A SYSTEMATIC ANALYSIS ON WORM DETECTION IN CLOUD BASED SYSTEMS

Hasan Mahmoud Kanaker, Madihah Mohd Saudi and Mohd Fadzli Marhusin
Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Nilai, Malaysia
E-mail: hasankanaker@gmail.com

ABSTRACT

An innovative breakthrough in computer science is cloud computing and involves several computers which are connected via the Internet or it is dispersed over a network. A large database, services, applications, software and resources are an integral part of this technology. It has the capability to operate a program or applications on numerous connected computers simultaneously and permits the users to enter applications and resources through a web browser or web service via the Internet anytime and anywhere. Current susceptibility in elementary technologies gravitates to expose doors for intrusions. Cloud computing offers enormous advantages such as cost reduction, dynamic virtualized resources, significant data storage and enhanced productivity. At the same time, numerous risks occur regarding security and intrusions, for example, worm can intercept cloud computing services, impair service, application or virtual in the cloud formation. Worm attacks are now more complex and resourceful making intruders more difficult to detect than previously. The motivation of this research is founded on ramifications presented by the worms. This paper presents different intrusion detection systems affecting cloud resources and service. Moreover, this paper illustrates how genetic algorithm can be integrated in detecting worm attacks in cloud computing more efficiently.

Keywords: cloud computing, intrusions detection, worms, genetic algorithm.

1. INTRODUCTION

Using internet and remote server for keeping data and applications is new technology known as cloud computing. Furthermore, users can use applications or services on the clouds through web browsers or web services by utilizing the internet [1]. It offers enormous potential to enhance productivity, decrease costs, dynamic virtualized resources, and distribution of many economic advantages among its adapters [2].Cloud computing contributes the different types of services; Software as a Service SaaS (e.g. Google Apps) [3]. Platform as a Service PaaS (e.g. Microsoft's Azure) [4]. Infrastructure as Service IaaS (e.g. Amazon Web Service) [5].

It is remarkable that cloud computing and improves the validity of an organization and maintain competent management support with minimum resources [6]. The latest technology, known as cloud, altered peoples' lives and fortified their employable years via several cloud services. Individual lives are affected by this technology via operations and storage abilities. Currently, many organizations have recognized the emphasis of the cloud for its compliance, operational benefits, and substantial cost savings. For example, in 2010 UK government introduced the G-Cloud, government cloud infrastructure. Vindictive codes transfer from one infected machine to another vulnerable machine through a network without the owner's permission [7]. Owing to the nature of a centralized network, susceptible and personal information has become an objective for attack by malicious worm which is one of the most precarious roads for attacking a cloud host. Regarding an attack, the intruder attempts to corrupt a barbed service, application or virtual machine in cloud formation and exhibits itself as a genuine user and hatches its personal barbed service, application or virtual machine, and utilizes the malicious code into the cloud structure [8]. Moreover, depending on signature based antivirus it has ability to detect high accuracy when the signature has been known. The shortcoming of this type of detection is when the malware morphs its signature completely. Generally, this type of antivirus would fail to detect a novel attack.

Cloud computing experiences numerous traditional attacks such as denial of service (DoS) attack, authentication attack, cloud malware injection attack, IP spoofing and distributed denial of service (DDoS). Efficient intrusion detection systems (IDS) must be embedded in cloud framework to alleviate such intrusions.

The rest of this paper is organized in the following sections: Section 2 the cloud computing paradigm is introduced. Section 3 presents worm attacks definition. Section 4 detection methods in cloud computing and worm attacks in cloud are described. Section 5 discussed General methods to detection malware. Section 6 presents various techniques for intrusion detection system (IDS) in cloud computing, and finally Section 7 conclusion and future works are depicted.

2. CLOUD COMPUTING

Cloud computing refers to both applications delivered as services over the internet and the hardware and systems software in the datacenters that provide those services [9], they defined the services as software as a service (SaaS). The datacenter hardware and software is what has been determined as a cloud. The researchers also mentioned two categories of cloud; the first one being the public cloud which is available to the general public and the second one which is the private cloud that is only operable for a company. Figure-1 illustrates the roles of the users or service providers for the cloud computing. Software installation, applications, services, maintenance and centralized control over versioning into cloud are the responsibility of service providers. These applications or services on the clouds can be utilized through web-browsers and web services by using the internet.

