International Journal of Knowledge Based Computer Systems
10 (1) June 2022, 17-21
http://www.publishingindia.com/ijkbcs/

To Study the Hypervisor Scanner Model with ANN for Cloud Systems

Anshu Mali Bhushan[1*], Harsh Kumar[2] and Devendra Singh Chauhan[3]
[1]Research Scholar, Computer Application Department, Himalayan Garhwal University, Pauri Garhwal, Uttarakhand, India. Email: hianshumali@gmail.com
[2]Faculty of Computer Application, Himalayan Garhwal University, Pauri Garhwal, Uttarakhand, India. Email: research@hgu.ac.in
[3]Assistant Professor, Department of Physics, Dr. PDBH Government PG College, Kotdwar, Uttarakhand, India. Email: dr.devchauhan78@gmail.com
*Corresponding Author

Abstract: The detection part is called the Hypervisor Scanner, which is programmed to detect malicious insiders. Using the feed forward neural network, the hypervisor scanner is generated and trained with a supervised learning algorithm referred to as the Levenberg-Marquardt algorithm. The three criteria are considered for service level agreement, such as bandwidth requirement, memory consumption and storage space. The Hypervisor Scanner can detect malicious insiders in cloud systems that breach SLA and suffer from an insecure cloud administrative domain that lacks control over the cloud service provider (CSP). Here, the Hypervisor Scanner is constructed using the biologically inspired classification approach referred to as artificial neural network modelling. ANN teaching uses the Levenberg-Marquardt learning algorithm. The LM algorithm works by minimising the average square error to boost the detection system. For detecting malicious insiders, the Hypervisor Scanner uses threshold values for SLA parameters. It is known from performance review and comparison that the Hypervisor Scanner is the appropriate one with high detection accuracy and low false alarm rate for the detection of malicious insiders. This can therefore be effective, robust and realistic in the detection of malicious insiders in and around the cloud world.

Keywords: Architecture, Cloud computing, Commercial and technological, Hypervisor Scanner.

I. Introduction

Due to the evolutionary growth of numerous existing methods and computing facilities, such as distributed networks, services, applications and infrastructures, including network collection, computing technologies and storage resources, cloud computing allows the development of a commercial and technical service model. While cloud computing is growing in academia, enterprise, and industry, it is still an evolving paradigm. Via optimization, cloud computing has the ability to minimise costs and increase the benefits of operations and economic features (Catteddu & Hogben, 2009) [1]. In addition, cloud computing greatly strengthens and allows Internet infrastructures to create a universal computing model. This potentially evolved computing model will turn out to be a great failure model without adequate protection and privacy solutions built for cloud systems. It is imperative to ensure information security controls when using the internet, cloud computing and wireless applications. Therefore, the protection and privacy issues of this unique model are major obstacles to its adoption (Bruening & Treacy, 2009) [2]. The architecture of the cloud is shown in Fig. 1. The figure illustrates the characteristics of cloud computing systems and how the functionality of the cloud computing model can be easily accessed by users.

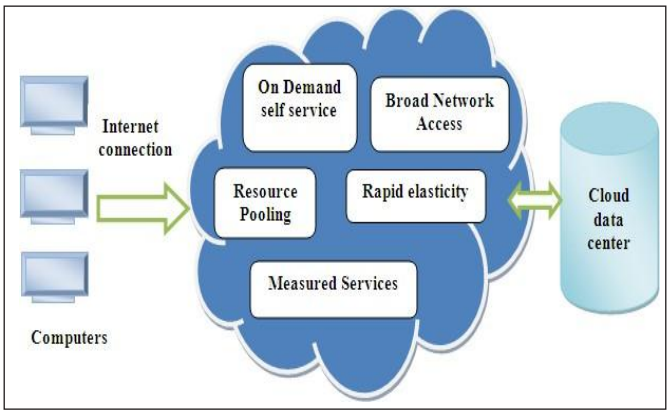

Fig. 1: Cloud Computing Architecture

The main objective of this research is to recognise and study the security problems that can impact the performance of cloud systems. The aim of the research work is to define a security mechanism that can be used to obtain prominent security solutions. As a result, this dissertation also aims to provide a malware detection component based on Hypervisor that is

appropriate for the detection of malicious activities against cloud technology in a dynamic cloud environment.

