International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 12, December 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

IMPROVED CLOUD SECURITY MECHANISM WITH A SELF-MONITORED INTRUSION PREVENTION SYSTEM

R.Sundar Raj[1], Dr.V.Murali Bhaskaran[2]

[1]Research Scholar, Research and Development Centre, Bharathiar University, Coimbatore-641 046, Tamilnadu, (India)

[2]Principal, Dhirajlal Gandhi College of Technology, Omalur (Tk), Salem-636 309, Tamilnadu, (India)

ABSTRACT

Universally, Intrusion is the one, that causes serious level of problems to the system when allowed inside the local private ambience, in Cloud computing it is very common. Already the previously proposed work of String Based Intrusion Detection System (SBIDS) by the authors of this paper, in which a biography related intrusion detection system using a string matching mechanism, has been proven well in all aspects of detecting the intrusions aimed to the cloud network and its data. Actually, that is the pre-level of intrusion management to ensure improved foundation level of cloud security, the post-level is the present work in which the enhanced level of intrusion management is done through the Self-Monitored Intrusion Prevention System(SMIPS). By supplying the patterns of SBIDS as an input to this proposed system, the intrusion is handled with the action history and updates through universal cloud intrusion dealings that has to be done by correlating the Cloud Service Providers (CSPs) and the necessitated deed can be done. This has been proved in all means through the results obtained through the implementation of the proposed system of SMIPS. Through these systems of SBIDS and SMIPS, both the dead ends of the cloud service may have a relaxed way of dealing with the impact caused through the ever-irritating intrusions.

Keywords: Hypervisor, IDS – Intrusion Detection System, NIC – Network Interface Controller, VMs- Virtual Machines, VMM- Virtual Machine Monitor.

I INTRODUCTION

Cloud Computing is a popular terminology being the technology in recent era that really depicts the means of delivering any and all form Information Technology to an end user as a service wherever and whenever they are in need of them. This allows the users to gain access to the applications and data in a web-based ambience on demand [1][2][3][4][5][6]. Instead of the succession of programs and data on an individual desktop computer, everything is hosted in the 'Cloud' which is an unformulated assemblage of computers and servers accessed through the internet. It does not require or demand the end-user's knowledge on the physical location and configuration of the system that delivers the services [3][8][9]. For the people those who develop and manage

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

computer systems, Cloud Computing is all about horizontal scalability in the form of server capability; the technical challenge is developing operating systems and applications to manage this sort of on-the-fly scaling while keeping the mechanics of it invisible to the end users, since the data of the users are kept stored in the Cloud [10][27][12][13]. Thus, Security is an important factor in this area that has to be strengthened, to not let the unauthorized users to gain access to the confidential data.

1.1 Hypervisor

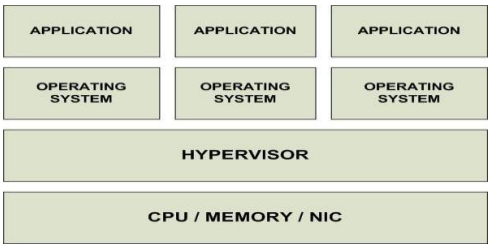

Fig. 1 Role of Hypervisor

The Hypervisor is a junction of abstracting hardware and allowing host resources sharing between the host machines and VMs. It is a program running on the host, and hence, susceptible to risk when the volume and complexity of application code increases. One attack of externally modifying hypervisor is known as Virtual Machine-based malware/rootkit, which attempts to execute malicious code instead of system call from hypervisor to the host operating system [23][27][13][20][18]. A Trusted Platform Module (TPM) in the host helps to create a trust relationship with the Hypervisor, whose role is depicted in Fig.1. It gets joint association with Network Interface Controller (NIC), and also with operating systems, also with the end user applications. This acts as a functional layer that performs the operations in an inter-relational way [23][20]. This is one of the important component that is residing in the technological aspect of Cloud Computing.

