International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 04 Issue 02 |2020

Securing Own cloud from Malicious File Uploads Using Clamav

TejaswiniSrinivasa Murthy[1],NithinTheeyaAnantha Padmanabha[2]
[1,2] *Master Student, Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India*

ABSTRACT

ClamAV Antivirus is an open-source antivirus used to detect threats such as Trojans, malware, viruses. In this project, we learn how to configure and secure ownCloud using ClamAV Antivirus. Cloud is a very rewarding and desirable platform for the hackers as they gain so much from an exploited cloud platform. As there are numerous active users on a cloud platform, it makes it much more necessary and difficult to protect the data from getting hacked.There are numerous ways to prevent malicious files from getting into the cloud. One such way is to filter the files at the time of upload. This process is performed with the help of an antivirus which is configured to scan and protect the system and also to stop malicious files from getting uploaded. As a security executive, it is our duty to make sure that the cloud is uninfected and safe for the clients to use it without worrying about privacy.

Keywords: ClamAV, ownCloud, Antivirus, Cloud Computing, Malicious files.

1. INTRODUCTION TO CLOUD COMPUTING

Cloud computing is the most trending in recent days because of its flexibility and support. It allows us to access personal and shared resources with minimal management. It sometimes relies on the internet. There are many third-party cloud services available in the market which saves expanding resources and maintenance. A most appropriate example of Cloud computing is Amazon Elastic Cloud Compute (EC2), which is highly capable, low cost and flexible.

Major characteristics of cloud computing include :

- On-demand self-service
- Distributed Storage
- Rapid Elasticity
- Measured Services
- Automated Management
- Virtualization

Cloud computing is the availability of computer resources like data storage and computing power. The term is often used to describe data centres available to many users over the internet. One of the important features of the cloud is functions distributed from central servers over multiple locations. Cloud computing types are service deployment models that allow us to choose the level of control over our information and the types of services we need to provide.

1.1 Types of Cloud Computing Services

The three main types of cloud computing services are:

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

1.1.1 Infrastructure-as-a-Service (IaaS)

Infrastructure as a service (IaaS) can be defined as a cloud computing model that allocates virtualized computing resources to the user through the internet. One of the main components of cloud computing is IaaS. IaaS is completely monitored and managed over the internet. The IaaS technology helps the users to save the cost and also manage their own physical servers by reducing complexity. All the resources of IaaS are offered as individual service components and the users select them depending on the need. The users are supposed to concentrate on installing, configuring and managing the software while the cloud service provider manages the IaaS infrastructure.

1.1.2 Platform-as-a-Service (PaaS)

PaaS is another type of cloud computing model in which a provider from third-party delivers hardware and software tools over the internet which are used in application development. Hardware and software are hosted on its own infrastructure by the PaaS provider. As a result, there is no need for developers to install in-house hardware and software to develop or run a new application. There is no need for PaaS to replace the company's entire IT infrastructure for software development. The users most frequently access the offerings through a web browser, which is provided through a cloud service provider's hosted infrastructure. PaaS is sometimes delivered through public, private and hybrid clouds to deliver services like Java development and application hosting.

1.1.3 Software-as-a-Service (SaaS)

The third cloud computing type is SaaS which is used for web-based applications. SaaS delivers software applications over the internet. Cloud providers host and manage these applications by making it easier to access the same application on all of our devices at once from the cloud.SaaS applications are usually accessed by users using a thin client such a web browser. SaaS is the most common delivery model used in many business applications including software such as office, messaging, DBMS, CAD, virtualization, CRM, ERP, etc. All the leading enterprise software companies have incorporated the strategy of SaaS.