A. Hypervisors and Virtualization

Virtualization is an important feature that makes it easier for customers to access conceptual infrastructure and services as isolated VMs (Takabi *et al.,* 2010) [3]. A virtual machine monitor or hypervisor is a component of software for platform virtualization that enables multiple operating systems to run simultaneously on a host device. As this facilitates the generation of virtualized sharing services, the attack surface is thus strengthened. Therefore, a mechanism is required to guarantee strong VM isolation, arbitrated sharing, and stable VM communications. This can be done by using a versatile framework for access control and monitoring that handles VM control and sharing capabilities within a cloud host (Chen *et al.,* 2010) [4].

B. Layered Architecture of Cloud System in Virtual Environment

Cloud draws more individuals to use web services as well as misuse cloud services and its tools with faster growth of web-based services. A survey was conducted on business and technological problems that directly impact cloud computing efficiency at design and implementation levels (Nirmala & Sridaran, 2012) [5]. Cloud apps run outside the firewall and transfer to a public domain that has a good security awareness. Furthermore, the dynamic existence of virtual machines makes the process of monitoring more complex. In order to use the detection system, the hypervisor-based technology that encourages and regulates the execution of VMs and middleware can also be used. Hence, in this dissertation, the Hypervisor-based malware detection component is proposed to detect unauthorised access to malware in the cloud environment. In Fig. 2, the Hypervisor virtual cloud architecture is shown.

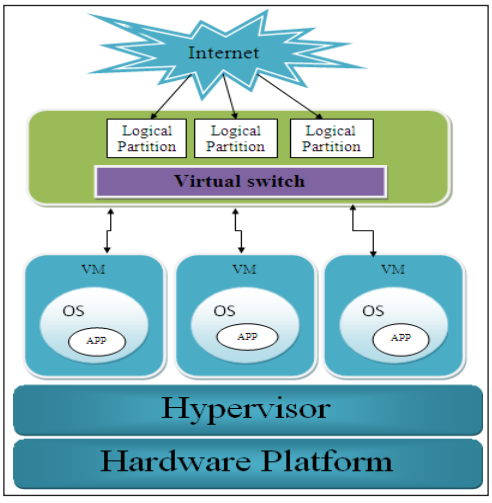

Fig. 2: Layered Cloud Architecture with Hypervisor

Virtualization offers web-based software and IT companies with improved and streamlined performance for applications in a cost-effective manner. This makes distribution of cloud service much simpler and scalable. Virtualization can be applied to anything in a cloud environment that relies on storage, operating system, network, device, and software/hardware virtualization forms of virtualization. One of the cloud providers, Infrastructure as a Service, provides data virtualization (IaaS). This allows many, on a pay-use basis, to have access to vast quantities of cloud resources. Virtualization suits are prepared for cloud computing with the three most critical virtualization properties: Partitioning, Isolation and Encapsulation. Virtualization (Bento & Aggarwal, 2012) [6] is described as the virtual description of something such as hardware, operating system, software, etc. Virtualization (Jin *et al.,* 2013) [7] is a method for providing parallel and interactive access to a large pool of information centre that supports many instances of control over multiple OS that successively generates hardware virtualization Hypervisor requires many OS instances to share the hardware facilities it is hosted on.

It addresses the similarities and differences between cloud computing and multiprogramming. Virtualization allows multiple operating systems to share CPU resources where they are handled by multiple OSes who have no knowledge of them. Normally the OSes are supposed to be managed by the underlying hardware. In cloud systems, different operating systems are managed and executed by the hypervisor layer.

The virtual machine runs a mechanism for the user on a single physical device. Virtual machines can transfer their states dynamically. The VM will move unconditionally from one platform to another. It is possible to clog, poise or infertile VM. Virtual machines run multiple programmes on a single hardware platform that are stored at different host device locations. Because of the complex existence of cloud technology (Vinothina *et al.,* 2012) [8], it is possible to migrate virtual computing environments and scale their properties over a multi-domain infrastructure. The operating system that is installed and executed on a virtual machine is the Guest OS. The Hypervisor controls the guest operating system that operates on virtual machines (Sabahi, 2012) [9]. Hypervisor enables numerous OS instances to share the hardware facilities on which it is hosted.

