Quest Journals
Journal of Software Engineering and Simulation
Volume 7 ~ Issue 12 (2021) pp: 26-37
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Virtualization Framework for Mitigating Client to Client Attacks in Cloud Computing.

O. Sarjiyus[1] and S. Vintenaba[2]
Department of Computer science Adamawa state university, mubi Nigeria.

ABSTRACT
This research titled "Virtualization framework for mitigating client to client attack in cloud computing" is aimed at identifying the security challenges in cloud computing with a view to developing a framework that has the capacity to minimize numerous security challenges that affect the efficiency of cloud computing services. As currency is based on building virtualization technology so that it can secure large scale cloud-based environment with limited security; malicious tendencies lead attackers to penetrate virtualization technologies that endanger the infrastructure, and then enabling attackers' access to other virtual machines running on the same vulnerable devices. The research revealed and discussed security issues such as DDoS and coordinated attacks that can allow infected virtual machine to penetrate hypervisor and steal sensitive and vulnerable data from resources. Various security issues were identified and discussion made on them, Virtualization as the block for cloud computing, its vulnerabilities and security issues were identified. Hypervisor and its security challenges was not left out. Mitigating techniques such as intrusion detection systems (IDS) were used to secure cloud-based systems. The existing system was analyzed and its various challenges were identified, and the proposed model was suggested, that is the introduction of the "intrusion Detection system" (IDS) to be used for mitigating the security challenges of the cloud environment. Modelling tools such as sequence diagram were used to model system functionalities in the design of the new system. The method of data collection employed for this research is the secondary method. The proposed system was designed and tested and found to meet all basic the specifications.

KEY WORDS: *Attacks, cloud-based, hypervisor, virtual, vulnerable.*

***R**eceived 08 Dec, 2021; **R**evised 21 Dec, 2021; **A**ccepted 23 Dec, 2021 © The author(s) 2021.*
P**ublished with open access at **www.questjournals.org

I. INTRODUCTION

Distributed computing is a way of choosing certain Internet services. The mindset to run different virtual machines (VMs) over separate piece of hardware through virtualization is an important innovation which makes cloud possibilities. Grid computing entails different features that give it interesting results, at times these elements raise security concerns as Grid clients fully know of these issues and strive effortlessly to ensure they are fixed. Distributed computing entails 3 unique administrations [1]: SaaS (software as a service), PaaS (platform as a service) IaaS (infrastructure as a service) models. Most of these models have their safety concerns. I-SaaS software or service in their cloud climate, or request from an Amazon partners to obtain them. Thus, it may be hard for clients to ensure what they need is a measure of well-being. Customer information is held by SaaS suppliers or can be hosted over general foreign cloud. Although, the information can be removed along with the information or other SaaS service disconnected from applications identified with other customers.

In addition, each information can be replicated in different areas in different urban communities, especially in other countries that ensure high abundance of arrangements. From now on, there are likely to be information weaknesses and application crashes. In this model, customers need more data to understand how their information is stored, and furthermore, they have no control over it. ii-PaaS safety Issues: In PaaS (some of them are the designers of such situation), at the highest point of the stage is some of the application build controls. Generally, PaaS is more adaptable than SaaS and raises safety issues. It can take advantage of security weaknesses in your application code to put your software in danger. iii-IaaS Safety Issues: IaaS entails different safety concerns which depends on the cloud model and area (general, single, crossbreed, local area). General clouds are deemed to high risk and single clouds seem to exhibit less safety challenges. As the cloud information community passes through various outsider framework gadgets, the information may be manipulated by the attacker's foundation. Also, the revealed safety of the cloud framework is vital and each damage can temper with climate of the complete virtual device. [2] Virtualization is an important part of the innovation of distributed computing. Though, it drives to many safety issues. Another significant safety issue is the host device itself is entirely disconnected, and it has not been completely accomplished in present day safety plans. Virtualization changes tools by implementing visible tools below or assigning private VM between two distinct hosts [3] The innovation of Virtual Machine Monitor (VMM) is definitely given as Hypervisor which gives many attributes, the most valuable that is useful separation and capacity to transfer and transfer information , [4] Balance responsibility and avoid critical mistakes. In any case, this leads to increased security concerns and issues arising due to this turn of events. The framework exists to access the equipment and fill in as a supplier to enhance the working framework, but it does not provide security. After that, security issues had to be considered, and the arrangement looked for a huge range in which numerous security weaknesses were found in virtual conditions, including isolation weaknesses. Similarly, virtualization programming has a weakness that has been weakened by malicious clients. For example, a programmer took advantage of a weakness in a PC to execute illegal code. The value of virtualization in the tendency of safety issues and faults presented by virtual community [4]. Location of weaknesses and guarantees from attacks are one of the basic efforts to achieve a computer experience, as these attacks can lead to data breaches.

The problem is getting virtual gadgets. There, hacking an isolated real host can give the programmer admittance to the information stored on the virtual server [5]. As a result, virtualization innovations have created fresh safety issues. Roughly 70% of cloud buyers acknowledge that safety concern is one of their problems. The objective issues at the board stage of IaaS's main free source cloud are Eucalyptus, OpenNebula, Radiance, CloudStack and OpenStack. For those who don't want to take advantage of the business cloud, these activities offer other important options. Open source arrangements are powerless when it comes to documentation and confirmation. Because hypervisors utilize a variety of structures, hypervisors are used, but only device-based virtualization is used. Linux-based hypervisor programming. XEN and KVM (partial virtual machines) rely on the free source modules of Linux, and the XEN hypervisor PV is used in areas that rely on discrete maintenance; in order to monitor and manage virtual devices, and through the client, which can aggregate virtual devices. KVM is a simple free source module, suitable for making use of most of the elements of Linux. It can give an extremely powerful environment for virtual device and cloud management. The cloud expert organization is executing the VM provided by the client, and there is no information about the visitor's operating system. Although distributed computing gives easy and multiple advantages, it also brings multiple disadvantages and dangers to the processing framework. This in-depth review evaluates all perspectives that can impact the security of a distributed computing environment and ensure that information is stored through cloud infrastructure. Our commitment to this research is as follows:

a. Grouping attacks in the cloud.