1.2 Roadmap of the work

In the present section 1, Introduction to Cloud Computing and Intrusion Management is given. In Section 2, the outline of the existing form of Intrusion detection and prevention system is given. In Section 3, the overview of the improved version of the proposed IDS in a self-monitored style is presented. In Section 4, the algorithm of the SMIPS is described. In Section 5, the implementation of the SMIPS algorithm is described. In Section 6, the obtained results are analysed in a detailed manner. In Section 7, the conclusion of the work is drawn out.

II EXISTING FORM OF IDS AND IPS

The need of Intrusion Detection System and the Intrusion Prevention System is Omni-present, irrespective of the field. This is very much, a need in the dynamic sector of cloud computing where the chances of intrusions are more. Here both the Intrusion Detection System and the Intrusion Prevention System are discussed in its present form.

2.1 Main Technology Classification of IDS and IPS

Intrusion Detection and Prevention Systems are majorly classified into three categories that are as follows:

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

2.1.1 Network based IDPS (NIDPS)

This kind of detection and prevention system monitors network traffic for particular network segments or devices and analyses the network and application protocol activity to identify suspicious activity [3][13][23][18]. NIDPS can be used to protect the whole network or part of network, to safeguard multiple systems, such as VMs, at a time.

2.1.2 Host based IDPS (HIDPS)

This kind of detection and prevention system monitors all or parts of the dynamic behaviour and the state of a computer system. Much as an NIDPS, this will dynamically inspect network packets. An HIDPS might detect which of the program accesses what kind of resources. There is also a complementary approach, that combines both network-based and host-based components which provides greater flexibility in deployment [1][5][27][9]. HIDPS can be used to detect and prevent intrusion on VM, Hypervisor or host system where it is deployed.

2.1.3 Application based IDPS (AIDPS)

This kind of detection and prevention system concentrates on events which occur in some specific application through analysing the application log files or measuring their performance. Its input is data sources of running applications [3][18][20][12].

2.2 Miscellaneous Technology Classification of IDS and IPS

Intrusion Detection and Prevention Systems also consists of some other miscellaneous categories, that are as follows:

2.2.1 Wireless based IDPS (WIDPS)

WIDPS is almost similar to NIDPS, but it captures wireless network traffic, such as ad hoc networks, wireless sensor networks and wireless mesh networks [12][13][27][13].

2.2.2 Network Behaviour based IDPS (NBIDPS)

An NBIDPS system inspects network traffic to recognize attacks with unexpected traffic flows [23][2][20]. The inspection is done in a well-defined manner.

2.2.3 Mixed IDPS (MIDPS)

Adopting multiple technologies, MIDPS can fulfil the goal for a more, complete and accurate detection [12][23][27].

2.3 Methodologies of IDS and IPS

Intrusion detection methodologies are classified into three major categories:

2.3.1 Signature-based Detection and Prevention

A Signature is a pattern or string that corresponds to a known attack or threat. Signature based detection is the process of comparing patterns against captured events for recognizing possible intrusions. Because of using the knowledge accumulated by specific attacks and system vulnerabilities, Signature-based Detection and Prevention is also known as Knowledge- based or Misuse Detection and Prevention [2][20][13]. This method is

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

complementary to that of the Anomaly detection and Prevention system, because they concern on certain attacks/threats.

Pros of Signature-based method:

- Simplest and effective method to detect known attacks
- Detailed way of doing the contextual analysis

Cons of Signature-based method:

- Ineffective to detect unknown attacks, evasion attacks, and variants of known attacks
- Little understanding to states and protocols
- Hard to keep signatures/patterns up to date
- Time consuming to maintain the knowledge

2.3.2 Anomaly-based Detection and Prevention

An anomaly is a deviation to a known behaviour, and profiles represent the normal or expected behaviours derived from monitoring regular activities, network connections, hosts or users over a period of time. Profiles can be either static or dynamic, and developed for many attributes, for example, failed login attempts, processor usage, the count of electronic mails sent, etc. Then, Anomaly detection compares normal profiles with observed events to recognize significant attacks. Anomaly detection is also called Behaviour based Detection [4][13][20]. Some examples are attempted break-in, masquerading (masking), penetration by legitimate user, Denial-of-Service (DoS), Trojan horse, etc., This method is complementary to that of the Signature detection and Prevention system, since it focuses on unknown attacks.