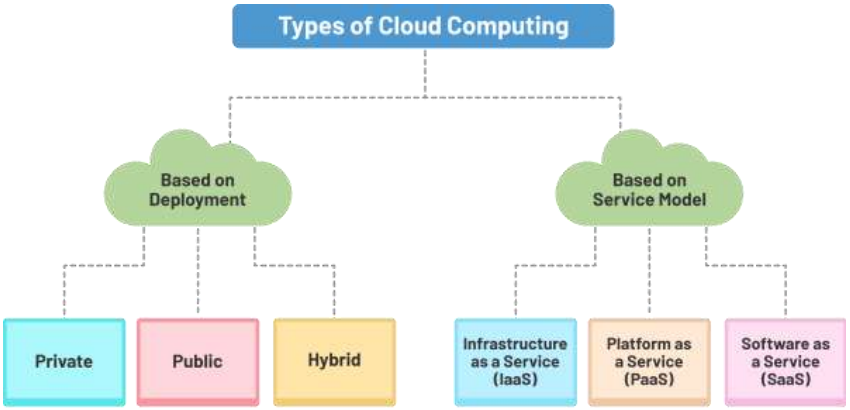

Fig-1: Types of Cloud Computing

1.2 Types of Cloud Deployments

1.2.1 Public cloud

Public cloud is usually offered by SaaS to users over the internet. It is one of the most economical options for users where the service provider bears the bandwidth and infrastructure expenses. The cost is determined by usage capacity. It has limited configurations due to its lack of SLA specifications. Public cloud is not the best choice for organizations with sensitive information as it compromises data and breaks security regulations. Some of the features of public cloud are high reliability, lower costs and zero maintenance.

1.2.2 Private cloud

Large organizations use the private cloud to build and manage their own data centres business and IT operations. The private cloud provides control over scalability and flexibility to improve the security of assets and business operations. Private cloud has the ability to maintain hardware and software environment over a private network. Government agencies and Large and Medium-scale financial enterprises usually go for private clouds.

1.2.3 Hybrid cloud

Hybrid cloud is the combination of private and public cloud, which provides more flexibility to businesses having control over critical operations and assets. Hybrid cloud enables companies to take advantage of the public cloud when necessary due to their workload migration. For example, public cloud is used to run high-volume applications like emails, and they utilize private clouds for sensitive assets like financials and data recovery.

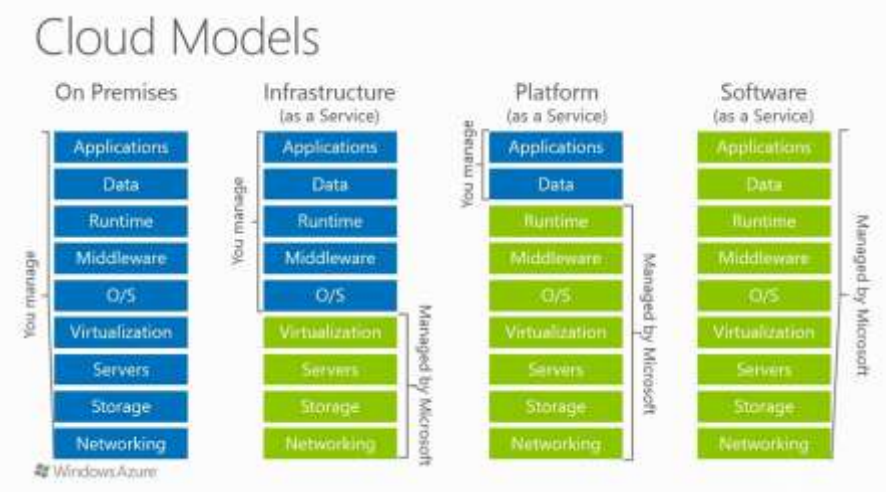

Fig-2: Cloud Models

2. CLAMAV AND OWN CLOUD

ClamAV is an open-source and multi-platform antivirus which supports multiple file-formats with file and archive unpacking. ClamAV is the only antivirus program which supports ownCloud and it detects multiple signature languages. It also has command-line utilities for on-demand file support with automatic signature updates. It is a versatile antivirus with a multi-threaded daemon which makes it a great tool to keep your system secure. ClamAV includes various utilities such as command-line scanner, automatic database updater and so on.