b. View safety concerns and track answers to address the weaknesses of distributed computing virtual machines.

c. Go to the length of security to secure the cloud environment. [6]

II. REVIEW OF RELATED WORKS

Recently, security concerns about distributed computers have received extensive attention and some specialists have looked at safety concerns in the virtualization layer. In a virtualized world, the hypervisor or virtual machine screen pulls other VMs back from the other gadget. Most of the shortcomings of virtualization contains extraordinary at the cloud stage and flow processes can barely fix them step-by-step. A major problem with virtualization security is the VMM. VMM is a product module that controls the association of all virtual devices with their equipment. The VMM is essentially responsible for monitoring and disconnecting each running VM, as well as creating and processing each virtual asset. Countless attack vectors can stimulate the complexity of the interconnect, and VMM focuses on more sections [6]. [7] recommended a proof method recognizable by KVM-based rootkits that leveraged virtualization innovations. Wojtkowiak [8] has uncovered 259 new virtualization weaknesses and new types of attacks (hyperjacking, hypervisor escapes, VM attacks, etc.) over the last five years. [4] broke XEN and KVM (parts-based virtual machine) insurance and showed the weaknesses of the hypervisor. [9] provided top-to-bottom weakness reports associated with codebase investigations of two regular open source hypervisors (XEN and KVM). [9] proposed a sequence of management program weaknesses, including three aspects: trigger source, attack vector and attack target. [10] Talked about the security of distributed computing, and ensured that the virtual machine-side transfer can be used to delete the encrypted private keys used by other virtual machines in similar situations. Security issues in the cloud virtualization part, such as hypervisors, virtual machines, and visitor circle pictures are identified by [11], [4]

III. METHODOLOGY

iii.i Existing system

There are a few models and devices to improve security and forestall assaults on software, information stockpiles, server farms and any equipment or programming assets. Firewalls and Antiviruses have been generally used to shield the servers and customers from assailants and any unapproved gets to. In any case, shockingly utilizing these two methodologies are insufficient and it brings about the interest for one more device and consequently urged specialists to foster an application which is called an interruption recognition framework (IDS). Interruption location frameworks have been utilized to recognize gatecrashers and assaults. It is characterized in classifications. Host-based Interruption Location Framework (HIDS), Organization Interruption Identification Framework (NIDS), Dispersed Interruption Discovery Framework (DIDS) which is generally utilized in appropriated frameworks, and Mixture Interruption Recognition Framework which can be blends of any of them. Interruption recognition framework has been isolated into two methods irregularity discovery and abuse identification. Abuse recognition utilizes a mark base which comprises of known assaults marks or examples to assess and coordinate with every similitude of the practices with the recorded marks. In the mean time, inconsistency recognition has been proposed to distinguish obscure assaults utilizing learning methods.

In this Part we talk about a few techniques proposed for keeping the cloud from assaults and gatecrashers, zeroing in on the mix of Virtual Machines (VMs) and interruption identification framework. Distinctive explores have been conveyed on accessible cloud virtualization which acquired new methodologies too. Cloud clients and suppliers have their own arrangement of center security necessities, as displayed in Table 1.

Table 1: Requirements for cloud security monitoring.

Requirement	Definition
Effectiveness	The objective goal of safety in cloud is effectively avoid and prevent accessibility and hack
Precision	Systems are required to enhance its accuracy in terms of detection attacks with minimum false-positive and false-negative rates
Transparency	The safety model needs to have minimum visibility from cloud service provider, developers, and service users and intruders sight
Non-Subvertability	The cloud host and physical layer in addition to VMs must be guarded against compromised service users with infeasibility to suspending the alarm system
Deployability	The system must be possible to be implemented over various accessible cloud framework
Dynamic reaction	System must be able to employ impressive techniques to defeat attacks intrusion with minimal effect on legitimate process and functionalities
Accountability	Security system must not affect the cloud's core functionality and applications, while it must log cloud activities to enable accountability

Host apparatuses are productive and incredible in observing host frameworks for identifying and forestalling assaults, despite the fact that it is undeniably challenging to distinguish new assaults (for example polymorphism and transformation). Moreover, it can conservative comparative alarms and recognize all the more inconsistency practices in connecting cautions coming from heterogeneous stages. Through characterization, preparing, highlight extraction, and meta-learning, an information mining calculation is used to recognize and hail malevolent assaults with VMM-IDS in virtualized server application to work with the executives and disconnection of VMs. VMM improves the intangibility of the interruption discovery framework and it very well may be utilized as a safeguard to keep away from the interruption identification frameworks from being distinguished and compromised, particularly HIDSs.

Moreover, not just fostering the VMM-IDS is a lot simpler, yet in addition HIDS and NIDS can be joined to partake in the benefits the two of them. For this situation, it is feasible to distinguish obscure and notable assaults also. They could expand the precision rate with a low level of bogus alerts.

iii.ii Model of the Existing System

In this Stage, a few techniques proposed for keeping the cloud from assaults and interlopers, zeroing in on the mix of Virtual Machines (VMs) and interruption identification framework. Interruption discovery frameworks have been proposed to identify gatecrashers and assaults. It is grouped in classifications. Host-based Interruption Discovery Framework (HIDS), Organization Interruption Location Framework (NIDS), Dispersed Interruption Recognition Framework (DIDS) which is broadly utilized in circulated frameworks, and Half breed Interruption Identification Framework which can be mixes of any of them. Interruption identification framework has been partitioned into two procedures irregularity location and abuse discovery. Abuse identification utilizes a mark base which comprises of known assaults marks or examples to assess and coordinate with every likeness of the practices with the recorded marks. In the interim, oddity discovery has been proposed to distinguish obscure assaults utilizing learning strategies.

