International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

Plant Disease Detection Using Image Processing and Machine Learning

Sharanayya Hiremath

Assistant Lecture, SVS College, Basaveshwar Circle, Ilkal, Karnataka, India

ARTICLEINFO

Article History:

Accepted: 15 Nov 2023

Published: 30 Nov 2023

Publication Issue

Volume 9, Issue 6

November-December-2023

Page Number

181-185

ABSTRACT

Cloud computing offers various advantages to its users, such as data storage on the cloud, on-demand access to resources, pay-per-use services, and so on. As a result of these advantages, a greater number of users have been drawn to utilize the cloud's services. Because cloud customers access its services over the internet, there is a possibility of security assaults on the user's data. To identify security attacks, an attack detection system is required. The attacks are detected using a model based on machine learning techniques. The detection of attacks will benefit both cloud consumers and cloud service providers. If the model is built with machine learning methods, it can improve the performance of security systems. The security features of the systems are managed by creating security systems that use machine learning techniques.

Keywords : IAAS, PAAS, SAAS

I. INTRODUCTION

1.1 Cloud overview

The most useful technology for users is 'Cloud computing,' which allows for easy access to computational resources. Resources are shared via a variety of internet interfaces. Because user expenditures in infrastructure are expensive and require specialization, it is typical for users to use cloud services. However, generally shared and distributed resources come with them unknown security threats. Removing security concerns simplifies cloud adoption and utilization. When the number of its user's increases, the cloud accelerates technology adaption and reduces the time required to implement new services, resulting in increased consumption of its services.

1.1.1Cloud service models

There are various ways in which cloud provide services to its users. Cloud users can get three types of cloud services from cloud:

Infrastructure-as-a-Service (IaaS)

It is the most beneficial service offered to cloud consumers. Cloud users are given with hardware resources via a virtual interface in this case. Cloud customers also have access to more storage space, which is extremely beneficial to businesses. This service provides granular control, which is a key advantage because cloud users can choose the components based on their needs.

Copyright © 2023 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

Platform-as-a-Service (PaaS)

This service model provides cloud users with services such as operating systems for hosting applications and other optional services. Users can run third-party applications or their own applications using these service models. Platforms supplied by PaaS that aid in the automation and democratization of software development.

Software-as-a-Service (SaaS)

Cloud users can get cloud software services via subscription. Cloud customers may be paid based on their use of that cloud software service. Cloud users can access these services without installing anything, while some cloud software applications require plug-ins.

1.1.2 Deployment models of cloud

Public cloud – this cloud's cloud services are easily given to its consumers by a service provider, which is referred to as a public cloud. This cloud is accessed by cloud users via the internet. These services are managed by cloud service providers and are available to cloud customers.

Private cloud – This cloud provides services that are confined to a single enterprise. Organizations utilize the cloud to host applications for their businesses as well as to store company data. Other organizations are unable to access the data stored on the private cloud. These clouds can be controlled by organizations or third parties.

Hybrid cloud – This cloud offers both private and public cloud services to its users. Private clouds are used by organizations for sensitive applications, while public clouds are utilized by organizations for non-sensitive applications. This hybrid cloud can provide scalable and adaptable services to organizations.

1.2 Attack detection in Cloud Computing

Cloud computing offers several advantages to its customers, including data storage in the cloud, on-demand access to resources, pay-per-use services, and so on. Cloud has certain drawbacks in addition to its many advantages. One of the major drawbacks of cloud applications is the possibility of assaults on the user's sensitive data kept on the cloud. In a cloud, attack detection systems are required to identify attacks on users' sensitive data. When it comes to security, detecting and responding to these threats has become essential task. There are numerous approaches for identifying cloud-based assaults; the most often utilized methodology for attack detection is machine learning. Methods for detection of attacks are two types

Knowledge-based detection: This type of attack detection is also known as misuse detection or signature-based detection since assaults are recognized based on data signatures or data knowledge. In this strategy, the system compares its present operations to the signatures of known assaults. Only known assaults are recognized using this method, which means that this method detects only attacks made from authorized users' systems.