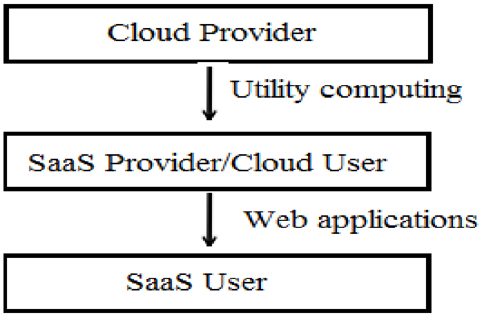

Figure-1. Users and suppliers of cloud, adapted from [9].

Cloud computing is defined as the hardware and software services fundamentally cached in web servers, and cloud connected on the internet [10]. A PC, PDA or some other device is necessary for the user to access services into cloud via a browser and an internet connection at any time anywhere. The users are supplied with the services and data they require by service providers. Management of video folders, web mail, photo and other services are supplied by cloud computing.

Cloud has been defined as a distributed computing paradigm [11] which is a dispersed computing model, steered by boundaries of scale consisting of virtuality, storage, platforms and services which are accessed and transferred on demand over the Internet to customers. Cloud architecture can be classified into four layers; applications, platform, unified resource and fabric [11]. The application layer consists of the applications which would operate in Cloud. The platform layer augments a collection of specially designed tools and services to a distribution platform as in the case of a web hosting domain. Unified layer consists of resources which have been remote or enveloped usually by virtualization such as a coherent filing system and database. Hardware resources such as storage, network and computing resources are contained in the fabric layer.

3. WORM ATTACKS DEFINITION

A worm is a pernicious code that can interfere with systems and applications and has the capability to morph their primary codes thereby causing those systems and applications to disintegrate and therefore cannot be employed for standard operation [12].

A worm has been defined as one of the most threatening types of malicious codes and encroaches enormous volumes of internet applications via software codes [13].

An intruder, during a cloud attack, will endeavor to implement into the cloud system and it requires the antagonist to form its own barbed service application (SaaS or PaaS) or VM to the cloud system and attempt to put himself as a cloud user. If successful, the cloud system will, as a matter of course, avert the legitimate users notic to the barbed service application plus the intruder’s code is accomplished [14].

In cloud computing [15] demonstrated an example on how a worm attack functions and ascertained its actions by adopting dynamic analysis. The outcome exhibited that the worm deleted a file in “C” directory, C:Windows\System32\Worm64.dll which was utilized by the worm to violate cloud server thereby destroying files, registry and data saved in the server.

4. WORM ATTACKS AND DETECTION METHODS IN CLOUD COMPUTING

Internet and remote servers are utilized for preserving data and application via cloud computing. Users are able to use services applications through cloud [16]. Unfortunately, cloud computing is at risk from openness including attacks from invaders. Security threats and worm injection attacks are serious issues of cloud computing [2, 17].

Worm attacks in the cloud are where the worm intrudes and becomes an authentic service operation thereby making cloud services unethical [17]. Worm attacks are complex can alter data significantly or results in a gridlock and compels the user to wait until the attacks are concluded. The worm operates in the cloud computing operations and obtains rights and concessions to control all cloud surroundings. Some solutions were contemplated to address this issue. Firstly, when a user accesses an account in cloud, the cloud supplier immediately forms user’s image in a Virtual Machine (VM) in the image archive system of cloud. Secondly, it was proposed that a higher level of integrity be introduced because it is extremely challenging for an intruder to enter in the Iaas level. It was also advocated using File Allocation Table technique (FAT).

