Texila International Journal of Academic Research
Special Edition Dec 2019

Artificial Intelligence (AI) Driven Solutions for Security Issues in OpenStack

Article by Mohammad Shawkat Akbar Almamun[1], Balamurugan E[2],Sangeetha K[3], Md. Shahidul Hasan[4]
[1]*Research Scholar, Texila American University,*
[2-3]*University of Africa, Nigeria,*
[4]*Research Scholar, Texila American University*
E-mail: liks18@gmail.com[1], rethinbs@gmail.com[2-3], hasan_1027@yahoo.ca[4]

Abstract

Cloud computing is one of the most substantial and fastest growing field today whereas cloud service providers offer resources as virtual machines, raw (block) storage, firewalls, load balancers, and network devices. One of the most vital issues in cloud computing is security. AI is a combination of multiple technologies such as machine learning, Artificial Neural Networks and Deep Learning and its widely accepted by technologist and global IT giants. There were few AI driven security solutions have already found in traditional applications in next generation such as firewalls, automatic intrusion detection systems, encrypted traffic identification, malware detection, and so on, therefore it would also be very suitable and supportive for ensuring security on Cloud based computation. This paper focuses on some of the important aspect and possibility of AI driven security approaches for OpenStack cloud. It brings out an exhaustive survey of such techniques, and also put forth the open challenges for further research. The paper is organized as follows as Introduction to Artificial Intelligence, Cloud Computing, Review of Literature, Security Issues in OpenStack and Conclusion.

Keywords*: Artificial Intelligence, Cloud Computing, OpenStack, Security*

Introduction

An increasing number of businesses are preferring cloud services for flexibility, efficiency, cost-effectiveness and strategic values. All types of organization and all sizes of customers from simple to enterprises are enjoying its great advantages. Cloud computing can be classified based on the services

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

IaaS refers to a combination of hosting, hardware provisioning and basic services needed to run a cloud. PaaS refers to the provision of a computing platform and the provision and deployment of the associated set of software applications (called a solution stack) to an enterprise by a cloud provider. Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network. Cloud computing is a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources such as network, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort Through cloud computing organizers are now able to extract business value by getting meaningful information. Moreover, test and development environment are one of the best usages of the cloud. With cloud computing, there are readily available environments that suit the needs. Another great advantage of using cloud is backing up data. While traditional backup systems can be a very complex and time-consuming operation, Cloud-based backup, on the other hand, can move data without worrying about security and availability issues to any location. Besides all these benefits, as it is evolving, few cloud service providers are providing services with unique nature of architectural infrastructure. Because it is comparatively new, it has several fundamental challenges that must be addressed and overcome to boost for adoption.

DOI: 10.21522/TIJAR.2014.SE.19.02.Art011
ISSN: 2520-3088

One of them is OpenStack cloud security issue It is a great challenge because of the fact that a company might have share all its sensitive information to a third-party cloud computing service provider and there is a chance that hackers might have access to this information. Therefore, the intention of this paper is to mitigate the security threat in cloud computing

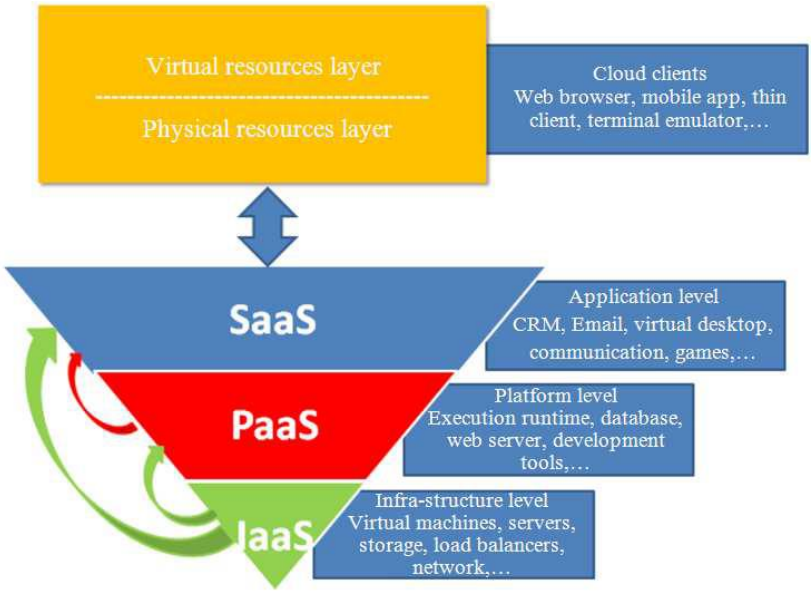

Figure 1. Cloud computing architecture

Literature review

Cloud computing

Cloud computing means, storing and accessing data and programs over the Internet instead of local computer's or servers hard drive kept in residence. Users can access all of the features and files of the system without having that system on their own computers. As Cloud services support people to consume the cloud resources on usage basis, therefore cloud computing ensures utmost use of resources. The use of Cloud services is increasing so rapidly that not only people are using this infrastructure for personal use but also businesses are increasingly using it to be able to access large amounts of data over a secure, online network connection.