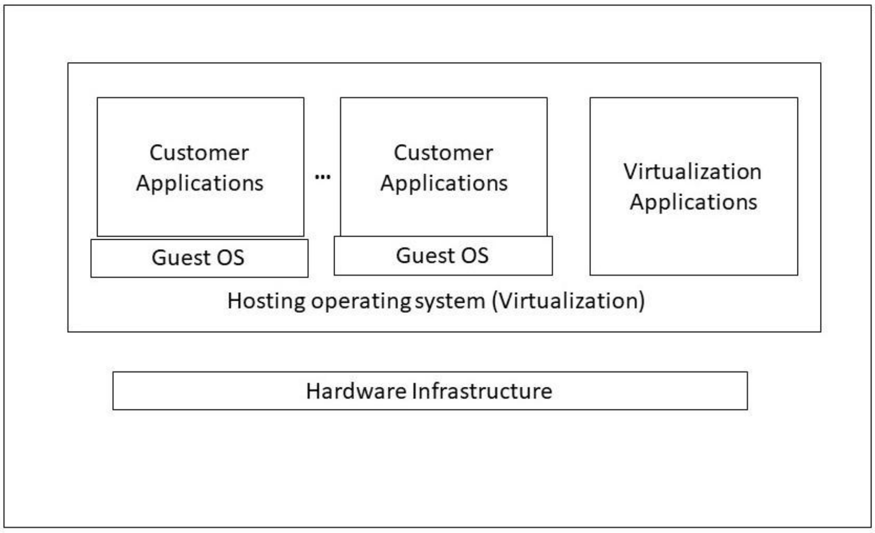


Figure 3.1: operating system-based virtualization.

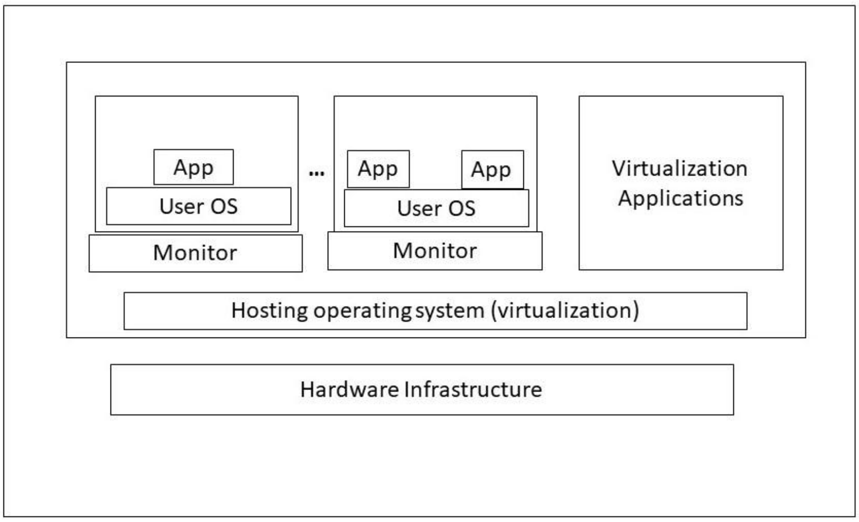

App
User OS
Monitor
...
App
App
User OS
Monitor
Virtualization Applications
Hosting operating system (virtualization)
Hardware Infrastructure

Figure 3.2: Application-based virtualization.h

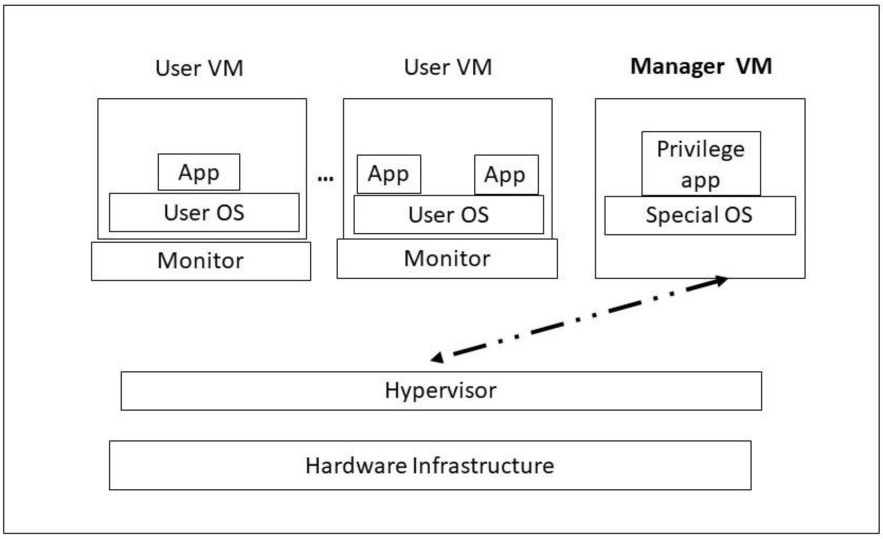


Figure 3.3: Hypervisor-based virtualization.

iii.iii Challenges of the Existing System

In the mean time, it is actually the case that organization-based apparatuses are not awesome for observing, distinguishing and keeping the host framework from the assaults, yet it is working emphatically in obstruction against the assaults. Customary interruption identification framework can only with significant effort manage new assaults, like DDoS, and composed assaults. The instrument proposed in endeavors to defeat the weaknesses of conventional IDSs for disseminated frameworks and distributed computing conditions to accelerate the reaction time, identifying, and catching of new dangers and interruptions, consequently diminishing bogus cautions. In the interim, clearly zero-day assault marks or examples are excluded from the information base, and in this way, the mark base should be update as often as possible. To address this shortcoming, oddity identification has been proposed to distinguish obscure assaults utilizing learning procedures. One of the disadvantages of peculiarity identification strategy is the more huge bogus positive rate when contrasted with abuse recognition. Interruption discovery framework becomes essential in giving recognition of interlopers and assaults. Since cloud is broadly available from everywhere the organization for inside clients and outer ones, it is dire to utilize interruption identification framework to distinguish potential assaults and added to the assurance instrument of the cloud.