C. Hypervisor Layer is Used to Deploy Malware Detection System for Cloud

Web-based services and cloud services are being built more rapidly, attracting many users to use web services and hack cloud services and resources. They may have a serious awareness of security as cloud apps run outside the firewall and move on to the public domain. In addition, the complex design of virtual machines makes the control process more difficult. Therefore, it is possible to use a virtual machine monitor or hypervisor-based technology. It can be used to use the detection

system as it progresses and monitors the execution of VMs and middleware. The Hypervisor-based malware detection system is therefore proposed in this research in order to recognize unauthorised access to cloud systems. The malware detection system based on Hypervisor is an intrusion detection system provided to the hypervisor layer. The Hypervisor-based malware detection component is designed to observe both host and network-based activities in the cloud infrastructure, based on the rapid flow of huge amounts of data. This conducts several tasks in the virtualization layer, such as tracking, managing and evaluating, instead of being directly deployed in virtual machine monitoring. In order to take appropriate action against malicious activities, the analysis and control of the Hypervisor-based malware detection component is provided to the cloud administrative module in the cloud environment. The malware detection component based on Hypervisor consists of two features that can distinguish it from conventional intrusion detection systems, including

- Isolation from attackers and
- Transparency to attackers.

The isolation of the malware detection component based on Hypervisor from attackers secures it from direct attacks. The portion of hypervisor-based malware detection is clear to attackers, as it is both host and network-based IDS without virtual machines being directly accessible. The malware detection component based on the Hypervisor should guarantee virtual machine security and ensure virtualization layer safety. In the detection method, most of the attacks in the cloud environment often seek to compromise. But this malware detection component based on the hypervisor is built in such a way that it is not neutralised or compromised by any action. In virtual networks, Hypervisor monitors VMs and middleware by allowing VMs to be inspected by the host system. The Hypervisor is positioned between the virtualization layer and the kernel. Hypervisor Detector can discover any form of attack by actively and passively monitoring cloud environments, thereby ensuring that cloud components have not been compromised. The Detector Hypervisor minimises VM transparency.

II. Research Methodology

The Proposed Hypervisor Scanner Developed with ANN

Even if the existence of the malicious insider is not open, this chapter defines the malicious insider as an authorised user who breaches the Service Level Agreements (SLA) and infuriates the hacking of cloud infrastructure by affecting cloud services and resources. In order to use cloud services, consumers must acquire a legal conformity with CSP called Service Level Agreements. According to SLA, the cloud service provider (CSP) (Maurer *et al.,* 2012) [10] is responsible for the efficient provision of services and resources. CSP must also be guaranteed to mitigate breaches of SLA and optimise consumption of energy. Huge numbers of users have to share cloud services. This limitation demands that the computing activity of a single user does not accumulate cloud resources. In certain cases, by sending a broad resource request to access the cloud resources, malicious insiders attempt to break SLAs. The three attributes of SLA (Maurer *et al.,* 2012) are addressed in this section, such as 1) Bandwidth requirement, 2) Utilisation of memory and 3) Space space. Threshold values are allocated to each factor, such as memory consumption and storage space, as shown in Table I, and for bandwidth requirements. The dishonest cloud administrator, who is deficient in CSP management, is unable to analyse user behaviours. Often called the hypervisor layer, the virtual machine monitor (VMM) provides abstraction between real and virtual machines that can monitor and supervise virtual machine activities. By taking this into account, at the Hypervisor layer, the detection component called Hypervisor Scanner is built to track the virtual clients requested for services and resources.

Table I: SLA Attributes and Their Threshold Values

Sr. No.	Attribute for SLA	Threshold Limit
1	Bandwidth	8Mbits/s
2	Memory utilization	500MB
3	Storage capacity	1200GB

III. Results and Discussion

In order to have a better classification (Abdel-Azim *et al.,* 2009) [11], the Hypervisor Scanner is modelled using the Artificial Neural Network modelling technique on whether the user is malicious or normal with greater accuracy. In this model, for training ANN, the Levenberg-Marquardt (LM) back propagation training algorithm (Linda *et al.,* 2009) [12] is used. Kenneth Levenberg and Donald Marquardt created the Levenberg-Marquradt algorithm (Yu & Wilamowski, 2012) [13] to provide a better solution to the issue of minimising a nonlinear algorithm. The writers (Pradeep *et al.,* 2011) [14] addressed the relevance of ANN's LM training algorithm. Based on the above-mentioned SLA features, the Hypervisor Scanner part is skilled and tested to determine the malicious insider that violates the SLA. How this method works is explained in Algorithm.