Pros of Anomaly-based method:

- Effective to detect new and unforeseen vulnerabilities
- Less dependent on OS
- Facilitate detections of privilege abuse

Cons of Anomaly-based method:

- Weak profiles accuracy due to observed events being constantly changed
- Unavailable during rebuilding of behaviour profiles
- Difficult to trigger alerts in right time

2.3.3 Stateful Protocol Analysis of Detection and Prevention

The Stateful in SPA indicates that IDS could know and trace the protocol states (e.g., pairing requests with replies) thought Stateful Protocol Analysis process looks like Anomaly Detections; they are essentially different. Anomaly Detections adopts preloaded network or host- specific profiles, whereas Stateful Protocol Analysis depends on vendor-developed generic profiles to specific protocols. Generally, the network protocol models in Stateful Protocol Analysis are based originally on protocol standards from international standard organizations [3][23][22]. This kind of detection and prevention system is also known as Specification- based Detection and Prevention.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Pros of Stateful Protocol Analysis method:

- Know and trace the protocol states
- Distinguish unexpected sequences of commands

Cons of Stateful Protocol Analysis method:

- Resource consuming to protocol state tracing and examination
- Unable to inspect attacks looking like benign protocol behaviours
- Might incompatible to dedicated Operating Systems or Anomaly based Detection and Prevention system

III IMPROVED VERSION: SBIDS TO SMIPS

3.1 Objective and Dynamic response of the proposed system

SMIPS is an Intrusion Prevention System that is proposed in a self-monitored style based on the inputs obtained from SBIDS, which is an Intrusion Detection System on a string basis. The proposed SMIPS monitors network traffic and system activities to detect possible intrusions with the help of SBIDS and dynamically responds to intrusions for blocking the traffic or quarantine it. SMIPS should be configured accurately for the expected results. If this is not being taken for the consideration, it stops the flow of packets resulting in network unavailability. For intrusion prevention, mostly firewall with IDS is used, which contains signature specifying network traffic rules. Based on the preconfigured rules, IPS decides whether network traffic should be passed or blocked. In response to detected attack, IPS can stop the attack itself, can change the attack contents or change security environment. In this present work, that proposed a self-monitored and an efficient host, network and application based intrusion detection and prevention approach, which does not require installing IDS and IPS on every node. By installing it in network level, it may get flowed to the hosts merged in to it and to the applications running on it.

This approach of SMIPS, solves trust problem and transferring alert message problem, that creates a panic and an immediate concentration with the appropriate recovery measures. It has a very less overhead and no false alarm rate and also prevents the DDoS attacks, which is a very big threat and a disturbance for the cloud suppliers and users, with a maximum effect. Also, the string pattern classification algorithm and matching algorithms are ideologically considered, which cooperatively detect DDoS attacks and send their logs to remote IPS machine that can monitor itself in an efficient manner, for constructing an efficient SMIPS algorithm. SBIDS is the framework in which Linux kernel implements. SMIPS is a firewall management intrusion prevention program based on SBIDS, that is made upon string patterns. StrTable extensions consist of two parts: First part is interacting with SBIDS application layer which is developed as shared library and second part is SMIPS kernel developed as kernel dynamic library. Kernel dynamic library is uploaded at runtime.

3.2 Mechanised control of the proposed system

A firewall Graphical User Interface is used to configure firewall rules. StrTable's application extension is used for authentication of rules configured by users and to parse the parameters of the rules. Each rule filled in data

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

structure supplied by StrTable. General data structure, then transferred to STRFETCH function which transforms data structure to another structure defined as StrTable application module. Also pointer to StrBuffer storing the packet information is transferred to STRFETCH function to identify the rules irrespective of the rules matching the data. The StrBuffer saves the data of the packet, such as source Internet Protocol address, destination port and socket number, which is captured when it goes through the STRFETCH. In many of the previously proposed systems, attacks cannot be prevented, but by this approach, it can be prevented with the idea of converting the intrusion patterns in the form of string, through which even the substring track is possible. The new kind of intrusions, that are spread world-wide are the upgraded intrusion, with the reference made to the available ones. Thus, the pattern of the intrusion string, even though cannot match at full length, can be found at the substring level with the details of StrBuffer history, using the knowledge base and compared with predefined instructions imposed to the system as per the administrator's concern.

