 : Proposed IDS Model

IDS would be placed outside the servers on bottle neck of network points such as switch, router or gateway for network traffic monitoring to have a global view of the system. It is to be facing the issue of huge quantity of data through network access rate in cloud environment. To handle a large number of data packets flow in such a surroundings an IDS come near has been proposed in this paper. The IDS able to process huge quantity of data and could reduce the packet loss. After an efficient processing the proposed IDS would pass the monitored alerts to a third party monitoring service, who would in turn directly inform the cloud user about their system under attack. Figure 4, shows the proposed IDS model. The cloud user accesses its data on remote servers at service provider site over the cloud network. User requests and actions are monitored and logged through a IDS. The alert logs are readily communicated to cloud user with an expert advice for cloud service provider.

VIII. Conclusions

Cloud computing is a model used in creature enterprise web and application server to a cloud of computers. Because of the enterprise nature of the system, there is a risk of security attacks on services and resources in cloud computing. Attacks are from either both outside and inside the cloud provider's network. In this paper, we have introduced the security issues of cloud computing and in terms of attack types and their defense mechanism by means of intrusion detection and prevention systems. We discuss existing threats for a Cloud infrastructure and are motivated to use IDS and its management in the Cloud. We propose the deployment of integrated and layered IDS on cloud that designed to cover various attacks. This IDS integrates knowledge and behavior analysis to increases a cloud's security.

References

[1] *S. Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing. IEEE, 2009, pp. 729–734.*

[2] *K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection for grid and cloud computing," It Professional, vol. 12, no. 4, pp. 38–43, 201*

[3] *H. Hamad and M. Al-Hoby, "Managing Intrusion Detection as a Service in Cloud Networks," International Journal of Computer Applications, vol. 41, no. 1, pp. 35–40, Mar. 2012.*

[4] *M. Jensen, N. Gruschka, L. L. Iacono, and G. Horst, "On Technical Security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing, pp. 109-116, 2009.*

[5] *R. Wu, G.-joon Ahnl, and H. Hul, "Information Flow Control in Cloud Computing", IEEE Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom) , pp. 1-7, 2010.*

[6] *M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." IEEE Xplore, pp 23-31, Jun. 2009.*

[7] *C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, January 2013.*

[8] *A. J. Duncan, S. Creese, and M. Goldsmith, "Insider Attacks in Cloud Computing," Proc. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, 2012, pp. 857–862.*

[9] *Zhou CV, Leckie C, Karunaseker S (2010) A survey of coordinated attacks and collaborative intrusion detection.*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Computer Secure 29(1):124–140

[10] Kazi Zunnurhain, Susan Vrbsky "Security Attacks and Solutions in Cloud"

[11] R. Bace and P. Mell, Intrusion detection systems. US Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2001.

[12] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," Computer Networks, vol. 31, no. 8, pp. 805–822, 1999.

[13] R. Bace and P. Mell, "NIST Special Publication on Intrusion Detection Systems", National Institute of Standards and Technology, 2001.

Authors Profile

T. V. S. Jeganathan received his M.Phil(C.S) Degree from Periyar University in the year 2013. He has received his M.Sc (C.S), Degree from Bharathidasan University, Thichy in the year 1995. He is working as Assistant Professor, Department of Computer Science, Siri PSG Arts & Science College for Women, Sankari, Salem, and Tamilnadu, India. His areas of interest include Artificial Intelligence, Data mining and warehousing and Cloud Computing.

T.Arun Prakasam received his M.Phil(C.S) Degree from Periyar University in the year 2007. He has received his M.Sc (C.S), Degree from Periyar University, Salem in the year 2006. He is working as Assistant Professor, Department of Computer Science, Siri PSG Arts & Science College for Women, Sankari, Salem, and Tamilnadu, India. His areas of interest include Software Engineering, Distributed Computing, Gird and Cloud Computing.