ADVANCE CONCEPTUAL MODELING PLATFORM ON CLOUD ATTACKS

SHYAM UDGIRE
Prof PADMAPRIYA

Student Department of MCA, AMC Engineering College(VTU), Bengaluru, India

Professor Department of MCA, AMC Engineering College(VTU), Bengaluru, India

Abstract:

Cloud security has emerged as a prominent and extensively researched concern in recent years. It is crucial to address the potential exploitation of vulnerabilities in cloud systems which can direct to the undermine the virtual machines and the execution of large scale Distributed DDOS Denial of Service attacks. The process often involves attackers taking advantage of multiple steps, including low frequency vulnerability scanning, exploiting identified vulnerable virtual machines, and ultimately launching DDoS attacks using compromised zombies. Detecting zombie inspection attacks within cloud systems, particularly Infrastructure as a Service (IaaS) clouds poses significant challenges due to the possibility of cloud users deploying exposed applications on their virtual machines. To mitigate the compromise of unprotected virtual machines in the cloud, we propose a multi phase distributed mechanism called NICE incorporates analytical models based on attack graphs and employs reconfigurable virtual network based for the detection and measurement of appropriate counter measures.

1.Introduction

Cloud computing is a technology that leverages the internet and centralized remote servers to store data and run applications. It enables users and businesses to access applications and personal files from any computer with internet connectivity, eliminating the need for local installation. This technology improves computing efficiency by consolidating data storage, processing, and bandwidth. Cloud computing typically involves network-based services that are provided by virtual hardware running on real machines, allowing for versatility in grading without influence end users. It creates a network-based environment focused on resource sharing and utilizes virtualization technologies and self service capabilities for computing resources. Cloud environments host various virtual machines on the same physical server infrastructure.

Recent studies highlight that security is a crucial concern for users transitioning to the cloud. The abuse and malicious use of cloud computing are identified as the top safety threat according to the (CSA) Cloud Security Alliance survey. Attackers exploit vulnerabilities within clouds to launch attacks and make use of cloud system resources. Unlike traditional data centres where system supervisor have full control and patching known safety exposure in cloud data centres becomes complex due to the freedom of cloud users to control software on their handled (VMs) virtual machines potentially violating Service Level Agreements (SLAs). More over the installation of vulnerable software by cloud users further undermines cloud security. The challenge lies in establishing an effective system for vulnerability and attack detection/response to accurately identify and minimize the impact of security breaches on cloud users.

In cloud systems, where infrastructure is shared by millions of users, the shared nature of resources allows attackers to exploit cloud vulnerabilities and conduct more efficient attacks. Such attacks capitalize on the shared computing resources, network connectivity, data storage, and file systems among potential attackers and cloud users. Cloud security is an evolving field within computer security, network security, and information security. It encompasses a range of policies, technologies, and controls deployed to safeguard data, applications, and associated infrastructure within cloud computing. Enterprises consider security a paramount concern but approach it with different perspectives. It is important to note that the cloud itself is not inherently less secure. Various forms of cloud attacks exist, including DDoS attacks against the cloud and cloud-based defence against DDoS attacks.

2.Types of cloud computing:

Software as a service (SaaS)
Platform as a service (PaaS)
Infrastructure as a service (IaaS)

SaaS (Software as a Service)
In cloud computing refers to the subscription-based internet distribution of software applications. Users can access the program using a web browser, and it is hosted and managed by a third-party provider in the cloud rather than having to install and maintain it on individual PCs or servers.

The following are some salient features and advantages of SaaS in cloud computing

1. Accessibility: SaaS apps can be used from any location with an internet connection, enabling users to access their software and data from different gadgets and places.

2. Scalability: SaaS systems that are cloud-based can simply scale up or down in response to user demand. Without seriously disrupting users, the supplier is able to distribute more or fewer resources to meet shifting needs.
Platform as a Service (PaaS)
It is a cloud computing architecture that gives developers a platform and an environment to create, launch, and manage applications without having to worry about supporting infrastructure. In PaaS, a whole development and deployment platform, including operating systems, programming languages, libraries, tools, and frameworks, is provided by the cloud service provider.

The following are some essential features and advantages of PaaS:

Development environment for apps: PaaS gives programmers a ready-made platform with all the tools and services they need to create, test, and deploy applications. Developers are no longer need to set up and maintain their own development environment as a result.
Scalability: PaaS solutions enable applications to be scaled dynamically in response to demand. They make available resources like processing speed, storage, and bandwidth.

Infrastructure as a service (IaaS)
The cloud computing concept known as Infrastructure as a Service (IaaS) makes use of the internet to deliver virtualized computing resources. Without the need for real hardware, customers may access and control basic computing resources like virtual machines, storage, and networking infrastructure on demand with IaaS.
IaaS's salient features and advantages are as follows:

IaaS provides virtualized computer resources that can be provided and controlled remotely. Virtualized infrastructure. Users can build and set up virtual computers, storage volumes, and networks according to their own needs.
Scalability: IaaS enables users to scale up or down the infrastructure resources according to their requirements. In order to adapt to changing demands, they can easily increase or decrease the number of virtual machines, storage space, or network bandwidth.

