STUDY ON SECURITY CAPABILITIES IN CLOUD COMPUTING ENVIORNMENT

Shobha Elizabeth Rajan, Sreedevi P. , Ameena Beevi A.
Dept. of Computer Science & Engg., MG University, India
shobharajan90@gmail.com

Abstract - A move to use cloud computing, requires customer to have a clear understanding of potential security benefits and risks associated with cloud computing, and set realistic expectations with their cloud provider. Consideration must be given to the different models of service delivery: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a (SaaS) as each model brings Service different security requirements and responsibilities. The paper tries to study on the security features and capabilities currently prevailing in cloud computing field and the security provider by cloud service providers. Also the paper ties to review on the existing attempts to overcome the security pitfalls.

Keywords — Cloud service providers, Security, Artificial intelligence, Intrusion detection.

INTRODUCTION

Cloud computing security or cloud security is an growing sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). [13] There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The responsibility goes both ways, however: the cloud service provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures. When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report [12], insider attacks are the third biggest threat in cloud computing. [14] Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity. In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. The result would be a chance that one user's private data can be viewed by other users. To manage such conditions the cloud service providers should provide with logical storage segregation and data isolation[13]. The immense use of virtualization in cloud infrastructure brings security concerns for customers or tenants of a public cloud service. [15] Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist[16].

Since the era pushes for the growth of the data, the need for the storage space and the security issues with the storage spaces is of great importance. The extend of security features provided to the systems so far and the extend to upgrade the cloud system with security feature is to be considered with great importance. The paper intends to study on few existing cloud service providers and the security they offer. Also the works carried out so far in cloud computing field for enhancing security.

STUDY AND LITERATURE SURVEY

Even though the vulnerability of the existing cloud service are not much high, the growing technological world could make it a factor of concern. Let us consider a few providers glowing in the market based on 2015 review. [23] Dropbox is one the cloud service providers been rated well. It provides security features by; using encryption method for storage and transfer of data, uses SSL/TLS for file transfer, creating a secure tunnel protected by 128-bit or higher AES encryption, vulnerabitility checks are performed regularly on storage and infrastructures, two-way verification, file accessible only to users with authorized links. In short it is designed with multi layer protection, secure data transfer, encryption, network configuration and application and user level controls that are distributed across a scalable and secure infrastructure.

[24]iCloud on the other hand has data encrypted both in transit (using SSL) and on the server. Rather than using AES-256 bit encryption, it uses a minimum of 128-bit AES which is less secure. But it uses 256-bit for the iCloud keychain (used to store and transmit passwords and credit card data, also employing elliptic curve asymmetric cryptography and key wrapping which is good).The iCloud keychain encryption keys, however, are created on your own devices and Apple can't access them. It cannot access any of the core material that could be used to decrypt that key data and only trusted devices that you have approved can access your iCloud keychain. Secure tokens are used for authentication when accessing iCloud and there is optional two-step verification.[25]There are several to keep user files safe in OneDrive. User files aren't shared with other people unless user save in public folder or choose to share them. To help protect OneDrive files from hardware failure, multiple copies of each file are saved on different drives and servers. Other things which help protect user files are: create a strong password, add security info to your Microsoft account, use two-step verification, back up OneDrive files. [26]Google Drive Sharing Policies**,** Change Google Docs Permissions in Bulk**,** View Publicly Shared Documents**,** Correct Public Document Sharing Policy**,** Google Drive Visibility**,**Google Drive Inventory are the security features provided by google drive. Inspite of all the security features provided by the providers reviews show that they have underwent many vulnerability issues[24]. The research field is constantly working on researches to handle the intrusion detection in various fields. Cloud computing field is also in it. [7] Multiple criteria linear programming and particle swarm optimization to enhance the accuracy of attacks detection is an attempt. Multiple criteria linear programming is a classification method based on mathematical programming which has been showed a potential ability to solve real-life data mining problems. However, tuning its parameters is an essential steps in training phase. Particle swarm optimization (PSO) is a robust and simple to implement optimization technique has been used in order to improve the performance of MCLP classifier. [6] proposes a self adaptive ids and a model. The major characteristics that a Hybrid Intrusion Detection System has to possess are Dynamic Nature, Self adaptive, Scalability and Efficiency. The Intrusion Detection System should have the capacity to change its nature of detection whenever it is necessary, which we call it as Dynamic Nature of a Hybrid Intrusion Detection System. The system is for private cloud, where the number of users in the private cloud will be limited in number. Hybrid Intrusion Detection would be the solution for the above problem statement. Hybrid Intrusion Detection System can be defined as a system that has the combination of both anomaly detection method and misuse detection method.

El-Sayed M. el at [8] explores a new countermeasure approach for anomaly based intrusion detection using a multicriterion fuzzy classification method combined with a greedy attribute selection. The proposed approach has the advantage of dealing with various types of attributes including network traffic basic TCP/IP packet headers, as well as content based, time-based and host-based attributes. At the same time, to reduce the dimensionality and increase the computational efficiency, the greedy attribute selection algorithm enables it to choose an optimal subset of attributes that is most relevant for detecting intrusive events. The simplicity of the constructed model allows it to be replicated at various network components in emerging open system infrastructures such as sensor networks, wireless ad hoc networks, cloud computing, and smart grids.