In ordinary virtualization, since the virtualization activities communicate straightforwardly with VMM on the Host operating system, controlling the progressive of the VMMs are restricted. SVL model gives appropriate construction to build the security to the most elevated opportunities for virtualization. All in all, in light of the fact that the apportioned assets to the virtualization are self-virtualized, and the chance of getting to them by unapproved client is limited. Moreover, DDoS assault from inward cloud is confined, and every one of the deals between the VMs are controllable like controlling deals with actual layer. Cloud suppliers have critical controls in IaaS also. Utilizing reasonable response instrument at assault time, it dodges the chance of assaults and accordingly defeats the circulation of the interruptions. In the mean time dependent on the sharp response, since all typical cycles are copied and shadowed utilizing the Copy Processor and VM-Shadow, they won't end. Despite the fact that SVL model has high intricacy particularly in execution, it can adapt against the information spillage, DDoS assault, just as unapproved client access. As far as we could possibly know, there is no comparable model carried out; it is expected that SVL model can resolve the previously mentioned issues.

iii.iv Design of the improved system

In this stage, the utilitarian determination are utilized for making an interpretation of the model into a plan of the plan framework. An unmistakable depiction of the multitude of necessities use for the plan of the genuine answer for the issue will be introduced.

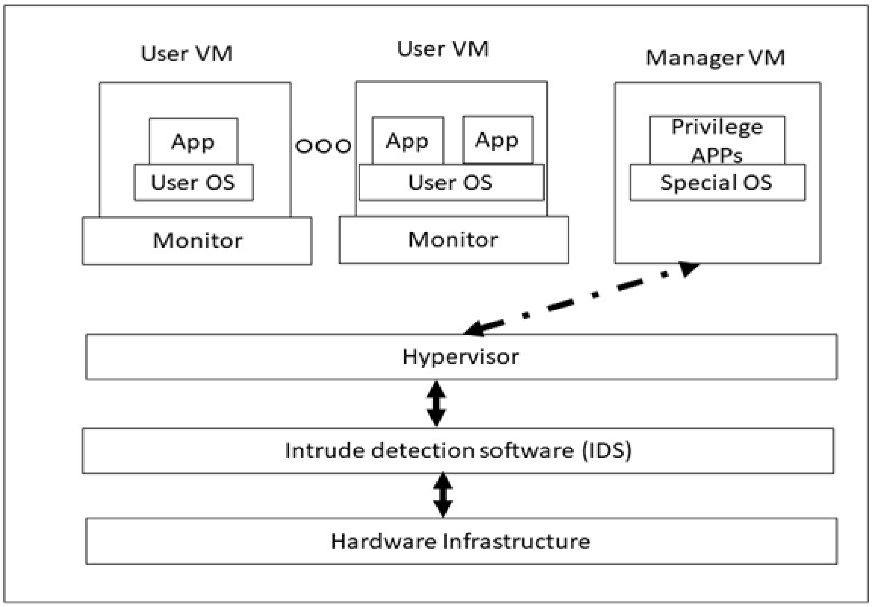


Figure 3.4: Operating system based Virtualization model

a. *Operating system-based virtualization:* In this methodology, Virtualization is empowered by a facilitating working framework that upholds various detached and virtualized visitor operating system on a solitary actual server with this trademark that all are on a similar working framework bit with has control on Equipment foundation Only. The facilitating working framework has perceivability and command over the VMs. This methodology is basic however it has weaknesses. For instance, an assailant can infuse portion scripts in facilitating working framework and this can cause all visitor operating system need to run their operating system on this part. The outcome is aggressor have command over all VMs that exist or will build up in future. Be that as it may, with the presentation of the IDS the aggressors will be identified and keep from assaulting VM in every one of the models proposed.

b. *Application-based virtualization:* An application-put together virtualization is facilitated with respect to top of the facilitating working framework. This virtualization strategy imitates each VM which contains its own visitor working framework and related applications. This virtualization engineering isn't regularly utilized in business conditions. Security issues of this methodology are like Working framework based.

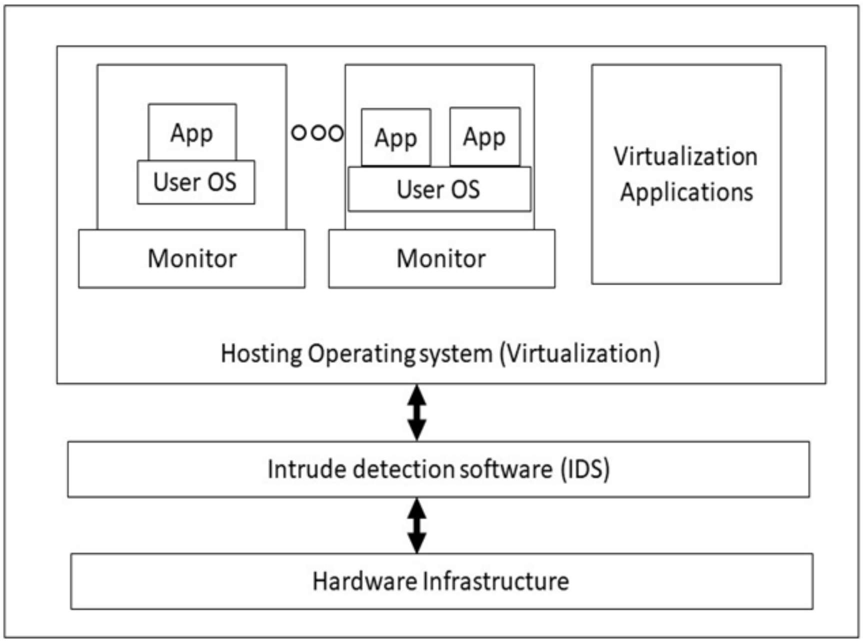

App
User OS
OOO
App
App
User OS
Virtualization Applications
Monitor
Monitor
Hosting Operating system (Virtualization)
Intrude detection software (IDS)
Hardware Infrastructure