[17] proposed a higher mandate of security in the hardware level, because it is significantly onerous for an attacker to enter the IaaS level and challenging for an intruder to infringe in the IaaS level. This technique monitors what about the applications that the user is going to operate. It can also be verified that it has been utilized and executed previously from the user’s machine to determine validity and integrity. Also, they use hypervisor method for scheduling all instances but prior to that the provider authenticates the integrity of the instance from the FAT Table of the user’s VM. The other direction is to store the OS type of the user when they open an account. Before launching an instance in a cloud it surveys the OS type from which the instance was requested based on the OS type of the user. For the cloud provider these solutions require a lengthy period of time to process.

During a worm injection attack an attacker will attempt to develop a personal vindictive service [2] into the cloud structure to contaminate service, VM or application. The user will then request the vindictive service, thinking that it is a legal service, and the malicious code will be inserted into the system. Normally, the attacker uploads a virus programme and disperses it on cloud structure. When users use the vindictive service, the cloud bombards the virus over the internet to the client, thereby infecting the client's machine. [2] advocated a counter-measure to remedy this problem such as ascertaining the authenticity for receiving messages and storing the original image request and comparing it with the hash value by using the hash function. This solution is not foolproof because the attacker can form a genuine hash value to handle cloud system and for this reason they were unable to adequately detect worm and avoid the attack in cloud computing environment.

A new retrospective detection approach was proposed based on Portable Executable (PE) format file relationships [18]. Using a Hadoop platform a system was implemented including map reducing jobs for distributed computing and data storage, three computers and used 18 worms. Retrospective detection was used and permits the identification of worms from aged information when host or users enter related files. When a threat is diagnosed it then forms PE logs format files in each computer where the logs hold information about all new PE files. Should any modifications be detected in PE it is then effortless to capture worm to retrospective detection of worm attacks. The log compiles a logging programme which collects file information and later the logs will be commissioned to the cloud server where file indexing processes each log and relation indexing and map reduction. The file indexing details what PE file are in existence and in which computer. The relation indexing shows which computer holds a definitive liaison with PE files. In map reduction, the file indexing and relation indexing form one index to retrospective method of detecting worm attacks by cloud computing. This system produces an increased disclosure rate (94%) together with a decreased false positive rate as compared to previous studies.

Table-1. The challenges of different worm detection methods.

Title	Method used for worm detection	Challenges for improvement
Cloud Computing: Network/Security Threats and Countermeasures [2]	-Check the authenticity for received messages. -Store the original image file using hash function.	-Attacker can create alegitimate hash value to deal with cloud system.
Security attacks and solutions in clouds [17]	-Using File Allocation Table technique (FAT). -Utilize the Hyper visor method. -Storing the OS type of the user.	-Process time for the cloud provider is very high.
Retrospective detection of malware attacks by cloud computing [18]	-Portable Executable (PE) format file relationships. -May reduce job. -Hadoop platform. -File indexing. -File-relation index.	-These methods are only effective on Hadoop platform. -Some worms can generate different log file each time so cannot be detected easily. -Process time is high due to a large number of files. -Detection method based on behavior only.

5. METHODS TO DETECTION MALWARE

5.1 Signature based detection

Signature based detection method involves using patterns extricated from numerous malwares to authenticate them. A signature like a fingerprint is a unique characteristic for individual files but the drawback with this method is that significant manpower and time is required to extract unique signatures. It is insufficient to use this method solely for the detection of malware. It would be an obstacle to encounter malwares which mutate their codes in individual infections such as polymorphic and metamorphic [19].

According to [20], they suggested a detection system to expose intruders and attacks in a cloud computing environment based on the signature method. This system investigates network traffic and checks for sceptical activity. It has the ability to take steps against barbed traffic such as, impeding the user IP address from entering the network. By utilizing the intrusion detection system, it exposes unknown signatures founded on seeking for definitive signatures of known threats. A signature based intrusion detection system monitors packets on the network and compares them with a database of signatures from acknowledged malicious threats. They deploy intrusion detection system sensors for cloud users who require an intrusion detection system to expose attacks on their services and to be aware if the used services or hosts are attacking other victims. The cloud provider can use VMM functions to monitor virtual machines.

