Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Guaranteeing User Safety in Public Cloud Environment

Mrs. Deepa S[1], Marella Nikhitha[2], Monisha Garrepelly[3], Shanmuga Priya A V[4]
Asst. Professor[1], Department of Computer Science and Business Systems, R.M.D Engineering College, Chennai, Tamil Nadu, India
deepa.csbs@rmd.ac.in
Student[2,3,4], Department of Computer Science and Business Systems, R.M.D Engineering College, Chennai, Tamil Nadu, India
ucb20124@rmd.ac.in , ucb20125@rmd.ac.in , ucb20212@rmd.ac.in

Abstract:

Flexibility and availability are important in the IaaS model, but security concerns affect some organizations. This article describes security measures such as virtual printers and storage protection to protect sensitive data. The program focuses on verifying host platform configuration, remote storage of confidential information, and external key management. Experiments with the Public Health Information Pilot Project demonstrate its benefits and potential for integration.

Introduction

Cloud computing simplifies hardware complexity for users by offering on-demand services and enabling payment for services used. It includes important resources such as self-service, technical assistance, and fast turnaround. However, as data moves to the cloud, security threats, especially Denial of Service (DoS) and Distributed Denial of Service (DDoS), emerge and become a serious concern. While DoS attacks will cause business interruption on important targets, DDoS attacks will cover many areas and make protection difficult. This article discusses various DDoS attacks and explores their air defenses.

Objective:

The main goal of the project is to improve the security of Infrastructure as a Service (IaaS) platforms, especially for organizations that manage sensitive data. This is done using a framework that includes powerful mechanisms for configuring virtual machines and protecting storage. The project aims to build trust in the platform's configuration, store data in remote private storage, and reduce the risk of encryption keys being compromised. Ultimately, the goal is to integrate security resources into the existing cloud environment.

Literature Survey:

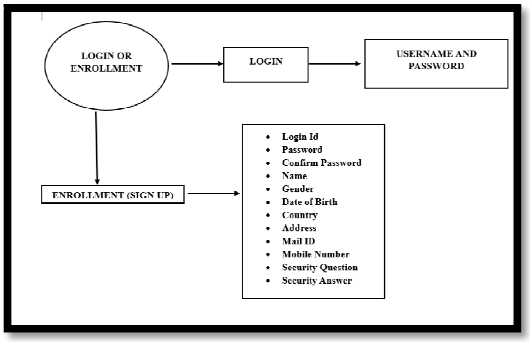
The cloud-as-a-service (IaaS) model offers tenants more flexible and cost-effective products, freeing them from complex hardware, computer rentals, and complex operations. Many organizations use sensitive data to prevent migration and reuse IaaS platforms for protection. In this article, we use encryption protection process (OBP) to ensure the performance and security of data stored in the cloud, and also use other technologies such as standard measures and third-party services to update the importance of cloud management.

Available. It is easy to ensure security and reduce data leakage. Businesses are investing in tight security and planning best practices [9]. The main goal of the project is achieved through IaaS. In its simplest form, IaaS tells users that it is a shared platform because it supports cloud-based virtual machines. Guests can interact with the virtual environment by providing simple rules for exporting electronic health records (EHR) created by the virtual network. bump on the road. platform. Threats and migration to IaaS have increased in recent years [5] [7] [8]. First, since the content of the main content is not completely closed, it will not be available and enhanced by other cloud platforms [8]. Nuno Santos Krishna P. Gummadi Rodriguez. [2] Provide mechanisms to ensure operators are reliable from remote locations. These platforms will protect virtual machines running on a single host. AntonisMisalas, Nicola Paradi and Christian Gelman. [1] It aims to create a paperless healthcare system where patients and doctors can make appointments online, create electronic prescriptions, and store their medical history in a repository that is easily accessible to anyone with access rights. McDaniel, Kevin Butler, Radoucion, ErezZadok, Quiren and Marian Winslet. [3] Long-standing problems with large machines. A recent report prepared for the President and the House Committee on Democracy and the Environment [3] highlighted the need to begin connecting our technology to the past, as well as the security of our nation's critical infrastructure.