Anomaly detection: This assault detection method is also known as behavior-based detection. This method identifies attacks depending on the condition of the data, which implies assaults are discovered based on various data properties. This approach is mostly used to detect unknown attacks. Unknown attacks are attacks carried out by unauthorized users.
There are three types of attack detection systems.

Host-based attack detection systems: This attack detection system is installed on the monitored system and tracks changes to critical files.

Network-based attack detection system: This type of attack detection system monitors and analyzes the network for attack detection.

Application-based attack detection systems: This type of attack detection systems will detect the attacks within the particular application.

1.3 Intrusion detection

Cloud computing is a system in which all resources are available over the internet and users save sensitive data in the cloud. There is a risk that data kept in the cloud will be subjected to security breaches. Attack detection systems (i.e. intrusion detection systems) are essential in cloud computing to secure users' sensitive data and to preserve security elements such as confidentiality, integrity, and availability. Security attacks are launched from both authorized and unauthorized user systems, and are referred to as known and unknown attacks, respectively. Many intrusion detection systems are now being developed, but they are unsuitable for developing technologies such as cloud computing. There is a requirement for an intrusion detection system that detects intrusions automatically.

1.4 Machine learning techniques involved in the attack detection process

Kajaree Das *et al.* [1] gives a survey on various algorithms that are commonly used for text interpretation, pattern recognition, and a variety of other commercial purposes, and it is successful in dividing research in data mining to identify unknown consistency or in consistency in public data that is increasing by the second, and this evolution machine learning is carried out by the three most favorable algorithms, which are entirely based on these fundamental concepts.

Salima Omar *et al.* [2] gives an overview of how to use supervised and unsupervised methods to solve the challenge of attack detection. This document describes many supervised machine learning methods and unsupervised machine learning algorithms used for attack detection, as well as the benefits and drawbacks of all supervised machine learning algorithms.

Vineet Richhariya *et al.* [3] Using machine learning methods, create an effective mechanism for detecting attacks on a network. This is accomplished through the use of modified detection algorithms based on naive Bayes and k-means. The addition distances of the Euclidean of the points from the cluster centres are treated as the similarity metric, and then a modified Naive Bayesian is applied to the cluster centre to detect the assaults. These algorithms are used to improve performance by increasing detection rate and decreasing false +ve rate.

Zecheng He *et al.* [4] Using machine learning methods, concentrate on detecting DDoS attacks in the cloud at the source. The suggested system uses statistical analysis from VM and cloud servers to prohibit packages being delivered to the outside world, and it is evaluated as well as their performance is compared, and all four types of DOS attacks are successfully recognized.

Daniel Grzonka *et al.* [5] The suggested model would monitor system controls as a distinct service, and it is one of the most powerful monitoring systems for gathering all information from cloud storage. It assists the system in providing security and improving system performance during scheduling, execution, and task gathering processes in large-scale service-oriented environments, as well as preventing unauthorized task injection and modification, optimizing the scheduling process, and maximizing resource usage.

Manali Trivedi *et al.* [6] provides a survey on cloud resource provisioning based on machine learning. For resource provisioning, cloud computing employs a variety of strategies. There are numerous issues with

resource provisioning, such as workload auto scaling and CPU utilization. When resources are provisioned using machine learning, they can be delivered in a more efficient manner. Some techniques are used in this for CPU utilization and scaling, and some techniques use machine learning algorithms, and model accepts requests from the user, then request manager manages the requests, then ml processor checks which request wants how much resources based on previous requests, and then resource provisioning is executed and scaling decision is made.

Deepali Arora *et al.* [7] Represents how to determine internal and external user threats to data stored in the cloud using machine learning algorithms, for and develop smart Quality of Services, and provide solutions to ensure end-to-end security in that anomaly detection techniques with clustering algorithms are used to detect attacks in the cloud environment. The system categorizes users as hazardous or harmless based on their conduct. Furthermore, it is represented by the supervised learning algorithm.