3.3 Defence strategy

The defending agents, expert system, the detecting and identifying agents are used for real time defence, detection of intrusions and identification. If the intrusions are detected that are not at all familiar and does not have occurred previously, then the Observer Station calls the Shielder, prevents and generates alerts to the administrator or Virtual Machine Monitor (VMM). For some of the well-known and frequently caused intrusions, the ActBuffer history is taken for carrying out the preventive measures by itself and then give Review report. The Observer Station is used to monitor both the internal as well as intrusions from external means.

An intelligent SMIPS module based on dynamically distributed Cloud firewall linkage is used for real time interactive defence and better optimization of Cloud firewall. When the user of internal network accesses external host or network or application resources, SMIPS uses string feature detection and recognition mode of Cloud security for analysing and deciding safety of resources using string patterns which are accessed by the cloud users.

3.4 The need of compatibility

Having their own strengths and weaknesses, individual Intrusion Detection System and Intrusion Prevention System are not capable of providing full-fledged security. Thus, the attempt has been done to merge the previous work of SBIDS, which has been proved with the appropriate results to the currently proposed approach named SMIPS. It is very effective to use combination of SBIDS and SMIPS, which is called SBSMIDPS (String Based Self Monitored Intrusion Detection and Prevention System) that would be implemented, in future.

In the current work, the compatibility of SBIDS and SMIPS is proved, and the implementation of the SMIPS is done with a comparative analysis of it with traditional approaches, based on the results obtained. Apart from just identifying possible intrusions, SMIPS stops, takes some remedial measures and reports them to security administrators, if cannot be dealt by itself. Proper configuration and management of SBIDS and SMIPS combination can improve the level of security to the greater extent.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

3.5 Self dealt cloud firewall linkage

Considering the Cloud scenario, Host-based SMIPS can be deployed at VMs or hypervisors to protect the machines on which it is placed. Network-based SMIPS can be used to protect multiple VMs from network end points. Application-based SMIPS can be used to protect variety of applications, that are implemented in host or network level. Incorporating SBIDS on Virtual Machine allows monitoring the activity of itself. Cloud user should be held responsible to deploy, manage and monitor SBIDS on VM.

Placing SBIDS on underlying hypervisor, it provides an ability to detect intrusion activity including communication between VMs on that hypervisor. However large amount of communicating data reduces performance of traditionally approached IDS or causes cloud packet dropping. Deploying, managing and monitoring IDS should be done by the Cloud provider. However, in the currently proposed system, the virtual network that is established in host system allows VMs to communicate directly without using an external network. SMIPS can be located within such network to monitor traffic between the VMs as well as between the VM and host and can take preventive measures.

3.6 Enhanced operation of Virtual Machine Monitor (VMM)

Most of the currently available IDPS, works on cloud that operate at each of the infrastructure, platform, and application layers separately, and mainly support detection and prevention independent from the other layers. For the operating SMIPS in infrastructure layer, hypervisor is used to protect from different types of attacks in the infrastructure layer in which the Infrastructure is provided as a service. The proposed approach is having improved reliability and availability of the system, because the infrastructure can be secured most of the time, and running services can rely on the secure infrastructure. This model has also presented a solution to heal the system if the infrastructure collapsed due to the high severe attacks over the system. A Virtual Machine Monitor (VMM) solution is proposed in an improvised manner that embeds as a software layer to control the physical resources and it allows running multiple operating systems.

The VMMs are capable of improving the efficiency of attack detection and prevention in SMIPS in a self-monitored and automated way because they have complete control of the system resources and good vicinity to the internal state of the virtual machines. Thus, this proposed solution can overcome the difficulties in monitoring virtual machines that are dynamically provisioned, that are either adding or removing.