Artificial neural network

Artificial Neural Network is the most considered technology in the last two decades that is used in various engineering applications because through its basic function it has the mimicking ability of human mind and effectively employs modes of reasoning and/or pattern recognition

Learning theory

Computational learning theory is the investigation of theoretical aspects of machine learning of what can and what cannot be learned from data. It is a multidisciplinary area which is brought together the techniques and approaches of computer science, statistics and applied mathematics. Learning theory leads to model selection methods by which we can choose automatically what model would be appropriate for a certain training set.

Training

The network is ready to be trained when the data set is ready. To achieve the learning process two approaches can be used: supervised or adaptive training. In supervised training, to monitor how well an artificial neural network is converging on the ability to predict the right answer both inputs and outputs are provided. For adaptive training, only the inputs are provided.

The neural networks benefit from continuous learning in order to face new situations and environments using self-organization mechanisms (SOM

Security Issues in OpenStack Cloud

OpenStack is an open source cloud-based operating system platform for public and private clouds that manages huge pools of compute, storage, and networking resources across a datacenter. Administrative controls are done through a dashboard while a web interface is used to support users in the provision of resources. RackSpace and NASA jointly started this project in 2010. Practically, modification of source code and sharing those modifications with the community is the key benefits of this model as the source code can then be checked by many people compared to proprietary code, which is restricted to its owners.

OpenStack is made up with lots of different moving parts. Everyone can add additional components to OpenStack to help as well as to meet their needs just because of its open nature. But we found that OpenStack society has jointly identified nine key mechanisms that are a part of the "core" of OpenStack, which are spread as a part of any OpenStack system and also officially preserved by the OpenStack community. In order to make a thorough analysis of the OpenStack software from a security viewpoint, first and foremost, we need to identify security-related issues that should be taken care of when using cloud computing solutions.

We have found several flaws in OpenStack; these threats may be addressed in the current releases of OpenStack (Slipetskyy, 2011; Cigoj and Klobucar, 2012)

1. Users cannot reset their passwords on horizon; regular users can only have their passwords reset by the administrator within the horizon interface. We do not currently know how this flaw will impact
2. The administrator of a project on horizon is automatically made the administrator of the whole system. OpenStack utilizes the concept of projects and tenants to group people into logical units for cloud computing. However, the administrator of a single project is granted managerial rights to all projects, not merely the project at hand, by the interface. The administrator's privileges, including the creation of new users and projects, have the potential to change other projects, remove items
3. Cleartext is used in the network API. OpenStack api endpoints encourage the use of cleartext and no SSL/TLS support is available right now. This allows for easy man-in-the-middle attacks and even "sniffing" passwords over the wire can be trivial
4. No authentication in the client-server system. It appears that any host with access to the db and to the AMQP system can act as a compute node and launch VMs
5. Usernames and passwords. Passwords and usernames that are used for accessing images will be stored in Cleartext in the db and in external storage. When glance stores images on swift, for example, the username and password of the swift account will be stored as Cleartext in the db together with the URL of the swift object. This could potentially allow the information of any swift user to be accessed and read from the db. This storage of information is unnecessary because the username and password are already stored in the glance configuration file

AI for traditional cyber security

We need AI in the cases where human expertise is absent and humans are unable to explain their expertise. Moreover, AI help to give better solution where solution changes with time and solution needs to be adapted to particular cases. Furthermore, AI is needed where Problem size is too vast for our limited capabilities. Analyzing these basic criteria, the following area of security can be beneficial by utilizing AI properly.

Threat detection.

Traditional security measures depend on specific firewall and antivirus software for detecting and preventing web-based security threats. As these software needs timely updating therefore the level of security of website depends on the security personnel's attitude. On the other side, algorithm-based AI can be used to detect threats and other potentially malicious activities timely fashioned. Moreover, where conventional systems simply cannot keep up with the sheer number of malware that is created every month, AI based security system can successfully step in and address this problem by using complex algorithms.

