iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33805

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

Cloud System Hardening

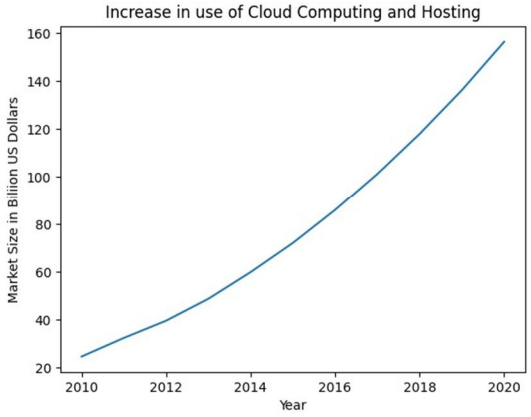
Akshay Bhalerao[1], Parth Pandya[2]
[1, 2]*TY BTECH, Computer Engineering, Vishwakarma University, Pune*

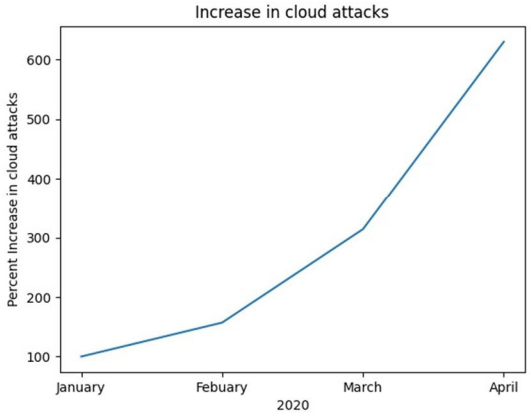
Abstract: ***This research deals with hardening the operating systems used in cloud. Hardening is the process of reducing the risk and vulnerabilities of a system by removing non essential programs and also by installing and correctly configuring firewalls and other security applications. Cyber attacks are increasing day by day. Most of the operating systems rely on the ease of use over security. The same operating systems are used in the cloud, which if successfully attacked, can lead to severe loss of data and other confidential information. This research provides an attempt to secure these operating systems used in the cloud, by making various changes in the configuration and also in the privilege and access management. We also propose a machine-learning driven firewall, to offer better security to fend off various attacks.***

Keywords: Cloud Security, Operating System, Cloud Computing, Data Security, Virtual Machine, IAAS, Infrastructure as a service, Brute Force, SSH, DDOS, DOS, SAAS, Software as a service, machine learning, firewall, K-means clustering.

I. INTRODUCTION

So, providing several means of protection to the computer or operating system is know as hardening. Hardening provides various protection at various levels like host, user, application, physical and operating system level. The use of clouds is increasing day by day. People are using cloud for various purposes like data storage, data processing, hosting websites, providing the cloud as an IAAS(infrastructure as a service), or even as SAAS(software as a service) in which everything, including the software is hosted on the cloud. Due to all this, spending money and resources only on Web Application Firewalls or any other security plugins is not enough. Not hardening the operating system used in these clouds, can make the cloud extremely vulnerable to hackers.





To avoid this we are proposing some changes in the security configurations and access management policies. To begin with, we must first change the default SSH port. We must install SSH Guard, for protection against brute force attacks. We must use load balancers and firewalls, to block the suspicious traffic to avoid DDOS attacks. Backups and Updates should be taken regularly.

The unused ports should be kept closed. Idle accounts should be disabled or deleted. Alternative means of authentication other than text based passwords should by used. A password policy must be enforced. Users should be restricted from becoming super users. If the cloud is being used for processing purposes then login time-out must be enforced. Logs must be maintained of all the user activity.

We also propose to use a firewall, which uses machine learning algorithm, to fend off attacks on the application layer such as SQL Injection, Cross Site Scripting(XSS), Domain Name Server(DNS) Attacks, and cookie poisoning attacks. The said firewall, will help with dynamic attack pattern recognition and update it. This will help us secure the following factors: integrity, authentication, and availability. The goal of the proposed model, will be to cluster malicious and nonmalicious traffic.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

II. METHODOLOGY/WORKING

The first step in securing the cloud should be changing the default SSH port. The default SSH port is port 22. Attacker can easily try to connect this port if the ip-address is known. These attempts of the attacker to connect to the default SSH port can be avoided using strong passwords, but even these strong passwords can be bypassed using brute force attacks. So even if the ip-address is known to the attacker, the attacks on the SSH port can be prevented, if the SSH is not present on its default port 22. This can be done by editing the sshd_config file. In this file we can change the port number, to any other unused port number.