IV THE SMIPS ALGORITHM – PROPOSED APPROACH

The new algorithm is proposed here, for performing the intrusion prevention system in a self-monitored way. The algorithm that is given here may be implemented to any simulation tool, programming languages and even in real-time scenarios with due fine-tuning. The generic form of the algorithm is presented as a Pseudocode as given below:

Algorithm 1. SMIPS

ALGORITHM Self-MonitoredIntrusionPreventionSystem (NS[0,…..k-1], OS[0,…..l-1], SS[0,…..m-1], A[0,…..n-1])

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

//Implements the self-monitored string matching based intrusion detection and prevention system in a self-monitored way

//Input: An array NS[0,…..k-1] of k characters representing the string pattern of the newly occurred intrusion in current network; An array OS[0,…..l-1] of l characters representing the string pattern of the already occurred intrusion in current network; An array SS[0,…..m-1] of m characters representing the sub-string pattern of the newly occurred intrusion in current network; An array AS[0,…..o-1] of o characters representing the actions taken for the early occurred intrusion in current network; An array US[0,…..p-1] of p characters representing the actions taken for the early occurred intrusion updated globally in other networks; An array MS[0,…..q-1] of q characters representing the actions taken for the early occurred intrusion updated globally in other networks.

//Require: ActBuffer, StrBuffer, Shielder, Observer Station, Signalling (True Positive [TP], True Negative [TN], False Positive [FP] and, False Negative [FN])

01- Call ALGORITHM StringBasedIntrusionDetectionSystem ;
02- Sort the request of cloud resources in the form of Virtual Machine, according to the arrival;
03- The requests are arranged in the decreasing order of arrival rate and based on the amount of resource requirement;
04- for each request R
05- Identify the whole range of the network from source i to destination j;
06- Check for the intrusion by circularly referencing StrTable
07- for i = 0 to n-m do j = 0
08- If intrusion packet is found in the network
09- Then call STRFETCH; NS[k-a] = TO_STRING (Intrusion packet data); Compare (NS[k-a], OS [0,….. l-1]);
10- If output value is TRUE
11- Then
12- Fetch OS[k-a] match from AS[0,…..n-1];
13- Perform the stored action from the action log history by referring ActBuffer;
14- Send the prevention action report to the Source i; Send the True positive signal to the destination j;
15- Else
16- SS[k-a] = TO_SUBSTRING (NS[k-a]); Compare (SS[k-a], OS[0,…..l-1]);
17- If output value is TRUE
18- Then
19- Fetch SS[k-a] match from OS[0,…..n-1]; Fetch OS[k-a] match from AS[0,…..n-1];
20- Perform the stored action from the action log history by referring ActBuffer; Refer StrBuffer;
21- Send the prevention action report to the Source i;
22- Send the True positive signal to the destination j;
23- Else

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

24- Reconfigure the action log; MS[0,…..n-1] = Merge (AS[0,…..n-1], US[0,…..n-1]);
25- Compare (Merge (NS[0,…..n-1], SS[0,…..n-1]), MS[0,…..n-1]); while j < m and P[j] = T[i+j] do
26- If output value is TRUE
27- Then
28- Fetch Merge (NS[0,…..n-1], SS[0,…..n-1]) match from MS[0,…..n-1];
29- Perform the stored action from the action log history by referring ActBuffer;
30- Send the prevention action report to the Source i; Send the True positive signal to the destination j;
31- Report through Signalling to the Source i; Call Shielder from Observer Station; j = j+1;
32- Run the IPS in monitor mode
33- Verify whether the system is tuned properly; Check whether False positives and False negatives are reduced;
34- When system fails or blocked,
35- All the actions will be temporarily suspended for a while,
36- Alert message of not to transmit any data or carry out applications during the stage to i and j;
37- Flowing data and running applications are temporarily being brought to the hibernated state;
38- Resumed it after the system rollbacks to the normal state;
39- Send the instruction for the frequent verification is insisted to the users; Impose Firewall rules; Wait for signalling;
40- If any systems related to the transfer of data or applications went offline
41- Alert is given through the remote signalling method; Enable the users to take over the job back without any loss;
42- All the data are duly backed up, if any severity happens, provide the data from the backup;
43- If j = m Then return i ;