ClamAV is an antivirus toolkit used in Unix. The main purpose of this antivirus is the integration with mail servers. This toolkit provides scalable and flexible multi-threaded daemon. It is a command-line scanner and a tool for automatic updating via the Internet. These programs are based on a shared library distributed with ClamAV package. The virus database should be regularly updated.

ownCloud gives us universal access to our files through a web interface. ownCloud provides us with a platform to easily view contacts, calendars and bookmarks across all our devices. It is also easy to install with minimal server requirements. It doesn't need any special permissions. ownCloud is extendable via a powerful API for applications and plugins.

2.1 Features ofownCloud

- **File-Sharing:** It is easy to share the files to anyone at any point of time using the ownCloud app on the mobile phone. We need not fire up our laptop, access the internet, access the VPN, start an email and attach the file. File Sharing can be done within few seconds using our mobile phone.
- **Syncing:**ownCloud keeps a track of all the file versions with the help of sync client that keeps the web, desktop and mobile device on the same page. The users need not worry about the latest file version even if they are away from their laptop. ownCloud actively monitors the changes in the files and pushes the latest version to all devices and all relevant users wherever they are.
- **Encryption & Security:**ownCloud is a software provided to install in our data centre, following the policies and procedures. Encryption secures the files on the server and still allows sharing the files among users. The file Firewall ensures all the access requests follows the rules set by the administrator and existing infrastructure such as IDS and log management.ownCloud's Encryption adds modularity and flexibility into your overall encryption architecture. We need to manage the encryption keys in the key stores and to customize encryption to meet your specific regulatory and business needs.
- **Ransomware Protection:**Ransomware attacks are the trending and ever-present malware risk, both for large enterprises as well as for private users. Once the hard drives or parts of it are affected, it can become encrypted leading to unrecoverable data loss that directly refers to significant effort and cost. ownCloud Ransomware Protection App protects companies by blocking the uploaded files which are originated from ransomware to preserve original and uninfected files in ownCloud. Addition to that, the App can automatically block user accounts where ransomware was detected and also provides smart ways to restore infected files.

3. CLAMAVVS. AVAST CORE SECURITY

3.1 ClamAV

ClamAV is the best and widely referred antivirus in Linux. It is open-source and free to use. It is recognized as adaptable antivirus to detect trojans, malware and viruses. ClamAV also supports standard mail gateway scanning. It is easy to use and fast to run because it doesn't have a native GUI and works through the terminal.

Features:

- Open-source
- Free
- Cross-platform works in Linux, Windows and Mac OS
- Works from the terminal
- Support on-access scanning for mailing service
- POSIX compliant support
- Portable

3.2 Avast Core Security

Avast Core Security is one of the final choices as a Linux antivirus. This antivirus also came up among the best in the AV-Test. It works with both Ubuntu and Linux 32-bit and 64-bit software architecture. This antivirus supports core security, network security and also provides file server security.

Features:

- Real-Time Protection and anti-spyware
- On-demand scanning and planned scanning function
- Core security, network security
- Home and industrial safety
- The regular update for assuring new threat

4. CONCLUSION

To conclude, this paper titled “Securing own Cloud from Malicious File Uploads using ClamAV” which has been developed using Ubuntu. This project helps us to prevent malicious files from getting into the cloud server by filtering them at the time of upload, which provides Easy implementation and Generates report flexibly. Thus the project entitled above should include all the above-mentioned features and it is confirmed that it is up to the specifications entitled for the project.

Key features of this application:

It can secure own Cloud from malicious file uploads using ClamAV Antivirus.
Threats which can be prevented from uploading are:

- Trojans
- Viruses
- Malware

5. REFERENCES

[1]https://doc.owncloud.org/server/9.0/admin_manual/configuration_server/antivirus_configuration.html

[2]http://www.cdgcloud.com/cloud/core/doc/admin/configuration/server/antivirus_configuration.html

[3]https://linuxtechlab.com/install-clamav-clamtk-linux/

[4]https://www.quora.com/topic/ClamAV?q=clamav

[5]https://www.clamav.net/