MODULES:

Module:1 User Authentication and Enrollment

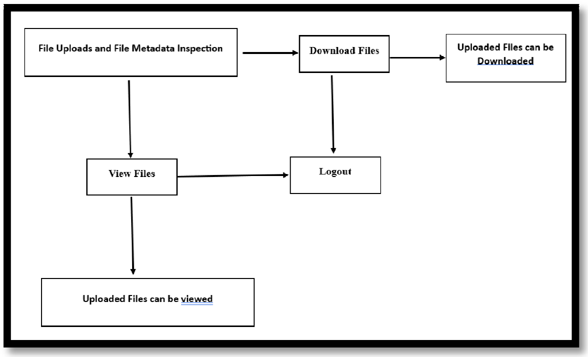
Access is a simple process that allows access to specific pages and prevents unauthorized access. When the user logs in successfully, a unique login name is created, which allows the website to track the user's actions during the session. The basis of user authentication and registration is the user registration module. New users must register and receive a unique password associated with their chosen username. To access their account, users must provide a valid username and password to authenticate and secure their account.



Module 2-File Uploads, File Metadata Inspection and File Dowonloads

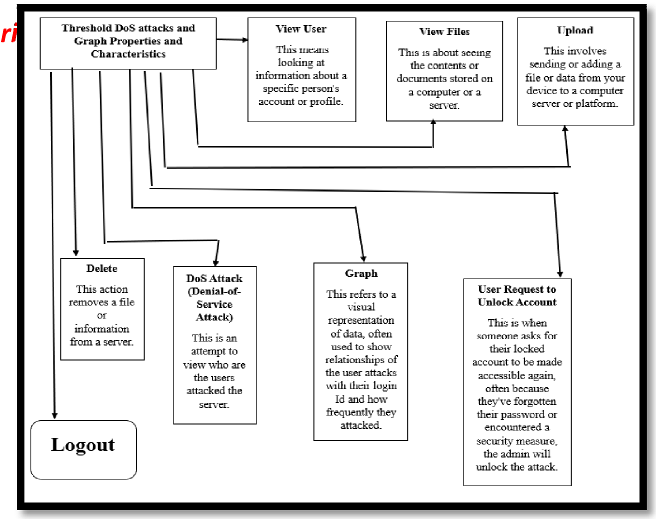
- File upload module is mainly used to upload files from cloud. This method can also be used to detect inappropriate behavior of authorized users towards other users.
- In File Upload Details, you can view file details and tell the user how to upload files. Users can easily find content information.

- Users can download the required files from the uploaded files.


File Uploads and File Metadata Inspection
Download Files
Uploaded Files can be Downloaded
View Files
Logout
Uploaded Files can be viewed

Module 3-Threshold DoS attacks and Graph Properties and Characteristics

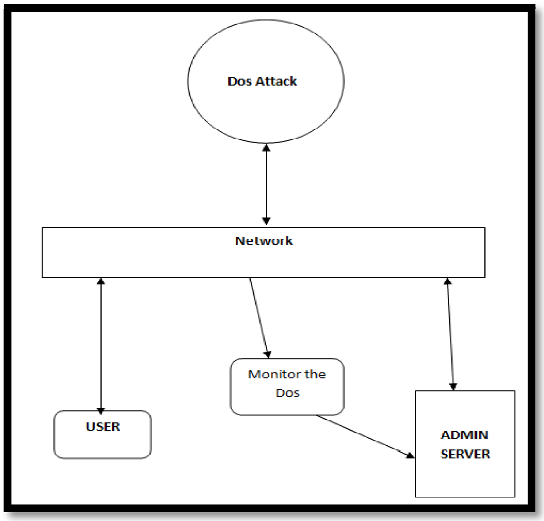
- A begin is worth it. You relate the starting with measurements (voting information). When this examination is composed it is compared to the beginning point. In case information isn't put away in understanding with the limit, it may cause debased hardware or arrange execution. The word "suit" is used here because you'll be able set edges and levels such as most extreme, least and offset.
- Details appeared within the chart of DOS attackers. The month and time points of interest of assaults within the organize are appeared within the realistic subtle elements. A chart, too known as a chart, may be a graphical representation of information in which the information is spoken to by images such as lines on a bar chart, lines on a bar chart, or portions on a chart. gives work or a few great structures and diverse data.


Threshold DoS attacks and Graph Properties and Characteristics
View User
This means looking at information about a specific person's account or profile.
View Files
This is about seeing the contents or documents stored on a computer or a server.
Upload
This involves sending or adding a file or data from your device to a computer server or platform.
Delete
This action removes a file or information from a server.
DoS Attack (Denial-of-Service Attack)
This is an attempt to view who are the users attacked the server.
Graph
This refers to a visual representation of data, often used to show relationships of the user attacks with their login Id and how frequently they attacked.
User Request to Unlock Account
This is when someone asks for their locked account to be made accessible again, often because they've forgotten their password or encountered a security measure, the admin will unlock the attack.
Logout

Problem Statement:

"Improving user security in public cloud infrastructure is very important. Our goal is to solve the problem by creating a framework that ensures security. The framework will protect users' data, prevent vulnerabilities and maintain good encryption keys, thus increasing trust in public cloud services."