V IMPLEMENTATION OF SMIPS ALGORITHM

5.1 Implementation of SMIPS in Snort

Snort can be implemented by the rule-based approach, where in which when implemented, the SMIPS consists of the following elements: (i) A Filter Specification, to what threat of a certain flow the rule works; (ii) A String, to be the signature of suspicious payloads; (iii) A position for the occurrence of that string; (iv) A corresponding action when all the conditions are met. According to the Amdal's law, string matching would be the first consideration to dramatically improve the performance, as it accounts for about 75% CPU load of SMIPS. The implementations have given satisfactory performance. The simulative prototype implementation a maximum range of throughput of 15 Gbps. Due to the drawbacks of the hardware way, through which usually high cost, hard to modify, and tied to a specific implementation, where Snort is most widely used open-source tool. The Snort focuses on the network intrusion detection. Both have their own signature string sets but with a great diversity and the expression is not expanded for simplicity. Snort explores many for exact-match signature

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

detection and to detect the other signature patterns in the form of strings. There is a considerable rise in the implementation and improvement to both tools. Snort can performance well on Linux and Windows Operating System. Snort achieves a maximum traffic processing throughput of 5.5 Gbps. A log maintaining method is proposed to do the string search for intrusion detection and prevention applications.

VI RESULT ANALYSIS

6.1 Speedy performance of SMIPS

A virtualization oriented SBIDS for cloud computing environment that was proposed before this present work, performs well with SMIPS, which used network data flow monitoring and real time file integrity. Beside the structure of SMIPS, detection technique is the other highlighting factor of this work. String matching algorithms is faster because it only recognizes the limited number of intrusions by multiple level matches, while anomaly learns the traffic and actions to identify the safe activities and potential intrusions.

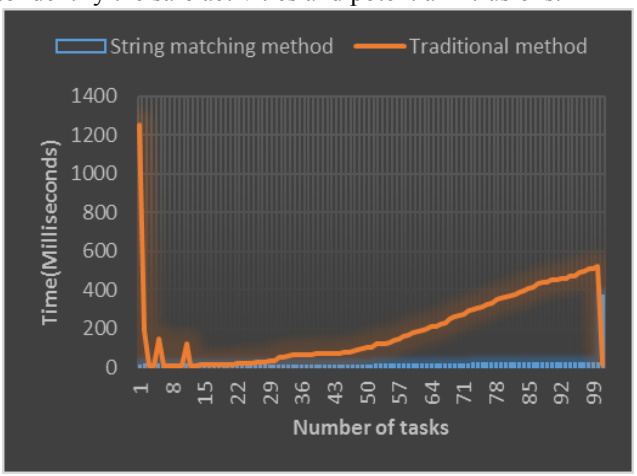

Fig. 2 Speed maintenance rate

The models of SBIDS and SMIPS, which employed both types are known as Hybrid which they have the best accuracy and performance among the other individual methods. These efficiencies are evidence to acknowledge the performance of proper requirements that are to be identified before initiating any development, and that has been done here. The speed of the proposed system of SMIPS is proven higher than the traditional approaches through Fig. 8. The speed is comparatively higher and is worth adapting it.

VII CONCLUSION

The technology of Cloud computing is upgrading day by day with new improvisations and due fine-tuning processes. This kind of technology adapts itself to all systems that has real time usage. The growth of it is becoming wider, and by implementing this SMIPS in a real time application its root may be deepened by vanishing out the hesitation that lies in the cloud willing minds regarding the security inurement approach in the cloud technology. SBIDS being the pre-level of intrusion management to ensure improved foundation level of cloud security, the post-level is the enhanced level of intrusion management that is done through the presently proposed Self-Monitored Intrusion Prevention System(SMIPS). By the intrusion patterns that are derived in the

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

form of strings, that are stipulated by SBIDS, the exact match part of the intrusion is detected efficiently with a biography memory. This system has been proved in all means through the results obtained through the implementation of the proposed system of SMIPS. Through these systems of SBIDS and SMIPS, the state of relaxed dealing of intrusions is carried out in an efficient manner as a single system SBSMIDPS.