[21] conferred an anti-malware system called Split Screen which is based on signature-based parameters. This system executes an extra screening stage prior to the signature matching in their system. Screening steps are used to filter non-infected files and identify malware signatures that are not of interest. The files can then be scanned using only the necessary signatures. Split Screen was implemented as an extension of ClamAV and was proven that scanning throughput is improved using signature sets using half the memory.

[22] presented a model to detect malware on cloud computing integrating intrusion ontology representation using signature methods. This model uses multiple engine services which follows a set of defined parameters and standards for web service technologies. This model is founded on analysis with specific applications residing on the client. It can enhance their performance if they are moved to the network, where instead of running complicated software on every host, it gives each process a light to enter the system files. Then it sends them to the network to be analyzed by multiple engines and then to decide whether or not they are executed according to the report of threat delivered. This model is a multi-engine based file analysis service deployed in cloud computing, via a group of protocols and standards for web services. It is used to identify the files with malicious codes through the remote analysis by multiple engines. The result offers the contingency of expanding the rate of the assertion characterization of harmful files.

An efficient solution for detecting known or variations of attack is signature based detection but is unable to detect unknown attacks or variation of known attacks.

- **Behavior based detection**

Behavior based malware detection technique scrutinizes programme behavior to decide whether it is corrupt. It has the ability to expose various types of malware based on signature techniques but this method is very difficult to detect thereby possibly causing a false alarm as the technique observes what an executable file does. Various samples of malware can be identified by a single behavior.

[23] proposed a novel approach to monitor the execution status of user application programs and detects auspicious processes in cloud servers using behavioral method. They combined the hypervisor to monitor all OS level system calls in all VMs in cloud computing environment. Two phases were used in this approach, which is the learning stage and the detection stage to search for the malware in the cloud. During the training phase, they intercepted and analyzed a stream of system calls for a sufficient time period to cover the majority of normal system operations. While in detection phase, they observed the stream of system calls and detected any deviation from the previously defined model of normal behavior. Malware performs benign functionalities inconsistent with normal behavior, which is instrumental for attack detection. The detection of the suspicious processes in cloud by monitoring system calls of processes running in each virtual machine. The proposed behavioral modeling scheme aims at addressing the software-oriented threats in categories.

[24] proposed a flexible and automated approach to extract malware behaviour by observing all the system function calls performed in a virtualized execution environment. Similarities and distances between malware behaviors are computed which allows classifying malware behaviors. The main features of this approach reside in coupling a sequence alignment method to compute similarities and leverage the Hellinger distance to compute associated distances. The classification process proposed by this work is using a phylogenetic tree. However, this technique has a limitation due to the wrongly classified malware behavior.

A framework was implemented for improving behavior based analysis of malware [25]. The framework only improves the capabilities of existing dynamic behavior based detectors such as TTAnalyze, Panorama and CWSandbox and is not the malware detector. The framework was founded on cloud computing environment by examining a piece of malware on behalf of multiple end users in concert.

Cloud can detect anonymous attacks at different strata by behavior detection techniques. In cloud, huge numbers of incidents like (system level or network level) develop making it arduous to observe or domination them using behavior detection technique.

There are numerous techniques utilized to enhance detection precision and efficiency of signature based detection and behavior based detection, such as Genetic Algorithm (GA), Artificial Neural Network (ANN), Fuzzy Logic, etc.

6. INTRUSION DETECTION SYSTEM (IDS) IN CLOUD COMPUTING

6.1 Genetic algorithm (GA) based IDS

Genetic algorithms (GAs) [26] are used to choose network features or to decide optimal parameters which can be used in other mechanisms to generate useful solutions to optimization and improve accuracy of IDS.

[27] presented Genetic Programming (GP) for detecting novel attacks on networks and four genetic operators; namely reproduction, mutation, crossover, and dropping condition and are used to evolve new rules from network features. However, these new rules take more time to generate.

[26] proposed a method to detect misuse and anomaly by combining fuzzy and genetic algorithms.

Fuzzy is used to include quantitative parameters in intrusion detection, whereas genetic algorithm is used to find best fit parameters of introduced numerical fuzzy function.