Figure. 3.5: Application-based Virtualization model

c. *Hypervisor-based virtualization:* As referenced previously, a hypervisor is installed in the equipment foundation or the facilitating working framework piece. The Hypervisor is accessible at the booting season of machine to control the sharing of framework assets across different VMs. A portion of these VMs are special segments that they dealt with the virtualization stage and facilitated VMs. In this engineering, the advantaged parts have perceivability and command over the VMs. This methodology build up most controllable climate and can play out extra security instruments, for example, Interruption identification frameworks. Be that as it may, it was powerless due to the hypervisor is weak link. Assuming hypervisor slammed or assailant oversees it, all VMs are on the aggressor control. Notwithstanding, assume responsibility for hypervisor from VM level is troublesome however not feasible.

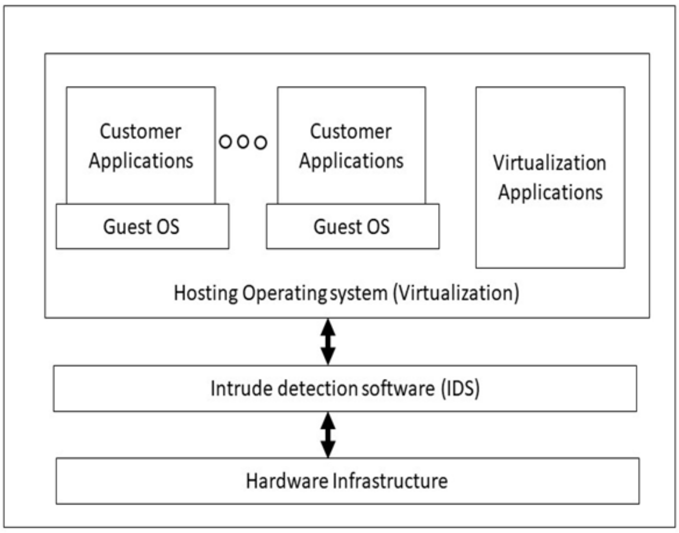
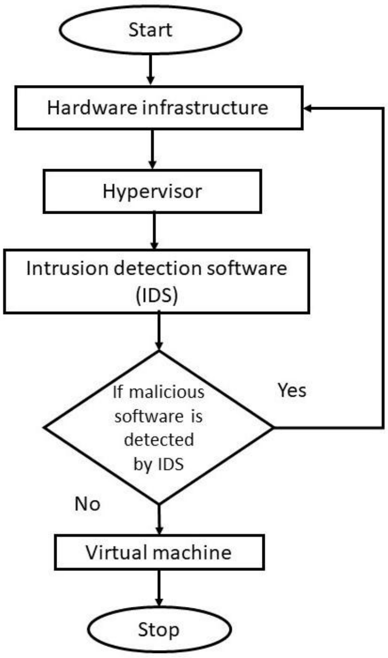

Customer Applications
Customer Applications
Virtualization Applications
Guest OS
Guest OS
Hosting Operating system (Virtualization)
Intrude detection software (IDS)
Hardware Infrastructure

Figure 3.6: Hypervisor based Virtualization model

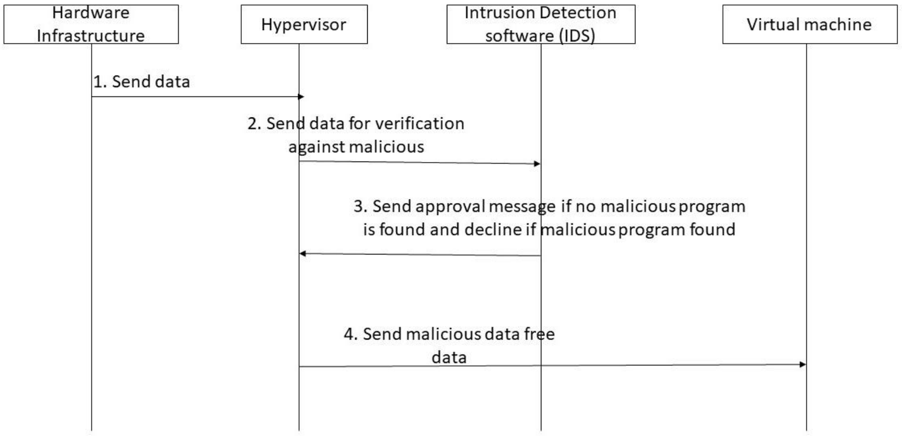
iii.v Strengths of the new (improved) system

The proposed framework if execute will enjoy benefits, for example, the programmers exercises will be observed by the interruption decoction framework (IDS) and be kept from approach or command over the virtual machines. What's more, the confined IP address will likewise keep unapproved client from approaching the server.

Flowchart


Start
Hardware infrastructure
Hypervisor
Intrusion detection software (IDS)
If malicious software is detected by IDS
Yes
No
Virtual machine
Stop

Sequence diagram


Hardware Infrastructure
Hypervisor
Intrusion Detection software (IDS)
Virtual machine
1. Send data
2. Send data for verification against malicious
3. Send approval message if no malicious program is found and decline if malicious program found
4. Send malicious data free data