REFERENCES

[1] Arpit J. kuche & D M. Dakhane-Sant Gadge Baba, "A Survey of Mobile Virtualization using Cloud Computing", Amravati University, Amravati, Maharashtra, India- International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)-ISSN 2250-1568-Vol. 3, Iss. 1, Pp.191-196, Mar 2013.

[2] Aman Bakshi, Yogesh B, "Securing cloud from DDOS Attacks using Intrusion Detection System in Virtual Machine", iEEE Computer Society, Proceedings of Second International Conference on Communication Software and Networks, 2010.

[3] Arun Fera M, Manikandaprabhu C, Ilakiya Natarajan, Brinda K, Darathiprincy R, "Enhancing security in Cloud using Trusted Monitoring Framework", Thiagarajar college of Engineering, India, International Conference on Intelligent Computing, Communication & Convergence, Elsevier, Science Direct, Procedia Computer science,Vol.48, Pp 198-203, 2015.

[4] Bhaskar Prasad Rimal, Ian Lumb, "A Taxonomy and Survey of Cloud Computing Systems", Kookmin University, Korea and York University, Canada, Fifth International Joint Conference on INC, IMS and IDC, Pp.44-51, Nov 2009.

[5] David C. Chou, Eastern, "Cloud Computing: A value creation model", Michigan University, USA, Elsevier, Computer standards and Interfaces,Vol.38, Pp.72-77, 2015.

[6] Junaid Arshad, Paul Townend, Jie Xu, "A novel intrusion severity analysis approach for clouds", Elsevier, Future Generation Computer Systems, Vol.29, Pp-416-428, 2013.

[7] Raja Wasim Ahmad, Abdullah Gani, Siti Hafizah A.Hamid, Muhammad Shiraz, Abdullah Yousafzai, Feng Xia, "A survey on virtual machine migration and server consolidation frameworks for cloud data centers", University of Malaya and Dalian University of Technology, China, Elsevier, Journal of network and computer applications, Vol.52, Pp-11-25, 2015.

[8] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz,Andrew Konwinski, Gunho Lee,David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing", Electrical Engineering and Computer Sciences, University of California at Berkeley, Pp.1-23, Feb 2009.

[9] Mazhar Ali, Samee U. Khan , Athanasios V. Vasilakos, "Security in cloud computing: Opportunities and challenges" , North Dakota University, Kuwait University, COMSATS IIT, Elsevier, Journal of Information sciences,Vol.305, Pp-357-383, 2015.

[10] Dhinesh Babu L.D, P.Venkata Krishna, "Honey bee bahavior inspired load balancing of tasks in cloud computing environments", VIT University, Vellore, Elsevier, Applied Soft Computing, Vol.13, Pp.2292-2303, Feb 2013.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[11] Michael Miller, "Cloud Computing- Web based applications that change the way you work and collaborate Online", Fourth impression, Pearson, 2012.

[12] Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, Joaquim Celestino Junior, "An intrusion detection and prevention system in cloud computing: A systematic review", Elsevier, Journal of Network and Computer Applications, Vol.36, Pp-25-41, 2013.

[13] Dr. Kumar Saurabh, "Cloud Computing – Insights in to New- Era Infra structure", WileyIndia, 2011.

[14] Jianhua Che,Yamin Duan, Tao Zhang, Jie Fan, "Study on the security momdels and strategies of cloud computing" , State grid research institute and Shijiazhuang University of Economics, China, International Conference on Power electronics and engineering application, Elsevier, Science Direct, Procedia Engineering, Vol.23, Pp.586-593, 2011.

[15] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung, "Intrusion detection system: A comprehensive review", Elsevier, Journal of Network and Computer Applications, Vol.36, Pp-16-24, 2013.

[16] Kevin T.McDonald, "Cloud Computing –Managing Risk in the world of Cloud Computing", BPB Publication, 2010.