DOI: 10.21522/TIJAR.2014.SE.19.02.Art011
ISSN: 2520-3088

AI can recognize these patterns through supervised and unsupervised training and hence identify even the smallest behaviors of ransomware and malware attacks before it enters the system and then isolate them from that system. Using predictive functions AI supported security system surpass the speed of success of traditional approaches.

Authentication

To provide user access of multi-factor authentication AI system also can be used. A Company might have different levels of authentication privileges for different users and these privileges might differ for different location where they are accessing the data. Managing these types of Authentication would be a nightmare if the organization has many users. On that scenario when AI is used, the authentication framework can be a lot more dynamic and real-time. It collects user information to understand the behavior of this person and make a determination about the user's access privileges and then it can modify access privileges based on the network and location of the user.

Minimizing human involvement

Typically, security personals are assigned to keep vigilant of a website or a connected group. Because it is difficult for cybersecurity expert to work for hours without break or holidays therefore there is scope of security breach within these breaks. Within this scenario, AI supported system can deal better with high risk task without ant concern because it does not require any break. So, it is evident that AI makes human life easier to an extent.

AI with open stack security

It is a fact that with the rapid growing of public cloud utilization, potential risk of security breaches of sensitive stuff, especially data is also growing. In contrast with many thinking, the main responsibility for protecting corporate data in the cloud lies not with the service provider but with the cloud customer. The technology is passing security transition period. And therefore, the focus of responsibility is shifting from the provider to the customer. Enterprises are spending huge amounts of time and money for figuring out if any particular cloud service provider is 'secure' or not and eventually it is not paying back virtually. Artificial Intelligence be helpful in this dilemma as it can provide organizations with an up-to-date understanding of cloud security concerns such as threat detection, authentication and minimizing human involvement. By doing so users of OpenStack cloud can make educated decisions regarding cloud adoption strategies.

Conclusion

Though cloud computing is a good solution for many businesses as it enables global access to mutual pool of resources, it has numerous challenges in security issues which should be addressed properly. OpenStack environment has Disparate Structures and Folders and it is Dynamic Environment in nature. Therefore, with traditional services OpenStack environment requires extensive human intervention. An AI-powered monitoring would actively monitor all of the components OpenStack deployment and IT operation team can get instant deep-level visibility into security services. As a result, the security of OpenStack in real time increases significantly. This Initial finding that AI based security model is best suited for OpenStack Cloud Computing is based on mainly literature reading and relative comparisons of the results in different research papers. Further research can be helpful to support this claim

References

[1]. Ishan Gidwani, Dasrath Mane, 2015, Security Issues in OpenStack, International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 2, pp: 1147-1158.

[2]. Hala Albaroodi, Selvakumar Manickam and Parminder Singh, 2014, Critical Review of OpenStack Security: Issues and Weakness, Journal of Computer Science 10 (1): 23-33.

[3]. Sunil Kumar S, Manvi A, Gopal Krishna Shyamb., 2014, Resource management for Infrastructure as a Service (IaaS) in Cloud Computing: A survey. Journal of Network and Computer Applications 41(2014) 424–440.

[4]. Rakesh Kumar, Neha Gupta, Shilpi Charu, Kanishk Jain, Sunil Kumar Jangir, 2014, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, pg. 89-98.

[5]. Pieter-Jan Maenhaut, Hendrik Moens, Bruno Volckaert, Veerle Ongenae and Filip De Turck, 2017, Resource Allocation in the Cloud: From Simulation to Experimental Validation, proceedings of IEEE 10th International Conference on Cloud Computing.
[6]. Dr. Balamurugan E, Sathish Kumar K, Dr. Sangeetha, 2018, A Survey on Software as a Service (SaaS) Cloud for High Level Language Computing. International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC). January 28 & 29, 2018.
[7]. S. Russell and P. Norvig, 2015. Artificial Intelligence: A Modern Approach, Prentice Hall, New York.
[8]. B. Jennings and R. Stadler, Resource management in clouds: Survey and research challenges,2015 Journal of Network and Systems Management, vol. 23, no. 3, pp. 567 – 619, 2015.
[9]. Richars Layne, 2019. Artificial Intelligence and Cloud Computing, The Future of Scientific Research, https://www.tessella.com.
[10]. https://docs.openstack.org/ceilometer/latest/install/get_started.html.
[11]. https://thenewstack.io/how-openstack-provides-scalable-reusable-infrastructure-for-ai-ml-workloads/.
[12]. https://wiki.openstack.org/wiki/Gyan/TFiO.