IV. Hypervisor Scanner Modelled with ANN

The hypervisor scanner is constructed using the Levenberg-Marquardt back propagation algorithm for ANN modelling. For larger datasets, the conventional classification techniques involve significant computing power, memory and CPU resources. The common learning method (Yang & Fung, 2008) [15] for machine learning to improve the efficiency of the intelligent system is ANN. The artificial neural network (Abdel-Azim *et al.,* 2009) [11] is a very important modelling

tool for accurately classifying (Donghai & Weiwei, 2013) [16], especially where conventional analysis is difficult. ANN is an efficient method for mathematically simulating the capacities of the human brain. The neural network consists of the essential processing unit, a group of neurons. Since multiple neurons function at the same time, the brain can stimulate and generate better results quickly. The Artificial Neural Network works with multiple neurons simultaneously to boost their efficiency, according to the same methodology. Either through supervised or unsupervised learning methods, the ANN must obtain and foresee. The related patterns between input data and corresponding target values can easily be learned by ANN. Input and output specifications are necessary for the supervised back propagation learning technique, where the training takes place iteratively by using a collection of training samples.

The neuron (Pradeep *et al.,* 2011) [14] is the central operating entity with an input layer, a collection of hidden layers and an output layer for the neural network. The weight is the number for an artificial neuron and it represents the neuron's weight value. The input values are totally applied and altered by weights. The activation function finally regulates the output amplitude. The neuron model for neural networks is shown in Fig. 3.

This model of ANN has a structure of three layers of network 1. The input layer is equivalent to the number of parameters 2 with three input neurons. Hidden layer with 2 computational neurons that are hidden in order to determine the number of neurons in the secret layer, there is no clear formula. There are certain laws of thumb, anyway, for the neurons to determine. The formula used in this work is

$$N = \sqrt{(m+2)n} + 2\sqrt{n/(m+2)}$$

In which the number of input neurons is n and the number of output neurons is m. 3 Layer of output of one output neuron. Artificial neural network simulation for the Hypervisor Scanner as shown in Fig. 4.

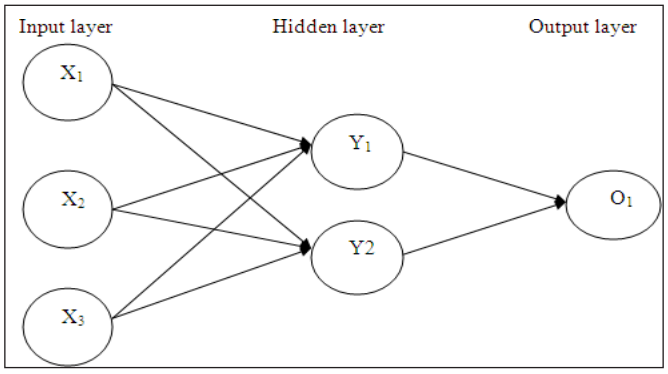

Fig. 3: Model of Neuron in ANN

The input signals flowing from the input layer in the feed forward network take the information from original data that advances through any hidden neurons in hidden layers, eventually reaching the output units. The input variable values are placed in the input units during the network execution and the secret and output layer nodes are gradually executed. To generate the output of the node, the activation value is passed through the activation function. By summing the weighted output values of the nodes in the preceding layer, each node in the layer calculates their activation value. The outputs of the output layer serve as the output of that network after execution of the entire network.

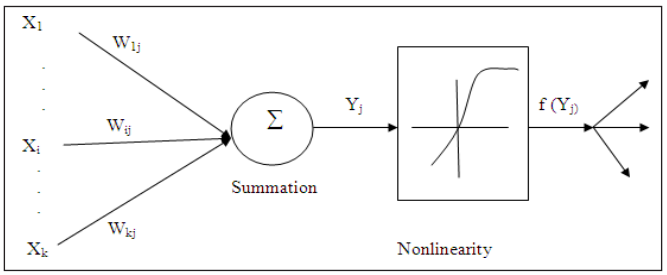

Fig. 4: ANN Modelling for Hypervisor Scanner

By using a simulation, the Hypervisor Scanner architecture is assessed. MatLab R2010 with Intel core2 processor operating at 2GHz, 2GB of RAM is used for Hypervisor Scanner simulation. Levenberg Marquardt's trainlm function is used to train the network, and is also the quickest algorithm for back propagation. The synthetic dataset is generated with characteristics such as bandwidth requirement, memory consumption and storage capacity with 500 data for experiment and study. The machine is trained to perform 100 iteration numbers. The dataset is split into three separate sets, called datasets for preparation, testing and validation. For networks, the training dataset is used to learn the patterns that occur in the dataset. To assess the skill of the qualified network, the testing dataset is used. By using the validation dataset, the performance of the network is assessed. Training uses 70 percent of the data in this model, testing uses 15 percent of the data, and validation uses 15 percent of the details.