Architecture Diagram:



Existing System:

Conduct a platform integrity assessment regarding the use of member support virtualized cloud infrastructure on existing systems. Many major cloud vendors say they will use this technique primarily to protect the cloud against insider and persistent threats. Many cloud providers offer data encryption at rest and can be configured by tenants on their virtual machines. Generally, cloud service providers manage and manage the keys required to encrypt and decrypt data at rest. This adds complexity to the existing data transfer process between different cloud providers, leaving tenants vulnerable to new vendor changes and products. Tenants can choose to encrypt data on virtual machines at the operating system (OS) level and manage their own encryption keys.

Drawbacks of Existing System

- When the virtual machine performs encryption, the host computer can still access the encryption keys.
- This shifts the burden of managing software encryption of all virtual machines to the tenant and increases the stopping point.
- This should be done by transmitting the encryption key to all virtual machines that can access the encrypted data and then removing the encryption key to ensure security, thus opening the possibility for an attacker to obtain the key.

Proposed System:

The implementation is DBSP (Domain Based Storage Protection), a virtual disk encryption system that completes data encryption directly on the computer and requires a key to regenerate the key. The encryption is stored in the metadata container. This approach simplifies the transfer of encrypted files and eliminates the need to manage disk encryption keys in the cloud. Additionally, as a software package, DBSP provides greater control over network operator selection, reducing the risk of switch access and increasing the burden on tenants. In its simplest form, the Infrastructure as a Service model provides shared tenants to business owners who run VM guests that communicate over a virtual network.

Proposed System and It's Advantages

• In IaaS, the trusted process starts with the virtual machine.

• Virtual machine key management and encryption capabilities enable transparent encryption of persistent data in the cloud.

• Policy and Security Policy (TTP) is managed by a trusted third party.

Future Work:

We believe instant protection is the best way to prevent DDoS attacks. We hope to be able to create a web protection system in the near future that requires the cooperation of many service providers to provide address verification and filtering.

Conclusion:

"In this study, we use data mining techniques to analyze Denial of Service (DoS) attacks, which are threats to IT resources. DoS floods users with forced messages, causing user dissatisfaction and poor performance. Our research covers: network security, network crime, clusters, outliers and authentication model. When the requirements are similar to the threshold, we use log data and real-time data to identify the attack. This allows the

DoS attack to seek profit and alert leaders to the threat."

References

[1] B. Bertholon, S. Varrette, and P. Bouvry, "Certicloud: a novel tpm based approach to ensure cloud IaaS security," in Cloud Computing, 2011 IEEE International Conference on, pp. 121–130, IEEE, 2011.

[2] A. Michalas, N. Paladi, and C. Gehrmann, "Security aspects ofe-health systems migration to the cloud," in the 16th International Conference on Ehealth Networking, Application & Services (Healthcom'14), pp. 228–232, IEEE, Oct 2014.

[3] M. Aslam, C. Gehrmann, L. Rasmussen, and M. Bj ̈orkman, "Securely launching virtual machines on trustworthy platforms in a public cloud – an enterprise's perspective.," in CLOSER, pp. 511–521, SciTePress, 2012.

[4] A. Cooper and A. Martin, "Towards a secure, tamper-proof grid platform," in Cluster Computing and the Grid, 2006. CCGRID 06.Sixth IEEE International Symposium on, vol. 1, pp. 8–pp, IEEE, 2006.

[5] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trustedcloud computing," in Proceedings of the 2009 Conference on HotTopics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA),USENIX Association, 2009.

[6] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 55–66, ACM, 2009.

[7] J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel,"Seeding Clouds With Trust Anchors," in Proceedings of the 2010ACM Workshop on Cloud Computing Security, CCSW '10, (NewYork, NY, USA), pp. 43– 46, ACM, 2010.

[8] N. Paladi, A. Michalas, and C. Gehrmann, "Domain based storage protection with secure access control for the cloud," in Proceedingsof the 2014 International Workshop on Security in Cloud Computing, ASIACCS '14, (New York, NY, USA), ACM, 2014.

[9] Cloud Security Alliance, "The notorious nine cloud computing top threats 2013," February 2013.

[10] M. Jordon, "Cleaning up dirty disks in the cloud," Network Security, vol. 2012, no. 10, pp. 12–15, 2012.