Information theory and GA based approach is used to detect abnormal behavior [28]. It determines a small number of network features closely linked with network attacks based on mutual information between network features and type of intrusion. However, this approach only considers discrete features.

Genetic algorithm is a family of computational models based on principles of evolution and natural selection, and is primarily used for finding optimal solutions to a specific problem [29]. According to [30] the process of a genetic algorithm starts with a randomly generated population, evolves through selection, recombination (crossover), mutation. Finally, the best individual (chromosome) is selected as the final result once the optimization criterion is met. Figure-2 shows the structure of a simple genetic algorithm.

In a cloud computing environment, a selection of optimization parameters (network features) will increase the precision of underlying IDS for intrusion detection. For that reason, Genetic Algorithm (GA) based IDS can be used in Cloud.

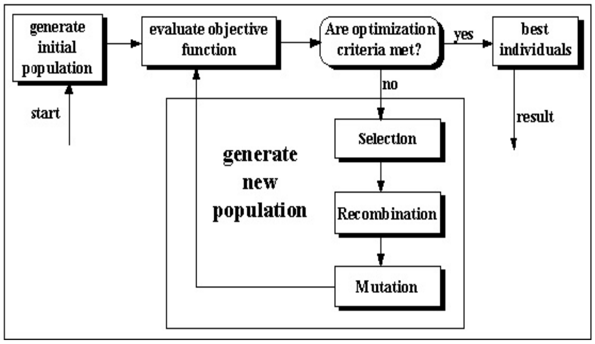

Figure-2. Structure of a simple genetic algorithm [30].

[31] has defined genetic algorithm as a programming mechanism, which mimics biological development as a problem solving approach.

The genetic algorithms which advocates the survival of the fittest among a population. Therefore, a solution obtained by applying genetic algorithms to any problem, consists of only those optimal candidate solutions which are said to satisfy a predefined fitness value [32, 33].

Based on previous work of genetic algorithms, the researchers' contribution in this paper will be use genetic algorithms to develop a model that effectively detects worm attacks and avoids worms from further propagation in cloud computing environment. Moreover, this research also aims to identify and evaluate various strategies of worm attacks, which vital prior designing and developing a robust model to track the worm attacks.

Genetic Algorithms will be utilized to research the most advantageous solution to detect worm attack in cloud computing more efficiently because GAs are easy to modify, provide a wider solution space, possess tremendous capabilities for parallel processing, easily discoverable global minima, do not need prior knowledge of the problem space, least affected by the discontinuities in the problem space and reliable enough not to become trapped in local minima.

The implementation of genetic algorithms offers many advantages to intrusion detection systems which are:

- Genetic algorithms work with populations of solutions rather than a single solution. This makes them suitable for behavior based intrusion detection, where the behavior attributes may exhibit varying values.
- Genetic algorithms are capable of working in multiple directions simultaneously. This makes them beneficial for analyzing the huge volumes of multi-dimensional data to be processed by an intrusion detection system.
- Genetic algorithms are highly re trainable. Therefore, using genetic algorithms for intrusion detection will add to the adaptability of the system.

6.2 Artificial neural network (ANN) based IDS

Role of ANNs [34] for intrusion detection is to be capable of generalizing information from incomplete information and to be able to distribute information as being normal or intrusive. Types of ANN used in IDS are as follows [35]: Multi Layer Perceptron (MLP), Multi Layer Feed Forward (MLFF) Neural Nets (NN) and Back Propagation (BP).

MLP based IDS were presented by [36], they showed that inclusion of more invisible layers increase the detection precision of IDS.

For misuse detection in network [37] suggested a three layer neural network. The feature vector used in [37] was composed of nine network features (Protocol ID, Source Port, Destination Port, Source IP Address, Destination IP Address, ICMP Type, ICMP Code, Raw Data Length, Raw Data). However, the intrusion detection precision is significantly low.

An efficient and effective solution of unstructured network data is ANN based IDS. The intrusion detection precision of this approach is based on number of invisible layers and training stage of ANN. Needs more training and more time for effective learning of ANN. Only use ANN based IDS cannot be an effective solution to detect intrusions for cloud as it requires a fast intrusion detection technique.