V. Summary

This proposed method uses a better governing system called Hypervisor Scanner to detect malicious insiders in a virtual cloud setting where the cloud is controlled by a single cloud management domain coupled with a lack of cloud service provider (CSP) power. Here, the Hypervisor Scanner is designed using the best classification technique called Artificial Neural Network Modelling. To train ANN, the Levenberg-Marquardt (LM) back propagation algorithm is used. For experiments, the three attributes of SLA are considered, such as bandwidth requirement, memory consumption and storage space. In terms of bandwidth requirements, memory usage and storage space, users request more resources and are branded as malicious insiders. The experimental results show that the proposed Hypervisor Scanner generates mean values of squared error and regression that are approximately equal to zero and one

respectively. It can be found from a performance comparison that the Hypervisor Scanner detects malware behaviour with a minimum error. The ANN-designed Hypervisor Scanner has high detection precision and a low false negative rate. This can therefore be reliable, robust and realistic in order to detect malicious insiders in and around the cloud world.

References

[1] D. Catteddu, and G. Hogben, "Cloud computing: Benefits, risks and recommendations for information security," European Network and Information Security Agency, Technical Report, 2009.

[2] Bruening and Treacy, "Cloud computing: Privacy, security challenges," Bureau of National Affairs, 2009.

[3] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24-31, Nov.-Dec. 2010, doi: 10.1109/MSP.2010.186.

[4] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security," University of California, Berkeley, Report No. UCB/EECS-2010-5, Jan. 20, 2010.

[5] A. P. Nirmala, and R. Sridaran, "Cloud computing issues at design and implementation levels - A survey," *International Journal of Advanced Networking and Applications*, vol. 3, no. 6, p. 1444, 2012.

[6] A. M. Bento, and A. K. Aggarwal, *Cloud Computing Service and Deployment Models: Layers and Management*. USA: IGI Global, 2012, pp. 1-365.

[7] H. Jin, F. Xu, F. Liu, L. Liu, B. Li, and B. Li, "iAware: Making live migration of virtual machines interference - Aware in the cloud," *IEEE Transactions on Computers*, vol. 63, no. 12, pp. 3012-3025, 2014.

[8] V. Vinothina, R. Sridaran, and P. Ganapathi, "A survey on resource allocation strategies in cloud computing," *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 6, pp. 97-104, 2012.

[9] F. Sabahi, "Secure virtualization for cloud environment using hypervisor-based technology," *International Journal of Machine Learning and Computing*, vol. 2, no. 1, pp. 39-45, 2012.

[10] M. Maurer, D. Borgetto, G. Da-Costa, J.-M. Pierson, and I. Brandic, "Energy-efficient and SLA-aware management of IaaS clouds," in *2012 Third International Conference on Future Systems: Where Energy, Computing and Communication Meet (E-Energy),* IEEE, May 2012, pp. 1-10.

[11] M. Abdel-Azim, A. I. Abdel-Fatah, and M. Awad, "Performance analysis of artificial neural network intrusion detection systems," in 2009 *International Conference on Electrical and Electronics Engineering, ELECO 2009*, IEEE, 2009, pp. II-385.

[12] O. Linda, T. Vollmer, and M. Manic, "Neural network based intrusion detection system for critical infrastructures," in *2009 International Joint Conference on Neural Networks*, IEEE, 2009, pp. 1827-1834.

[13] H. Yu, and B. M. Wilamowski, "Efficient and reliable training of neural networks," in *2009 2nd Conference on Human System Interactions*, IEEE, May 2009, pp. 109-115.

[14] J. Pradeep, E. Srinivasan, and S. Himavathi, "Diagonal based feature extraction for handwritten character recognition system using neural network," in *2011 3rd International Conference on Electronics Computer Technology,* IEEE, 2011, vol. 4, pp. 364-368.

[15] P. J. Yang, and C. C. Fung, "Artificial intelligence in malware - Cop or culprit?," 2008.

[16] Weiwei, and Donghai, "Cascade disturbance rejection control of the uncertain nonlinear systems with nonlinear parameterization," in *2013 American Control Conference,* IEEE, 2013, pp. 265-271.