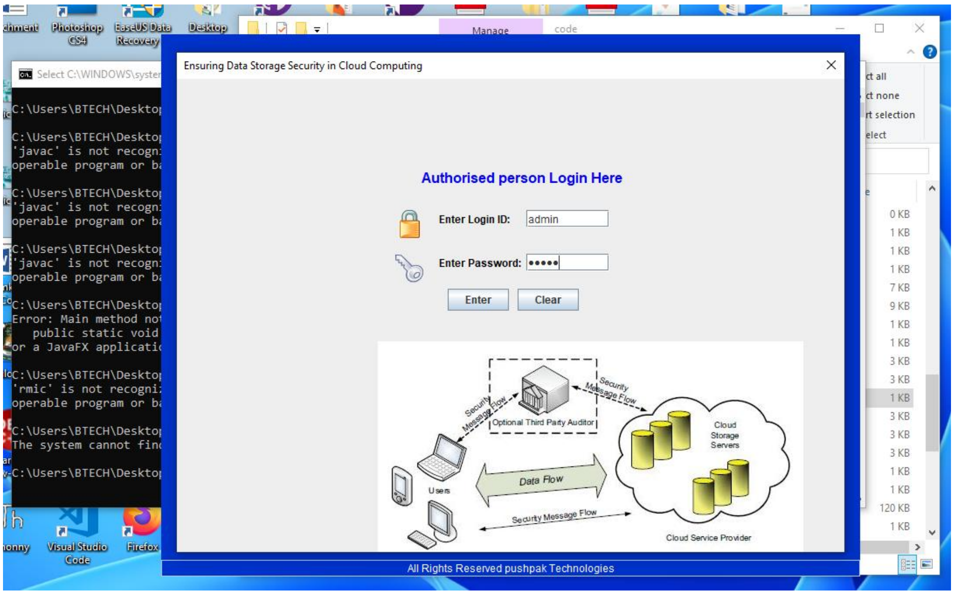
iii.vi Materials and methods

This proposed model uses different sorts of instruments and gear in various layers of safety. Each of the necessities in PC organizations can be utilized in this model as indicated by the size of the cloud framework. In other word on the grounds that the establishment of cloud is based on the Web which is the greatest organization all through the world every one of the offices and apparatuses that utilized in the organization, hence switches and switches can be utilized in this climate. Anyway the essential foundation of this model just spotlights on virtualized climate instruments.

These days the majority of the cloud climate utilizes VMware to virtualize their framework assets like stockpiles. In this specific proposed model scientist utilizes the reenactment assessment for testing and carrying out. Every one of the devices and recreation programming are run in VMware8.0 climate on a Dell PC with the elements, for example, Intel® center ™ i5 Focal handling unit (computer chip) M460 and 2.53GHz processor, 4.00 GB interior memory Irregular Access memory (Smash) and 64bit working framework. The greater part of the customers' working framework is Windows 7 which is the normal working framework for distributed computing inhabitants. All of the Microsoft strategy control center and firewalls, for example, ISA server utilized as the observing and strategy supervisors in this proposed model.

IV. RESULTS

In this level or section of the project work the proposed system designed will be complete and fully integrated and be validated and evaluated to ensure the aim of the study is achieved. The designed system was fully integrated and tested as implemented in the implementation level below.



```
C:\Users\BTECH\Deskto

C:\Users\BTECH\Deskto
'javac' is not recogn
operable program or b

C:\Users\BTECH\Deskto
'javac' is not recogn
operable program or b

C:\Users\BTECH\Deskto
'javac' is not recogn
operable program or b

C:\Users\BTECH\Deskto
Error: Main method no
   public static void
or a JavaFX applicati

C:\Users\BTECH\Deskto
'rmic' is not recogni
operable program or b

C:\Users\BTECH\Deskto
The system cannot fin

C:\Users\BTECH\Deskto
```

Ensuring Data Storage Security in Cloud Computing

Authorised person Login Here

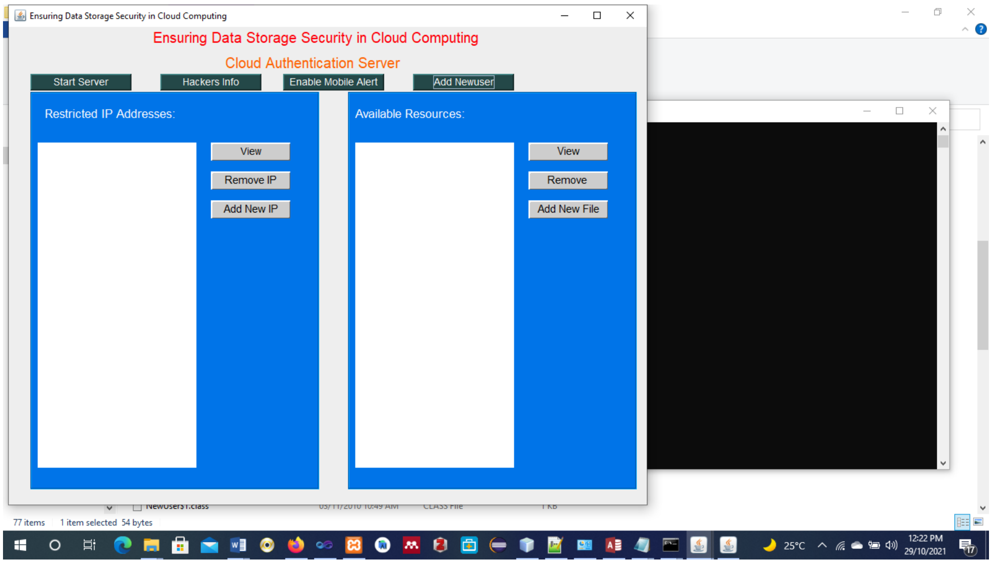
Enter Login ID: admin

Enter Password: •••••

All Rights Reserved pushpak Technologies

Figure 4.1: Authorized person Login

This design provide means for user to enter the authentication information in the space provided it is implemented as seen in the screen shot above, the system will take you to the Menu environment which is the cloud authentication server model.