3.cloud computing services:

Cloud services refer to various computing resources and functionalities offered over the internet by cloud computing providers. These services enable users to leverage remote computing power, storage, and software applications without the need for on-premises infrastructure. Here are some common types of cloud services:

Compute Services:

computing resources Compute services provide virtualized, allowing users to run applications and perform computational tasks in the cloud. This includes services such as virtual machines (VMs) in IaaS, serverless computing (Function as a Service), and containerization platforms.

Storage Services:

Cloud storage services offer scalable and secure storage solutions for storing and accessing data over the internet. This includes object storage, block storage, and file storage options, providing durability, redundancy, and flexibility for data management and backup.

Database Services:

Database services provide managed database solutions in the cloud. They offer scalable and highly available databases, eliminating the need for users to manage the underlying infrastructure. Examples include relational databases (RDBMS), NoSQL databases, and in-memory databases.

Networking Services:

Networking services facilitate the creation and management of networks in the cloud. These services include virtual networks, load balancers, firewalls, and content delivery networks (CDNs). They enable secure and efficient communication between cloud resources and users.

Security Services:
Cloud security services focus on ensuring the security and compliance of cloud-based resources. This includes identity and access management (IAM), encryption, threat detection, security monitoring, and compliance auditing tools.

Analytics and Big Data Services:

Cloud providers offer analytics and big data services for processing and analysing large volumes of data. These services include data warehousing, data lakes, real-time streaming, machine learning, and data visualization tools.

AI and Machine Learning Services:

Cloud platforms provide AI and machine learning services, offering prebuilt models, training frameworks, and APIs for implementing AI capabilities in applications. These services facilitate tasks such as natural language processing, image recognition, and predictive analytics.

IoT (Internet of Things) Services:

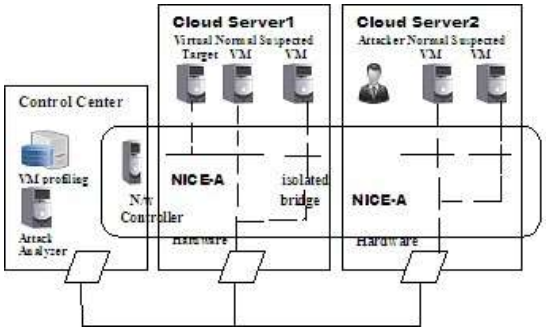
IoT services in the cloud enable the connection, management, and analysis of IoT devices and data. They provide platforms for collecting and processing sensor data, device management, and integration with other cloud services.

DevOps and Development Tools:

Cloud providers offer tools and services to support development, testing, and deployment processes. This includes code repositories continuous integration deployment(CI/CD) pipelines container registries, and development environments.

These are just a few examples of the wide range of cloud services available. Cloud providers often offer a comprehensive suite of services, allowing users to select and combine the services that best fit their needs, and pay for them on a pay-as-you-go basis.

4.System Architecture
A cloud-based system's design and organization, including the efficient integration and structuring of hardware, software, networking, and storage, are referred to as its system architecture. Multi-tier architecture, virtualization, scalability and elasticity, distributed computing, microservices and service-oriented design, data management and storage, security and compliance, and hybrid and multi-cloud integration are important elements of cloud system architecture.



5.Importance of cloud computing:

In today's technological scene cloud computing is quite important. Here are some main arguments in favour of Cloud computing

Scalability and Flexibility: Organizations may easily scale resources up or down in response to demand thanks to cloud computing's scalability and flexibility. Businesses can effectively handle changing workloads and accommodate expansion because to its scalability, which eliminates the need for major infrastructure investments or capacity planning.
Cost Effectiveness: By removing the requirement for up-front hardware and software investments, cloud computing results in cost savings. With cloud services, companies pay as they go for the resources they use, lowering capital spending and enabling predictable operational costs. The expenses related to operating and maintaining on-premises infrastructure are also removed by the cloud.
Cloud computing users' accessibility and mobility and Accessibility Users can access programs and data via cloud computing from any location with an internet connection. This accessibility encourages distributed teams' productivity, remote work, and collaboration. Additionally, it enables customers to access their resources from a variety of gadgets, such as tablets, smartphones, and computers.

Disaster Recovery and Business Continuity: Cloud computing provides reliable solutions for disaster recovery and business continuity. To ensure data and apps are backed up and accessible even in the case of a disaster, cloud service providers often operate redundant data centre in various regions. This improves the resilience of enterprises by lowering the risks of downtime and data loss.

Enhanced Security: To secure customer data, cloud service companies make significant investments in security measures. They use cutting-edge security measures, encryption.

Conclusion:

The paper introduces NICE a proposed solution aimed at detecting and mitigating collective attacks in cloud virtual networking environments. NICE leverages the attack diagram model for attack detection and prediction. The solution explores the use of programmable software switches to enhance detection exactness and counter victim misuse during collaborative attacks. However NICE focuses solely on network-based IDS for countering zombie preliminary attacks. Future research should consider incorporating host-based IDS solutions to cover a broader range of IDS capabilities inside the cloud system. Additionally the expandable of the NICE solution will be further investigated by exploring localised network control and attack analysis models based on present research findings.

Reference:

[1] Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang, "NICE: Network Intrusion Detection and Countermeasure, Selection in Virtual Network Systems,

[2] K.Santhi, "A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks"

International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May
2013

[3] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, "Detecting spam zombies by monitoring outgoing messages," *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 2, pp. 198-210, Apr. 2012.

[4] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using bayesian attack graphs," *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 1, pp. 61-74, Feb. 2012.