[38] proposed approach for cloud environment using ANN based anomaly detection technique, which demands more training samples as well as more extra time for detecting intrusions effectively.

6.3 Fuzzy logic based IDS

Fuzzy logic [34] can be used to handle inaccurate description of intrusions. It supplies some elasticity to the uncertain problem of intrusion detection.

Fuzzy association rules presented in [39] are utilized to detect network intrusion in real time. There are two rule groups produced which are mined online from training data. Features for comparison are taken from network packet header. This approach is used for large scale attacks such as DoS/DDoS.

[40] proposed Fuzzy IDS (FIDS) for network intrusions like SYN and UDP floods, Ping of Death, E-mail Bomb, FTP/Telnet password guessing and port scanning. Evolving fuzzy neural network.

(EFuNN) is introduced in [41] for reducing training time of ANN. It uses mixture of supervised and unsupervised learning. The experimental results shown indicate that using reduced number of inputs EFuNN has better classification accuracy for IDS than only using ANN. The approaches [41], [41] cannot be used in real time for detecting network intrusions as the training time is significant.

To reduce training time of [38], fuzzy logic with ANN can be used for fast detection of unknown attacks in Cloud.

6.4 Host based intrusion detection systems (HIDS)

A host-based intrusion detection system (HIDS) is an intrusion detection system which observes and analyses the information collected from a specific host machine, the information such as network events, system calls and file system. HIDS has the ability to observe any alteration occurring in this information and gives the reports existence of attack [42].

With cloud computing, HIDS can be running in VM or hypervisor and host machine to detect intrusive behavior through monitoring and analyzing log file, user login information, security access and control policies. In case of installing HDIS on VM it should be monitored by Cloud user whereas installing HDIS on Hypervisor, Cloud provider should monitor it [26].

[38] Proposed HIDS based architecture for Cloud computing environment. In this architecture, each node of cloud contains IDS which provides interaction among service offered, IDS service and storage service. The event auditor takes data from different resources like system logs. Based on the data received from event auditor, the IDS service is used for detecting intrusion by using knowledge based technique or behaviour based technique. Behaviour based technique is used to detect unknown attacks whereas the knowledge based technique is used to detect known attacks. The limitation of this approach is that it cannot detect any insider intrusions which are running on VMs.

- **Hypervisor based intrusion detection systems**

Hypervisor based intrusion detection system (HPIDS) is fundamentally an intrusion detection system designed for hypervisors and is a forum to operate VMs. HIDS permits users to monitor and evaluate communications between hypervisor and VM, between VMs and within the confines of the hypervisor based virtual network [42]. One of the paradigms of hypervisor based intrusion detection system is VM introspection based IDS [43].

A pool of virtualized computer resources and to manage various VMs and hypervisors is defined as cloud computing. Hypervisor based IDS in cloud computing is one of the significant methods to detect intrusion in a virtual environment [42]. The hurdles of this method are lack of experience by users.

[43] proposed virtual machine introspection based IDS (VMI IDS) architecture which realize hardware cases, events and software states of host. The responsibility of VM is hardware virtualization and also shows observation and interposition properties . VM interface is used for VMI IDS to connect with VMM; VMI IDS to take VM state information, observation specific events and controlling VMs. Summary of various Intrusion Detection Systems (IDS) are shown in Table-3.

Table-2. Summary of IDS techniques.

IDS Technique	Features	Challenges
Signature detection	**-A unique feature for each file. -An efficient solution for detecting known -Attacks.**	**-Required high amount of manpower and time to extract unique signatures. -By using this method alone in detecting Malware is insufficient. - Unable to detect unknown attacks**
Behavior detection	- It has the capability to detect different type of Malwares.	- It is very hard to detect Malware may cause false alarm
Genetic Algorithm based IDS	- Used to choose better features for detection. -Has best efficiency.	-Used in a particular mode rather than general.
Artificial Neural Network based IDS	-Multiple invisible layers in ANN increase performance of classification. -Classifies unstructured network packet efficiently.	- Huge number of samples needed for training effectively. - Has minimum elasticity. - It needs more of time at training stage.
Fuzzy Logic based IDS	- supply best elasticity to some uncertain Problems. - Used for quantitative features.	-Precision detection is lower than ANN.
HIDS	- determine intrusions by observation host's file system, system calls or network - No further hardware needed events.	- It can observe attacks only on host where it is deployed. - Need to install on each machine such as host machine, hypervisor or VM.
Hypervisor based IDS	- It allows user to observe and analyze connections between hypervisor, VM, between VMs and within the hypervisor based virtual network.	-Shortage of experience. - New and difficult to understand.