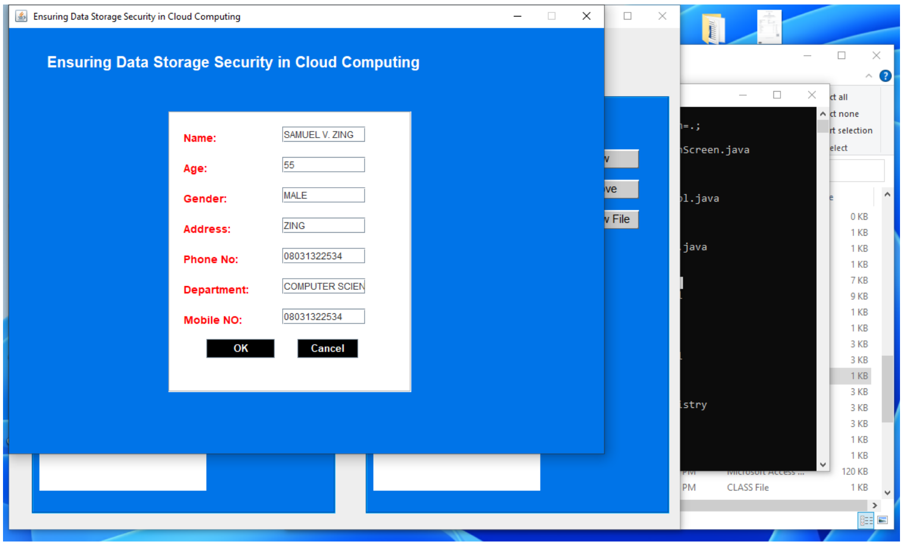


Ensuring Data Storage Security in Cloud Computing

Cloud Authentication Server

Figure 4.2: Cloud authentication server

This interface has three (3) basic areas that is the menu area, restricted IP address area, and available resources area. Where selection are made based on demand by the user. Add a new user was selected as demonstration and below screen was displayed to add new user (VMs).The new user was added as a tenant on the cloud computing environment.



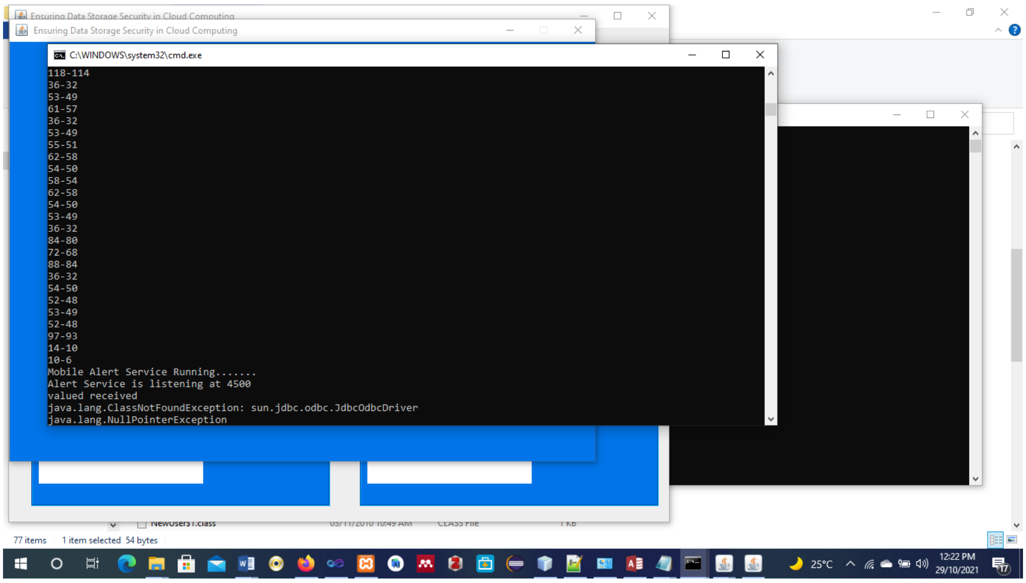
Ensuring Data Storage Security in Cloud Computing

Ensuring Data Storage Security in Cloud Computing

Name:	SAMUEL V. ZING
Age:	55
Gender:	MALE
Address:	ZING
Phone No:	08031322534
Department:	COMPUTER SCIEN
Mobile NO:	08031322534

Figure. 4.3: Add new user

A new user was added and information regarding the user identification is presented as seen in the spaces provided for the new user. The interface has two buttons, that is the OK button and the Cancel button. On the process of adding a new user, you may change your mind not to add the user, the click cancel to terminate the action.

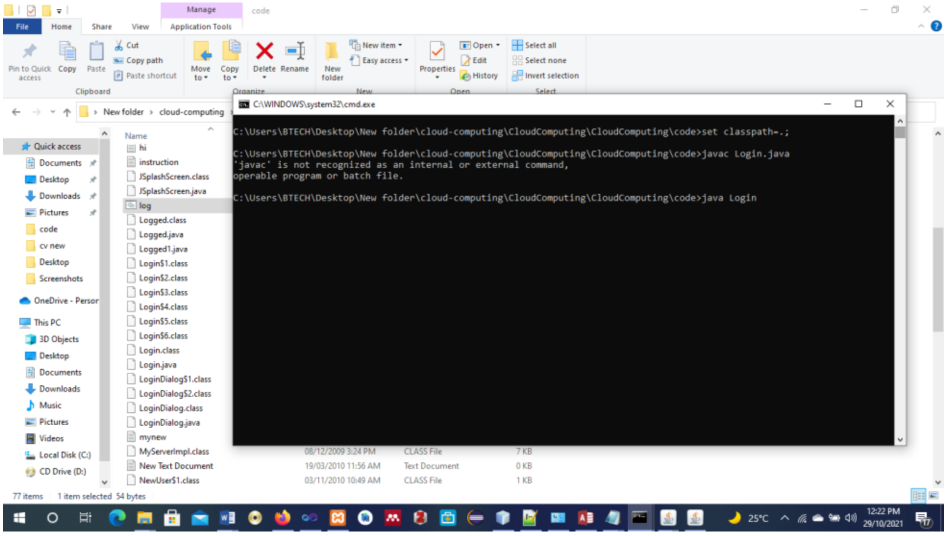


C:\WINDOWS\system32\cmd.exe

```
118-114
36-32
53-49
61-57
36-32
53-49
55-51
62-58
54-50
58-54
62-58
54-50
53-49
36-32
84-80
72-68
88-84
36-32
54-50
52-48
53-49
52-48
97-93
14-10
10-6
Mobile Alert Service Running.......
Alert Service is listening at 4500
valued received
java.lang.ClassNotFoundException: sun.jdbc.odbc.JdbcOdbcDriver
java.lang.NullPointerException
```