To connect to remote clouds, SSH is the most commonly used service. This must be protected from brute force logins. This can be done by using SSHGuard and Fail2Ban. SSHGuard can be installed on ubuntu using the command 'apt-get install sshguard' and Fail2Ban can be installed on ubuntu using the command 'apt-get install fail2ban'. SSHGuard protects the system from brute force attacks by monitoring and blocking the recurring and unsuccessful login attempts. Fail2ban automatically updates the ip-tables rule, if it detects any unsuccessful login attempts after reaching a certain count.

To connect to the cloud the password based authentication or plain text based authentication techniques should not be used, instead of this email authentication, or biometric authentication, or multi-factor authentication techniques should be used.

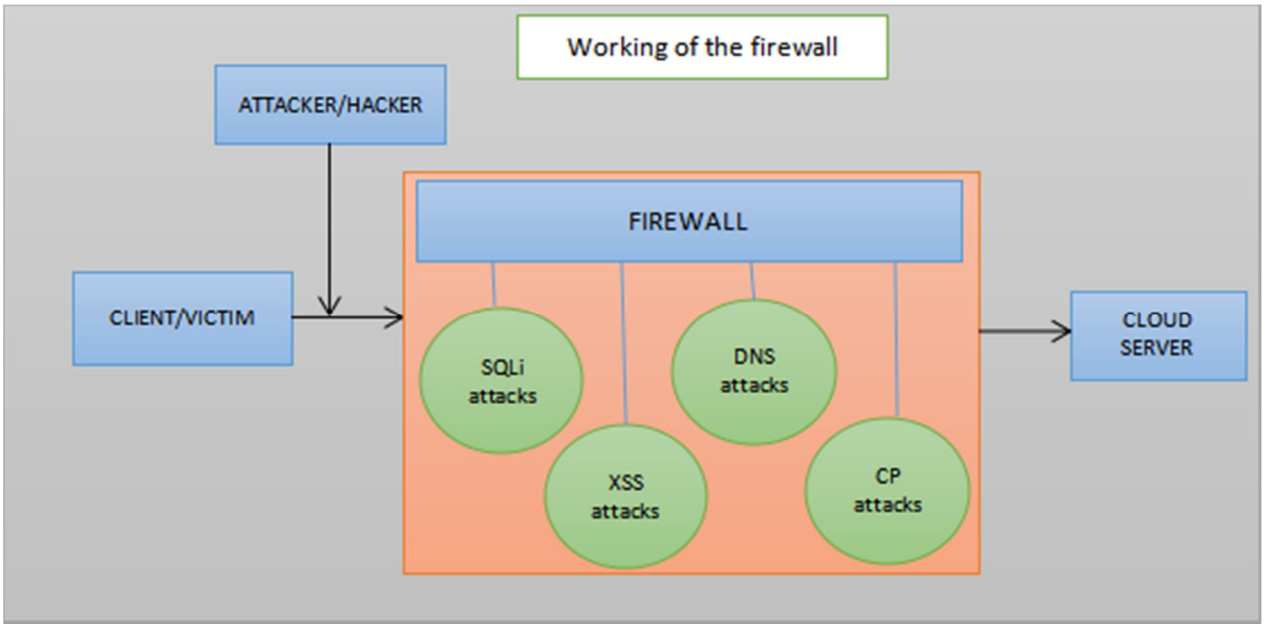
DDOS attacks are one of the common attacks on the cloud. The cloud must be protected from these attacks. To do this we must use both hardware and software based firewalls. Load Balancers must be implemented, so the servers or clouds are not overloaded. Ip-tables must be leveraged and configured in such a way that, the suspicious requests and bogus TCP flags must be blocked.

Backups should be taken regularly, and the OS used in the cloud must also be updated regularly. The unused ports must be kept closed, to avoid attacks on those ports which, if escalated would be fatal to the whole cloud.

If plaintext passwords are used for authentication, then a strong password must be implemented. If there are multiple users then the idle accounts must be deleted or disabled. We must check if there are any accounts with special permission like root permissions. These accounts must be given extra monitoring as they have lot of access, and make significant changes to the system, which may sometimes damage the system.

The normal users must be prevented to becoming super users, and also prevent any other privilege escalation attacks. This can be done by keeping strong passwords or multi factor authentication or by configuring the su file. The logs of all the users' activity must be maintained . So in case of any insider threat or insider malicious activity it can be easily tracked with the help of these logs.

We propose to use clustering(an unsupervised machine learning algorithm).Clustering is the task of dividing the population or data points into a number of groups such that, data points in the same groups are similar to other data points in the same group, and dissimilar to the data points in other groups. It is basically a collection of objects on the basis of similarity and dissimilarity. It is used as a process to find meaningful structure, explanatory underlying processes, generative features, and groupings inherent in a set of examples.The process flow, would be to drop the unsafe/malicious requests and responses from client to server and vice versa, and to let the safe/nonmalicious ones pass through the firewall.