7. CONCLUSIONS

Cloud computing is a fast emerging technology globally and offers many advantages such as decreased costs, dynamic virtualized resources, massive data storage and enhanced productivity. At the same time, cloud computing has various security risks and threats. Worm attacks in cloud are a developing threat and seen as one of the primary threats in cyber world. It is one of the most dangerous types of vindictive codes that can encroach into cloud formation and attempt to destroy a malicious service, application or VM. Research anticipates a contemporary method to detect worm attacks in cloud computing by using genetic algorithm which is ultimately more productive. For future work, genetic algorithm will be integrated to detect worms attack more efficiently in cloud computing environment.

ACKNOWLEDGEMENTS

The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) and Institut Sains Islam (ISI), USIM for the support and facilities provided. This research paper is supported by Universiti Sains Islam Malaysia (USIM) grant [PPP/FST/SKTS/30/12712] and [PPP/FST/SKTS/30/12812].

REFERENCES

[1] Jamil D. and Zaki H. 2011. Security Issues In Cloud Computing. 3(4): 2672-2676.

[2] Qaisar S. and Khawaja K. 2012. Cloud Computing: Network/Security Threats and Countermeasures, Interdisciplinary Journal of Contemporary Research In. pp. 1323-1329.

[3] Google apps. [Online]. Available: http://www.google.com/apps/business.

[4] Azure services platform. [Online]. Available: http://www.microsoft.com/azure.

[5] Amazon web services. [Online]. Available: http://aws.amazon.com.

[6] Mell P. and Grance T. 2011. The NIST Definition of Cloud Computing (Draft), Recommendations of the National Institute of Standards and Technology. p. 145.

[7] Saudi M. 2011. A New Model for Worm Detection and Response (PHD thesis), University of Bradford, United Kingdom.

[8] Biedermann S. and Katzenbeisser S. 2011. Detecting computer Worms In the cloud. In: Proceedings of the IFIPWG 11.4 International conference on Open Problems in Network Security. pp. 43-54.

[9] Armbrust M., Fox A., Griffith R., Joseph A., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I. and Zaharia M. 2010. A view of cloud computing. Commun. ACM 53 (4) (April 2010): 50-58.

[10] Aymerich F.M., Fenu G., Surcis S. 2008. An approach to a Cloud Computing network. Applications of Digital Information and Web Technologies, 2008. ICADIWT 2008. First International Conference on the. pp. 113, 118.

[11] Foster I., Zhao Y., Raicu I and Lu S. 2008. Cloud Computing and Grid Computing 360-Degree Compared. Grid Computing Environments Workshop, 2008. GCE '08. pp. 1, 10.

[12] Mcgraw G. and Software R. 2000. Attacking Malicious Code.

[13] Marhusin M. 2012. Improving the Effectiveness of Behaviour-based Malware Detection.

[14] Jensen M., Schwenk, Gruschka N. and Iacono L. 2009. On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing.

[15] Kanaker H., Saudi M. and Marhusin M. 2014, August. Detecting Worm Attacks in Cloud Computing Environment: Proof of Concept. In Control and System Graduate Research Colloquium (ICSGRC), IEEE 5th. pp. 253-256.

[16] Ren K. and Lou W. 2009. Ensuring Data Storage Security in Cloud Computing. Retrieved From http://www.ece.iit.edu/~ubisec/IWQoS09.pdf.

[17] Zunnurhain K. and Vrbsky S. 2010. Security Attacks and Solutions in Clouds.