A four level framework for Intrusion detection is proposed[10] in which first procedure concerns to generate different training subsets by using k-means clustering, second procedure based on the training subsets different neuro-fuzzy models are trained, third procedure a vector for SVM classification and radial SVM classification is perform. Finally the decision tree is built using C4.5 decision tree algorithm . It works in a sequence by cascading different decision making algorithms based on their efficiency to handle different levels. SVMs classify data by determining a set of support vectors, which are members of the set of training inputs that outline a hyper plane in feature space. Computing the hyper plane to separate the data points leads to a quadratic optimization problem. There are two main reasons that for using SVMs for intrusion detection. The _rst reason is that its performance is in terms of execution speed, and the second reason is scalability. SVMs are relatively insensitive to the number of data points, and the classification complexity doesnot depend on the dimensionality of the feature space.The principle goal of em ploying the KMeans clustering scheme is to separate the collection of normal and attack data that behave similarly into several partitions which is known as K-th cluster centroids. In other words, K-Means estimates a fixed number of K, the best cluster centroid representing data with similar behavior. Work proposed in [18] is a hybrid system of SVM and hybrid C5.0 - SVM approach. The motivation for using the hybrid approach is to improve the accuracy of the intrusion detection system when compared to using individual approaches. The hybrid approach combines the best results from the different individual systems resulting in more accuracy.In a hierarchical hybrid intelligent system each layer provides some new information to the higher level. The overall functioning of the system depends on the correct functionality of all the layers. In the proposed system the data set is first passed through the C5.0 and node information is generated. Node information is determined according to the rules generated by the C5.0. All the data set records are assigned to one of the terminal nodes, which represent the particular class or subset. This node information (as an additional attribute) along with the original set of attributes is passed through the SVM to obtain the _nal output. The key idea here is to investigate whether the node information provided by the

C5.0 will improve the performance of the SVM. Thus the system enables automatic dataset generation according to the newly arriving attacks. Thus a data set with updated would be possible and as a result the system starts responding to any newly arriving attacks. But the work has only been designed to work in network environment and not in a cloud environment. It is very clearly understood that hybrid IDS give a better result since the data is processed more than once. In [12] hybrid (various decision making algorithm combinations)ids are analyzed and leads to conclude to the following table. Considering the advantage and disadvantages of all the algorithms we could consider a better combination for a better result.

CONCLUSION

The paper aims to study the existing security measures and the loop holes opening to the vulnerability. Solving the whole security issue is equivalent to catching a shadow. The maximum we could do is to get as much as close to the secure side. Attacks and security intrusions are evolving to be more stronger and breaking all the available defenses. In all defensive measures a automatically evolving defensive system is not possible. The existing system are been updated with timely patches to adjust with the evolving attacks. In situation a dynamically adjusting system is worth designing. Artificial intelligent agent could be employed for this. The rate of tolerance against attacks could be lessen and detection of attacks could be enhanced. The paper tries to conclude that a dynamically detecting system is required.

REFERENCE:

[1] Meghana Solanki and Mrs. Vidya Dhamdhere, "Intrusion Detection System by using K-Means clustering, C 4.5, FNN, SVM classifier", *Int. Journal of Emerging Trends & Technology in Computer Science*, Volume-3,Issue-06, Page no (1-23), Dec 2014.

[2] Sourya Joyee De and Asim K. Pal, "A Policy-based Security Framework for Storage and Computation on Enterprise Data in the Cloud", *International Conference on System Science, IEEE*, Page no (1-12), Jan 2014.

[3] Sheng-Wei Lee and Fang Yu, "Securing KVM-based Cloud Systems via Virtualization Introspection", *International Conference on System Science, IEEE*, Page no (1-10), Jan 2014.

[4] Dan Gonzales, *Member, IEEE*, Jeremy Kaplan, Evan Saltzman, Zev Winkelman, Dulani Woods, "Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds", *IEEE Transactions on Cloud Computing,* Page no (1-14), Jan 2015.

[5] Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", *Advanced in Control Engineering and Information Science, Elsevier,* Page no (1-5), Dec 2012.

[6] Praveen Kumar Rajendran, B.Muthukumar, G.Nagarajan, "Hybrid Intrusion Detection System for Private Cloud: A Systematic Approach*" International Conference on Intelligent Computing, Communication & Convergence, (ICCC-2014)*

[7] Seyed Mojtaba Hosseini Bamakan, Behnam Amiri, Mahboubeh Mirzabagheri, Yong Shia, "A New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming", *Information Technology and Quantitative Management , Elsevier,* Page no (1-5), Dec 2015.

[8] Srinavasin, Madhan (2012). "'State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment". *ACM ICACC.*

[9] "Top Threats to Cloud Computing v1.0" (PDF). Cloud Security Alliance. Retrieved 2014-10-20.

[10] Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.

[11] Hickey, Kathleen. "Dark Cloud: Study finds security risks in virtualization". Government Security News. Retrieved 12 February 2012.

[12] Winkler,Vic (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, MA USA: Elsevier. p. 59 ISBN 978-1-59749-592-9.