[17] Gautham Shroff, "Enterprise Cloud Computing – Technology", Architecture, Applications, Cambridge, 2011.

[18] Dimitrios Zissis, Dimitrios Lekkas, "Addressing Cloud Computing Security Issues", University of Aegean, Greece, Elsevier, Journal of Future Generation Computer Systems, Vol.28, Pp-583-592, Dec 2010.

[19] Flavio Lombardi, Roberto Di Pietro, "Secure virtualization for cloud computing", Journal of Network and Computer Applications, Elsevier, Pp.1-10, Apr 2010.

[20] Dawei Suna, Guiran Chang, Lina Suna and Xingwei Wanga, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments"- Northeastern University, China, Advanced in Control Engineering and Information Science, Elsevier, Science Direct, Procedia Engineering, Vol.15, Pp 2852-2856, 2011.

[21] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, Muttukrishnan Rajarajan, "A survey of intrusion detection techniques in cloud", Elsevier, Journal of Network and Computer Applications, Vol.36, Pp-42-57, 2013.

[22] Qi Zhang, Lu Cheng, Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges", Journal of Internet Server Application, Springer, Vol.1, Pp.7-18, Apr 2010.

[23] Amit Gupta, Dinesh Kumar, Dushyant Singh, Lav Singh,"A Comparative Study of Cloud Computing (Key Principles and its Issues)", 2nd National Conference in Intelligent Computing & Communication-Dept. of IT, GCET, Greater Noida, India, ISBN: 9788175157538-2008.

[24] Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha Mat Kiah, Ahmed Patel, "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique", Elsevier, Engineering Applications of Artificial Intelligence, Vol.26, Pp-2105-2127, 2013.

[25] Victor Chang, Yen-Hung Kuo, Muthu Ramachandran, "Cloud computing adoption framework: A security framework for business clouds", Elsevier, Future generation computer systems, Vol.57, Pp-24-41, 2016.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[26] Anthony T.Velte, Toby J.Velte and Robert Elsenpeter, "Cloud Computing –A Practial Approach" ,TMH, 2010 .

[27] Ashfaq Hussain Farooqi, Farrukh Aslam Khan, Jin Wang, Sungyoung Lee, "A novel intrusion detection framework for wireless sensor networks", Springer, Pers Ubiquit Comput, Original Article, Verlag London Limited, 2012.

[28] Subashini S, Kavitha V, "A Survey on security issues in service delivery models of cloud computing", Anna University, Tirunelveli, Elsevier, Journal of Network and Computer Applications , Vol.34, Pp.1-11, 2011.

[29] Sancika Gupta, Padam Kumar, and Ajith Abraham, "A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Article ID: 364575, 12 pages, 2013.

[30] Seyed Mojtaba Hosseini Bamakan, Behnam Amiri, Mahboubeh Mirzabagheri, Yong Shi, "A New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming", Elsevier, Science Direct, Procedia Computer Science, Vol. 55, Pp-231-237, 2015.

Authors' Biography

R.Sundar Raj, Research scholar in Bharathiar University, Coimbatore and Assistant Professor, Department of Computer Science in Kongu Arts and Science College (Autonomous), Erode, Tamilnadu, India has received his B.Sc in Computer Science and MCA degree from Bharathiar University and secured University I Rank in both the degrees. He has also published research papers in International journals. He is currently pursuing Ph.D programme with his area of research as Cloud Computing.

Dr. V. Murali Bhaskaran, Principal, Dhirajlal College of Technology, Omalur, Tamilnadu, India has nearly 25 years of experience in technical education. He obtained his B.E. Degree in Computer Science and Engineering from Bharathidasan University, Trichy in the year 1989, M.E. degree in Computer Science and Engineering and Ph.D in Computer Science and Engineering from Bharathiar University, Coimbatore in the year 2000 and 2008 respectively. He has published more than 30 papers in Journals and Conferences both at National and also in International level. His areas of interest include Computer Architecture, Computer Networks, Network Security, Information Security, etc.,