[18] Liu T. and Chen Y. 2010. Retrospective Detection of Malware Attacks by Cloud Computing. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. pp. 510-517.

[19] Gutmann P. 2014. The Commercial Malware Industry Some History.

[20] Dhage S. and Meshram B. 2012. Intrusion detection system in cloud computing environment. Int. J. Cloud Computing. 1(2/3).

[21] Truelove J. and Brumley D. 2010. Split Screen: Enabling Efficient, Distributed Malware Detection.

[22] Martinez C., Echeverri G. and Sanz A. 2010. Malware Detection based on Cloud Computing integrating Intrusion Ontology representation.

[23] Dolgikh A., Birnbaum Z., Chen Y and Skormin V. 2013. Behavioral Modeling for Suspicious Process Detection in Cloud Computing Environments. pp. 177-181.

[24] Wagener G., State R. and Dulaunoy A. 2008. Malware behaviour analysis. Vol. 4.

[25] Martignoni L., Paleari R. and Bruschi D. 2009. A framework for behavior-based malware analysis in the cloud. pp. 1-15.

[26] Dhanalakshmi Y. and Ramesh Babu I. 2008. Intrusion Detection Using Data Mining Along Fuzzy Logic and Genetic Algorithms. 8(2): 27-32.

[27] Lu W. and Traore I. 2004. Detecting new forms of network intrusion using genetic programming. Computational Intelligence. 20(3): 475-494.

[28] Xiao T., Qu G., Hariri S. and Yousif M. 2005. An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm. Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC ‘05), Phoenix, AZ, USA

[29] Li W. 2004. Using genetic algorithm for network intrusion detection. Proceedings of the United States Department of Energy Cyber Security Group pp. 1-8.

[30] Pohlheim H. 2003. Genetic and Evolutionary Algorithms: Principles, Methods and Algorithms.

[31] Bobor V. 2006. Efficient Intrusion Detection System Architecture Based on Neural Networks and Genetic Algorithms. Department of Computer and Systems Sciences.

[32] EidHebba F., Darwish A., Hassanien A. and Tai-Hoon K. 2011. Intelligent Hybrid Anomaly Network Intrusion Detection System. In: CCIS 265. vol. Part I, pp. 209-218.

[33] Srinivasa K. 2012. Application of Genetic Algorithms for Detecting Anomaly in Network Intrusion Detection Systems. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunication Engineering. 84: 582-591.

[34] Han J. and Kamber M. 2006. Data Mining Concepts and Techniques 2nd edition. Morgan Kaufmann Publishers.

[35] Ibrahim L. 2010. Anomaly Network Intrusion Detection System Based On Distributed Time-Delay Neural Network. Journal of Engineering Science and Technology. 5(4): 457-471.

[36] Moradi M. and Zulkernine M. 2004. A Neural Network Based System for Intrusion Detection and Classification of Attacks. Proceedings of the 2004 IEEE International Conference on Advances in Intelligent Systems Theory and Applications.

[37] Cannady J. 2010. Artificial Neural Networks for Misuse Detection. National Information Systems Security Conference.

[38] Vieira C. and Schulter A. 2010. Intrusion detection techniques in grid and cloud computing environment. IEEE IT Professional Magazine.

[39] Su M., Yu G. and Lin C. 2009. A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach. Computer Security. pp. 301-309.

[40] Tillapart P., Thumthawatworn T. and Santiprabhob P. 2002. Fuzzy intrusion detection system, Assump University J. Technology (A.U. J.T.). 6(2): 109-114.

[41] Chavan S., Shah K., Dave N. and Mukherjee S. 2004. Adaptive neuro-fuzzy intrusion detection systems. IEEE international conference on information technology: coding and computing (ITCC’04). pp. 70-74.

[42] Modi C., Patel D., Patel H., Borisaniya B., Patel A. and Rajarajan M. 2013. A survey of intrusion detection techniques in Cloud. Vol. 36.

[43] Garfinkel T. and Rosenblum M. 2003. A Virtual Machine Introspection Based Architecture for Intrusion Detection. In: Proc. Network and Distributed Systems Security Symposium. pp. 191-206.