We propose to use k-means clustering for the aforesaid model. We have to define a target number k, which refers to the number of centroids we need in the dataset. A centroid is the imaginary or real location representing the center of the cluster.

The K-means algorithm starts with a first group of randomly selected centroids, which are used as the beginning points for every cluster, and then performs iterative (repetitive) calculations to optimize the positions of the centroids, it halts creating and optimizing clusters when either:

1) The centroids have stabilized — there is no change in their values because the clustering has been successful.

2) The defined number of iterations has been achieved.

Given a set of observations ($\mathbf{x}_1$, $\mathbf{x}_2$, ..., $\mathbf{x}_n$), where each observation is a d-dimensional real vector, k-means clustering aims to partition the n observations into k (≤ n) sets S = {S1, S2, ..., Sk} so as to minimize the within-cluster sum of squares (WCSS). Formally, the objective is to find:

$$\arg\min_{\boldsymbol{S}} \sum_{i=1}^{k} \sum_{x \in S_i} \| \boldsymbol{x} - \boldsymbol{\mu}_i \|^2 = \arg\min_{\boldsymbol{S}} \sum_{i=1}^{k} |S_i| \mathrm{Var} S_i$$

where $\boldsymbol{\mu}_i$ is the mean of points in Si. This is equivalent to minimizing the pairwise squared deviations of points in the same cluster:

$$\arg\min_{\boldsymbol{S}} \sum_{i=1}^{k} \frac{1}{2|S_i|} \sum_{\boldsymbol{x},\boldsymbol{y} \in S_i} \| \boldsymbol{x} - \boldsymbol{y} \|^2$$

The equivalence can be deduced from identity

$$\sum_{\boldsymbol{x} \in S_i} \| \boldsymbol{x} - \boldsymbol{\mu}_i \|^2 = \sum_{\boldsymbol{x} \neq \boldsymbol{y} \in S_i} (\boldsymbol{x} - \boldsymbol{\mu}_i)^T (\boldsymbol{\mu}_i - \boldsymbol{y})$$

Because the total variance is constant, this is equivalent to maximizing the sum of squared deviations between points in different clusters (between-cluster sum of squares, BCSS),which follows from the law of total variance.

A. Euclidean Distance Metric

The Euclidean distance function measures the 'as-the-crow-flies' distance. The formula for this distance between a point X (X1, X2, etc.) and a point Y (Y1, Y2, etc.) is:

$$d(\boldsymbol{p}, \boldsymbol{q}) = \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2}$$

III.LIMITATIONS

A. The changes suggested by us in this research paper, won't provide any security, if the cloud is publicly sharing any data by giving links directly to the cloud.

B. These configuration and policies cannot protect from social engineering attacks, like, phishing which directly leaks the passwords in plain text.

C. Interaction with the cloud occurs through internet channels, this means that attackers can intercept a request, and steal passwords to access cloud management systems, or get access of confidential or secure data.

D. Making all the changes proposed in our research, it may be a load on the cloud. In some cases where clouds are used as IAAS there are limited resources allocated to the user. High end or heavy firewalls can be a load to these resources and can slow down other operations.

E. Attack patterns have to updated manually.

F. The proposed system will be useful against intrusions, but it can not deal with sabotage.

G. Updating the attack patterns frequently is a must.

IV.CONCLUSIONS

By implementing these measures, like, changing the default SSH port, installing SSH Guard for the prevention of brute force attacks, using load balancers and firewalls to avoid DDOS attacks, we can eliminate a significant amount of risk. By updating the system at regular intervals, we can make sure that we get the latest patches to the bugs or vulnerabilities which could have been exploited. By enforcing password policies upon users, such as making them use a strong password will reduce the risk of a success of a dictionary based attack or even a brute force attack. By preventing the user from becoming a super user, we strip away all the privileges that he could have potentially had. By maintaining logs, we look for any malicious activities that someone maybe up to.

The machine-learning driven firewall, could play an important role protecting cloud systems. The rise in various types of attacks will require the firewall to be updated and tested regularly, or else some attack may go undetected and breach the security of the system.