Figure 4.4: Information screen

The interface above shows the necessary information regarding the new user added as well as any attempt by a hacker to infect the host server with malicious program. It also monitors the server against any security threats, and if any threat is found, the intrusion Detection System Neutralizes the attack and protect the server from being infected by the malicious program.



```
C:\Users\BTECH\Desktop\New folder\cloud-computing\CloudComputing\CloudComputing\code>set classpath=.;

C:\Users\BTECH\Desktop\New folder\cloud-computing\CloudComputing\CloudComputing\code>javac Login.java
'javac' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\BTECH\Desktop\New folder\cloud-computing\CloudComputing\CloudComputing\code>java Login
```

Figure 4.5: Idle screen model

The idle screen is similar to Figure.4.4, this screen appears when the information screen is not active. This shows that the server is not active and there is no any attempt by hackers to infect the server with any malicious program.

iv.i Discussion

In recent times cloud computing security concerns have attracted broad attention, and several researchers have researched various security issues in the virtualization layer. This work provides a scientific value to the community by reviewing, structuring and categorizing all the found security issues of virtualization in the cloud computing environment. The new system which is aimed at developing a framework to mitigate the security threats on the cloud computing environment was designed and implemented. A login interface is provided for the authorize user to enter the login ID and Password as a measure to avoid unauthorized user access to the system. The cloud authentication server is provided which has areas such as Menu, Restricted ID, and the Available Resource areas. In the menu area a means is made available for addition of new user on the server. Provision was also

Made for the monitoring of the server and display of information about the activities of the server. Intrusion Detection system (IDS) becomes vital in providing detection of intruders and hackers

Since cloud is widely accessible from all over the network for internal users and external ones, it is urgent to use intrusion detection system to detect possible attackers and contribute to the mechanism of the cloud.

V. CONCLUSION

In this overview, a great deal of insights concerning the virtualization framework have been introduced for distributed computing which implies that it acquires its security issues. In spite of the fact that, virtualization is an old model, it plays an essential part with current programming design and equipment. The strategies identified with virtualization were contemplated, particularly, the security issues identified with the combination of present day projects and gadgets. Virtualization for some, clients permits virtual server sharing for this to be a significant focal point of distributed computing clients. The presence of various virtualization procedures is another test on the grounds that each kind requirements distinctive security instruments. A few assaults target virtual organizations or virtual machine screens, particularly when speaking with VMs from a distance.

This concentrate additionally centers around assaults and weaknesses that are imperative to comprehend, assisting associations with embracing distributed computing. Understanding and recognizing security issues and weaknesses adds to making the framework all the more impressive and can alleviate assaults coming about because of framework weaknesses. Current security arrangements and countermeasures that add to the avoidance or relief of these assaults have likewise been recorded. Here, novel security arrangements are required what's more, old style arrangements that have been created and may not function admirably in view of the intricacy of cloud conditions.

At last, virtualization can be viewed as a blade that cuts both ways, thus, it should be managed cautiously, particularly, on the security side. Virtualization improves programming responsibility and security detachment and gives security elements to accessibility, classification and uprightness, if security arrangements are carried out well.

REFERENCES

[1]. Alameri I, Radchenko G (2017) Development of student information management system based on cloud computing platform. Journal of Applied Computer Science & Mathematics 11:9-14. https://doi.org/10.4316/JACSM.201702001 and Communications (ICDIPC2013)

[2]. Sosinsky B. (2011) Cloud computing bible. https://doi.org/10. 1145/358438.349303

[3]. Zhu G, Yin Y, Chai R, Li K (2017) Detecting virtualization specific vulnerabilities in cloud computing.

[4]. Pearce M, Zeadally S, Hunt R (2013). Virtualization: issues, security threats, and solutions. ACM Computing Survey 45(2):17:117:39https://doi.org/10.1145/2431211.243121. Programming Based on Virtualization Techniques,‖ Security and Communication Networks, 6(10), 2013, pp. 1236–1249.

[5]. Yilek, S., (2010). Resettable public-key encryption: How to encrypt on a virtual machine. Proceedings of the International Conference on Cryptographers Track at the RSA, March 1-5, 2010, Springer, Berlin, Germany, ISBN:978-3-642-11924-8, pp: 41-56.

[6]. Wu J, Lei Z, Chen S, Shen W (2017) An access control model for preventing virtual

[7]. Zhang Y, Juels A, Oprea A, Reiter M (2011), Homealone: Coresidency

[8]. Subashini, S. & Kavitha V., (2016). A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications. doi:10.1016/j.jnca.2010.07.006

[9]. Perez-Botero, D., J. Szefer and R.B. Lee, 2013. Characterizing hypervisor vulnerabilities in cloud computing servers. Proceedings of the 2013 International Workshop on Security in Cloud Computing, May 8, 2013, ACM, Hangzhou, China, ISBN:978-1-4503-2067-2, pp: 3-10.

[10]. Moyo T, Bhogal J, (2014) Investigating security issues in cloud computing. In: Eighth International Conference on Complex, Intelligent and Software Intensive Systems, Birmingham, pp. 141 – 146. http://doi.org/10.1109/CISIS.2014.21

[11]. Kazim M, & Zhu SY (2015) Virtualization security in cloud computing. In: Zhu S, Hill R, Trovati M (eds) Guide to security assurance for cloud computing. Computer communications and networks. Springer, Cham. https://doi.org/10.1007/978-3-31925988-8