Amjad Hussain *et al.* [8] create an anomaly attack detection system for virtual machines in a cloud environment using machine learning approaches. In that case, the feature selection over events is from a virtual machine monitor to detect anomalies while simultaneously training the system to learn new attacks and update the model. The experiment was run on NSL-KDD'99 datasets using the Nave Bayes Tree (NB Tree) Classifier and a hybrid technique of the NB Tree and Random Forest machine learning algorithms.

We found different methods of attack detection and different techniques of attack detection. Each method of attack detection has its own advantages and disadvantages. During attack detection process some issues are identified. These issues are discussed below.

II. ISSUES IDENTIFIED

Detection policy: The detection policy used for detecting assaults in a cloud is the most important component of determining if the data stored by the user is attacked or beneficial data. The detection method should be efficient enough to match data in various forms efficiently. Most researchers' detection policies are either mis-use detection for detecting known attacks or anomaly-based detection for detecting undiscovered attacks. As a result, a system that can identify both known and unexpected assaults is required.

Integration of Multiple formats: As we all know, the data entered by cloud users might be in a variety of forms. As a result, there is a requirement for a technique to process the user's input, and diverse formats must be combined on a single intrusion detection system.

Platform Dependence: Intrusion detection systems for detecting assaults are designed to meet specific needs and are built on a specific platform. The same intrusion detection mechanism is not available on all platforms. As a result, an intrusion detection system that is platform independent is required.

Poor design: All intrusion detection systems are designed in such a way that if a user wants to change some aspect of the intrusion detection system, the intrusion detection system must be halted, then the modifications are made as requested, and the intrusion detection system must be re-deployed. As a result, an intrusion detection system with two components is required, one core element consisting of detection algorithm and the second part related with pattern matching. This section should be updated as needed and should not interfere with the system's detection process.

III.CONCLUSION

Nowadays, a considerable amount of sensitive data from users is stored on the cloud, and protecting user data is critical. Data saved in the cloud can be safeguarded by understanding where the assault took place and what type of attack took place.

After reviewing the literature on various attack detection systems in cloud computing, many issues such as attack detection policy, data integration across multiple formats, platform dependencies, and poor attack detection system design were identified as challenges for attack detection in cloud computing. More emphasis is placed in these on attack detection policies for detecting known and unknown threats in the cloud.

IV. REFERENCES

[1]. Kajaree Das Rabi Narayan Behera " A Survey on Machine Learning Concept, Algorithm and Applications", International Journals of Innovative Research in Computer and communication Engineering, Volume 5, Issue 2, February 2017

[2]. Salima Omar, Asri Ngadi , Hamid H Jebur "Machine Learning Techniques for Anomaly Detection: An Overview", International journal of computer Application, Volume 79,PP 0975-8887,October 2013.

[3]. Vineet Richhariya, Dr J.L.Rana, Dr R.K. Pandya, Dr R.C.Jain " An Efficient Classification Mechanism using Machines learning Techniques for Attack Detection for Large Dataset", International Journal of Innovative Research in Science Engineering and Technology, Volume 1,Issue 2 December 2012.

[4]. Marwane Zekri, Said El kafhali,Noureddine Aboutabit and Yoursefsaadi, "DDoS Attack Detection using Machine Learning techniques in cloud computing environments", IEEE 3rd International conference of cloud computing technologies and applications 2017.

[5]. Lingvei Chen, Yanfang ye, Thirimachos Bourlai, " Adversarial Machine Learning in Malware Detection; Arms Race between Evasion Attack and defence" , European Intelligence and Security Informatics Conference 2017.

Cite this article as :

Sharanayya Hiremath, "Plant Disease Detection Using Image Processing and Machine Learning", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 6, pp.181-185, November-December-2023.