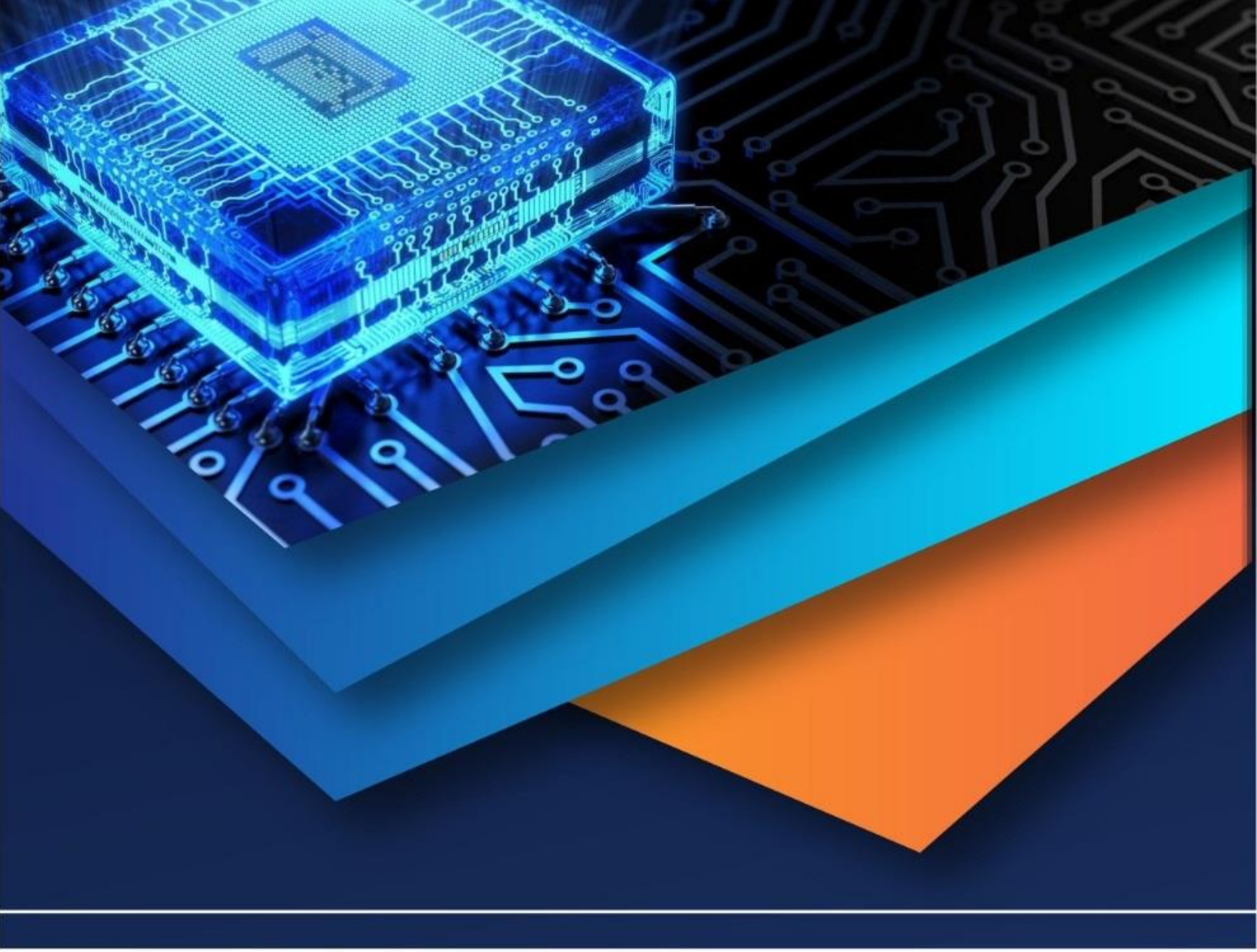
V. FUTURE SCOPE

As stated before, this research aims to harden the OS used in the cloud by various configuration, account and access management changes and policies. We can create an application, which can automate all these tasks, which can potentially reduce the man power needed, to harden the cloud systems.

Also, with the help of some machine learning algorithms, we can predict which systems, precisely lack which aspect of security, and work on that.

REFERENCES

[1] https://www.citefactor.org/journal/pdf/Smart-Firewall-Using-Machine-Learning.pdf
[2] https://en.wikipedia.org/wiki/K-means_clustering
[3] https://towardsdatascience.com/k-means-clustering-algorithm-applications-evaluation-methods-and-drawbacks-aa03e644b48a#:~:text=Kmeans%20algorithm%20is%20an%20iterative,belongs%20to%20only%20one%20group.&text=Keep%20iterating%20until%20there%20is,to%20clusters%20isn't%20changing.
[4] https://www.geeksforgeeks.org/clustering-in-machine-learning/
[5] https://www.cse.iitk.ac.in/users/dheeraj/btech/namitg+abakashs.pdf
[6] https://interpole.net/cloud-blog/secure-and-harden-os-in-cloud/
[7] https://www.forbes.com/sites/emilsayegh/2020/02/12/more-cloud-more-hacks-pt-2/?sh=4fd446c669b3
[8] https://timesofindia.indiatimes.com/gadgets-news/cloud-based-cyber-attacks-increased-630-globally-between-january-to-april-this-year-report/articleshow/76036079.cms



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY