A Novel VM Hardening Policy for Enhancing VM Security under Cross-Virtualization Platform

Golam Mostafa [1], Ananta Uzir [2], Nirmalya Mukhopadhyay [3]

[1]Dept. of Computer Science and Engineering, Assam Downtown University, Assam, India
[2]Dept. of Computer Science and Engineering, Assam Downtown University, Assam, India
[3]Assistant Professor, Dept. of Computer Science and Engineering, Assam Downtown University, Assam, India

---***---

ABSTRACT: To reduce IT expenses while boosting efficiency and agility for all size businesses the most of the organizations use virtualization technique. In simple words Virtualization is the technique of splitting a physical resource into as many logical resources we want or we can say that it is a technology that transforms hardware into software. It is the single most effective way. So, securing virtual machines in a virtualized environment is equally important as securing physical servers. By hardening the VMs we can secure the Virtual Machines. Vulnerabilities in virtual machine is crucial because virtualization eases many aspects of IT management. Weaknesses in virtual machine can be treats such as VM sprawl, Hyper jacking, VM escaping, Denial of services, etc. Since VMs are increasingly seen as a legacy technology, malicious VM can do whatever it wants. Early detection of vulnerabilities in virtualization is very important for virtualization and to protect against malicious attacks that cause to information leak. Now, there are many tools are there which can detect commons flows in software implementation, but many of the virtualization vulnerabilities are unique that can hardly address by existing techniques. This abstraction means that a virtual machine can be harden so that it makes less vulnerable to data breaches. In this research paper we conducted analyses of some vulnerabilities. Based on the vulnerabilities, we propose frameworks to these vulnerabilities for the virtual platforms which can find detect the bugs in virtualization and also, we give solutions to harden the VMs.

Key words: VM Hardening, Virtualization Security, Cloud Computing, Multi-tenancy.

INTRODUCTION

Cloud computing is a fast-growing computing technology that has been adopting by maximum IT organizations. Virtualization is the core computing technology in cloud computing. Virtualization enables the dynamic allocation and modifications of multiple Virtual machines with one physical host machine. Virtualization uses software to create an abstraction layer over computer hardware that allows the hardware elements of a single computer or simply virtual machines.

A Virtual Machine is a compute resource that uses software instead of a physical computer to run programs and deploy apps. It is virtualization/emulation of a physical computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementation may involve specialized hardware, software, or a combination. Virtual machines allow you to run an operating system in an app window on your desktop that behaves like a full, separate computer. The main purpose of VMs is to operate multiple operating systems at the same time, from the same piece of hardware. Without virtualization or Virtual Machines, operating multiple systems like Windows and Linux would require two separate physical units. Because applications run based on specific OS capabilities, Businesses that use a wide array of applications might find themselves deploying many different consoles and hardware installations to manage their apps. This can become unwieldy and expensive. Hardware requires physical space that isn't always available. Hardware also requires plenty of upkeep costs, repair costs when hardware fails, maintenance costs to make sure your hardware stays in shape and energy costs for power and cooling. Virtualization keeps costs down by placing all your OSs into a cloud-like structure, with multiple instances running on the same underlying, local hardware- which eliminates the need for hardware accumulation and excessive overhead.

The host VMs requires a hypervisor (specialized software). The hypervisor emulates the computer's CPU, memory, hard disk, network and other hardware resources that can be allocated to the VMs according to their requirements. So, VM is a very crucial technology much important, security in Virtual Machine is equally important. Virtual Machine hardening is reducing its vulnerability, which is larger when a system creates more virtual machines; in principle a single function virtual system is more secure than a multipurpose one. Reducing available ways of attack on virtual machines is the main purpose of VM Hardening.VM Hardening provides a secure computing platform and having a secure platform there is very less possibility of unwanted access, through which we can perform our computational tasks and store our data without any fear of losing them.

In this research paper, we offer a detailed analysis of VM configuration file to assess vulnerabilities inside the file. Once the vulnerabilities are detected, they have been resolved using specified threat prevention security protocols. We have designed one framework that will mitigate the threat holes that are identified. Finally, we enlisted some recommendations that can be deployed to achieve the secure virtualization implementation. So, the entire research purpose is to harden the VMs and enhance the overall security measures of a virtualized system.

LITERATURE SURVEY

Virtualization is such a fast-growing technology that lets one to easily create adjuvant IT services using resources which are traditionally cramped to device hardware. It allows one to utilize a physical system over all capacity by split into many clients or environment. By adding various benefits, there are lots of security issues and aspects arise with the growing consumers that should be mitigated. One should first research and analyze the existing issues that are obstructing the whole process to meet the optimal amenities and then step to alleviate those. Considering this purpose, we have studied and examined various researches to brainchild a framework to mitigate such issues that are conferred below.

The primary paper we have considered is "VM2: Automated Security Configuration and Testing Virtual Machine Images " was published by Gururaj Ramachandra et. all [1] in 2020. This paper proposed to a Virtual Machine (VM) by solidifying the diagram or picture of the Virtual Machine. Commonly, VMs are made from purported VM pictures, a sort of outline used to arrange and make a VM. In any case, to make a VM picture physically may be very tedious, particularly if the VM needs to meet certain security benchmarks. In this paper, they introduced VM2 (Virtual Machine Candy machine), an apparatus for making of VM pictures and testing them. Security benchmarks just as simple sharing the safe pictures. Their examination exhibited a huge decrease in security issues in solidified pictures made by VM2 in correlation with the relating pictures financially offered by Centre for Internet Security (CIS). In this paper they introduced VM2 (Virtual Machine Candy machine) apparatus that makes VM pictures dependent on clients' inclinations, tests these pictures with respect to security benchmarks and gives usefulness to simple offer the safe pictures.

Next paper we have contemplated is “Hardening Hypervisors against Vulnerabilities in Instruction Emulation” published by Kenta Ishiguro et. all [2] in 2018. This paper proposed to get a VM by solidifying hypervisors against weaknesses in guidance emulators. Weaknesses in the hypervisors are vital in multitenant cloud and alluring for the assailants on the grounds that a weakness in the hypervisor can subvert every one of the virtual machine’s security. This paper centers around weaknesses in guidance emulators are not uncommon; CVE-2017-2583, CVE-2016-9756, CVE-2015-0239, CVE-2014-3647, to give some examples. For In reverse similarity with heritage x86 CPU's, traditional hypervisors copy self-assertive guidelines whenever of mentioned. This plan prompts an enormous assault surface, making it difficult to get and of weaknesses in the emulator. This paper proposes FWinst that limits the assault surface against weaknesses in the emulator. The vital knowledge behind FWinst in that the emulator ought to imitate just a little subset of guidelines, contingent upon the fundamental computer chip miniature engineering and the hypervisor design. FWinst perceives copies settings in which the directions emulator is included, and distinguishes an authentic subset of guidelines that are permitted to be imitated in the current setting.

Our next considered paper was "Virtualization Vulnerabilities, Security Issues and Solutions, A Critical Study and Comparison" published by Darsnak Tank et. all [3] on 11 March in 2019. In their article, a new extensive overview on virtualization dangers and weaknesses are introduced. They additionally portrayed scientific classification of cloud-put together assaults with respect to the virtualized frameworks and existing guard component planned to help the scholarly community, industry and analysts to acquire further and significant bits of knowledge into the assaults so the related weaknesses can be recognized and along these lines required moves would be made. They give a comprehensive examination of different methods proposed by analysts to determine virtualization explicit weaknesses. This paper has investigated the basic dangers that exist in a cloud-based climate from both the cloud specialist co-ops and clients viewpoints that ought to be dealt with while purchasing or conveying administrations in cloud for guaranteeing undeniable degree of safety towards driving or logical assaults. This paper gives a premise to comprehend issues identified with virtualization security.

In the next phase we have studied a paper called “Increasing Windows Security by Hardening PC Configurations” published by Pablo Martin Lamora et. all [4] in 2019. This paper depicts that the specialized decisions and design includes and talks about the viability of the solidify PC approach. The PC solidifying setup has demonstrated that a halfway overseen security arrangement functions admirably for clients who don't need full organization capacities on their laptops, permitting clients to play out their obligations in a safer climate without influencing their work propensities. The appropriation of the task has been extremely sure and the solidify PC setup has been set up as the norm for new computers and establishments in divisions, for example, Account OR HR. The significant accomplishment of the undertaking lied in the foundation of a favorable place for security includes that have been subsequently embraced by all Windows laptops at European Council for Nuclear Research (CERN). The exertions keep on presenting new highlights and increment the appropriation of the setup to another office.

On the other hand, the paper we have studied was "Security Issues in Cloud Computing and their Solutions: A Review" published by Sabiyyah Sabir et. all [5] in 2018. In this paper, they gave the outline of distributed computing, its different security angles and keys factors which are influencing the cloud security alongside its various advantages. In this examination, different security issues with respect to information protection and unwavering quality, Key variables which are influencing the distributed computing, have been tended to and furthermore ideas on specific regions have been talked about. Distributed computing is a web based, arising innovation, will in general be winning in our current circumstance particularly software engineering and data innovation fields which require network figuring for huge scope. Distributed computing is a common pool of administrations which is acquiring prominence because of its expense viability, accessibility and extraordinary creation.

Next paper we have contemplated is “Cloud Computing and Security Issues” published by Rohan Jathanna et. all [6] in 2017. In this paper, they have featured the issues identified with distributed computing. Distributed computing has gotten quite possibly the most intriguing subjects with regards to the IT world today. Cloud model of processing a s an asset has changed the scene of figuring as it guarantees of expanded more noteworthy dependability, monstrous adaptability and diminished expenses have drawn in organizations and people like. It adds abilities to data advancements. Distributed computing is another idea that presents a lot of advantages its clients. However, it additionally raises some security issues which may influence its use understanding about the weaknesses existing in cloud figuring will assist associations with making the shift towards utilizing the cloud. In this paper, they have introduced security issues for cloud models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) which vary contingent upon the model. As depicted in this paper, stockpiling and organizations are the greatest security worries in distributed computing.

After that we have examined a paper named "Study of Security Issues in Cloud Computing" published by Varsha et. all [7] in 2015. In this paper, they research and complete a little report and feature every one of the issues of arising over a cloud identified with security of Cloud. The significant pressure of their examination dependent on existing writing is to comprehend the idea of multi-occupancy security issue. As we as a whole realize Distributed computing is an arising area and security of the information should be ensured over the organization. There are some security issues happening while at the same time utilizing administrations over the cloud. Distributed computing is a monstrous possibility both for the organizations and the assailants – the two players have the option to have their own prize from distributed computing. A boundless potential outcome of distributed computing can't be concealed distinctly for the security issues reason – the ceaseless examination and exploration for vigorous, ordinary and incorporated security models for distributed computing may be the lone way of motivation. In light of this reality that the effect of safety issues in distributed computing can be decline by multi-occupancy engineering.

Our next deliberated paper was "Virtualization Security" published by Abhinav Mishra et. all [8] in

2016. In this paper, they examined about the security issues and counter proportions of virtualization and Hypervisor and its design. Virtualization accompanies its own benefits and difficulties. As it conceals actual qualities of the assets and the idea of epitome comes into picture. Hypervisor based design requires less equipment assets and can impart all the more productively. All significant players have acquainted their hypervisor-based arrangement with the virtualization. One of the difficulties accompanies it is the virtualization security.

Next paper we have examined is "Data Security in Cloud Computing" published by Ahmed Albugmi et. all [9] in 2016. This paper talks about the security of information in distributed computing. It is an investigation of information in the cloud and angles identified with it concerning security. In this paper, they have examined about information insurance techniques and approaches utilized all through the world to guarantee greatest information security by diminishing dangers and dangers. Accessibility of information in the cloud is helpful for some applications however it presents chances by presenting information to applications which may as of now have security escape clauses in them. Additionally, utilization of virtualization for distributed computing may chance information when a visitor operating system is run over a hypervisor without knowing the unwavering quality of the visitor operating system which may have a security proviso in it. The paper will likewise give an understanding on information security angles for Information On the way.

Next paper we have considered is "Virtualization Security Issues and Mitigations in Cloud Computing" published by Ramakrishna S et, all [10] in 2017. In this paper, they have introduced different security issues identified with hypervisor in cloud. This paper additionally carried the issues conceivable with a malignant virtual machine running over hypervisor, for example, misusing a larger number of assets than designated by VM, taking delicate information by bypassing disconnection of VM through side channel assaults, permitting assaults to bargain hypervisor. In this paper, they additionally have brought safety efforts or prerequisites to be taken and models that are required by hypervisor to deal with different security concerns. Virtualization empower distributed computing worked with a few visitors VMS to share regular actual equipment. Hypervisor is the vital segment in virtualization. Subsequently it should oppose assault successfully by disconnecting VMS. However, truly it is defenseless and presented to a few security laws, for example, VM escape. It is supposed to be the most genuine among a few assaults said previously. A got away from VM will bargain a few co-occupants VMS. A few compositional and configuration changes are required in Hypervisor for expected opposition of VM get away from assault. Side channel assaults commandeer framework assets and take delicate information of co-inhabitant VMS. A few arrangements were examined in moderation of side channel assaults as adding commotion, and so on Hypervisor security empowers security to the cloud climate which brings about trust building and undertakings inspiration of movement to cloud.

Next paper we have considered is "Cloud Computing: Study of Security Issues and Research Challenges" published by Adnaan Arbaaz Ahmed et. all [12] in 2018. This examination paper presents an audit on the distributed computing ideas just as security issues characteristic inside the setting of distributed computing and cloud framework. This paper likewise dissects the key examination and difficulties that presents in distributed computing and offers best practices to specialist co-ops just as undertakings wanting to use cloud administration to improve their main concern in this serious financial environment and lift up its utilization. There are some security issues sneaking in while utilizing administrations over the cloud. Distributed computing has colossal possibilities, yet with equivalent number of safety dangers. One of the greatest security stresses with the distributed computing model is the multi-occupancy. The primary accentuation of this paper dependent on existing writing and to comprehend the idea of multi-occupancy security issue.

Next paper we have considered is "Virtualization Technologies and Cloud Security: advantages, Issues and Perspectives" published by Roberto Di Pietro et. all [13] in 2018 The goal of this paper is to reveal insight into mutt lease virtualization innovation and its development according to the perspective of safety, having as a target its applications to the Cloud setting. Virtualization is at the core of Distributed computing. Yet more lightweight methodologies, for example, Containerization and Uni-kernels exist, equipment upheld separation mechanisms give valuable in a wide range of situations where security prerequisites are significant. By the by, security weaknesses are as yet a significant issue, as featured by as of late found adventures. Improved virtualization approaches and more compelling separation and checking advances, that can likewise use extra figuring re-wellsprings of late computer processors and Graphics Processing Unit (GPU)s, are as yet in their outset. Such advances, combined with suitable programming partners, will perhaps improve the uprightness and security of assets in Cloud, worker ranches, and in versatile situations.

Next paper we have contemplated is "Virtualization-Based Security Techniques on Mobile Cloud Computing: Research Gaps and Challenges" published by Boubakeur Annane et. all [11] in 2019. In this paper, they have examined the primary difficulties in regards to the security and protection issues in portable cloud precisely zeroing in on the virtualization issue layer and give clear qualities and shortcomings of late significant virtualization security methods existing in the writing. To explain, the client slight virtual machines speak with one another to trade private and touchy data (for example questioned application executed in the distinctive host). They have contemplated the impediments of most existing virtualization security co-area methods proposed in the writing. Therefore, they have recognized that the primary impediment is the shortfall of securing touchy data traded between versatile application's undertakings sent on various VMs on the cloud.

Next paper we have examined is "A Taxonomy of Virtualization Security Issues in Cloud Computing Environment" published by Khalil Al-Shqeerat et. all [14] in 2019. In this paper they distinguished the fundamental difficulties and security issues of virtualization in distributed computing conditions. which audits the lightening procedures for improving the security of cloud virtualization frameworks. Besides, they find and investigate the compelling alleviation methods that are utilized to ensure, secure, and oversee virtualization conditions. They recognized Thirty weaknesses, clarified, and grouped into six proposed classes. Besides, fifteen principal virtualization dangers and assaults are characterized by misused weaknesses in a cloud climate.

Cloud service providers has to meet and mitigate various type of attacks from it's beginning. One of the considerable and sophisticated form of attack is Cross – VM Cache Side Channel attack. To get better understanding of this attack we studied a paper called "Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable" published by Abid Shahzad et. all [15] in 2015. In this paper they tended to explicit worries for the administration of secure processing in a Distributed computing climate. Which presents the after effects of a methodical audit of variables identifying with cross-VM store side channel assaults and counter measures to forestall assaults or moderate effective interruptions.

Cloud is something that is fully dependent on internet and that's why it should counter the security challenges. Including resources and other services are provides through the internet so why to protect these components we need know understand the infrastructure first. On behalf of this concern, we analyzed a paper " Analyzing Security Threats to Virtual Machines Monitor in Cloud Computing Environment " published by Ahmad Fayez S. Althobaiti et. all [16] December 7, 2016. In this paper the creator centers around security of virtual assets in Virtual Cloud Computing Infrastructure (VCCI), Virtual Machine Screen Virtual Machine Monitor (VMM) by portraying kinds of assaults on VCCI, and weaknesses of VMMs and we depict the strategies for getting a VCCI.

When we take the services from the cloud, we assume that these come with correct security settings and never bother to check or update those. To know these security aspects, we have studied a paper “Leveraging Virtual Machine Introspection for Hot-Hardening of Arbitrary Cloud-User Applications" published by Sebastian Biedermann et. all [17]in 2014. In this paper they propose a design that can consequently and straightforwardly improve security settings of self-assertive organization applications in a distributed computing arrangement. Clients can send virtual machines with various applications, and the framework will endeavor to discover and test better security settings customized towards their particular arrangement.

Security issues are becoming a headache for cloud users' day by day. To know from where these attacks are going on, we should first know the infrastructure of the cloud computing and the paper we have studied for this is “Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures" published by Sarfraz Nawaz Brohi et. all [18]. This exploration paper centres around distinguishing and breaking down the security issues and dangers on VCCI. They depict the procedures of virtualizing a Cloud Confidence Index (CCI), sorts of assaults on VCCI, weaknesses of VMMs and we basically portray the meaning of safety devices and methods for getting a VCCI.

There are various types o attacks are going on since the virtualization technique is made its level of use at high. Some attacks are non-distinguishable like rollback attack. This topic has become a hot topic so why we have examined a paper named "Defending against VM Rollback Attack" published by Yubin Xia et. all [19] in 2014. In this paper, they propose an answer for shield VM rollback assault, without forfeiting ordinary functionalities gave by hypervisor. The arrangement depends on the perception that the end client is the one in particular who can tell if a rollback is pernicious. Thus, they can safely log all the rollback exercises of VM. By reviewing the log, a client can either check dubious rollbacks and request that the cloud administrator demonstrate the need of such tasks, or compel the procedure on a VM by characterize rollback strategy ahead of time, or both. The arrangement additionally needs insignificant client association.

The use of cloud computing is at its high point so why the risk as well. With this security aspects a survey paper is released called “A Comprehensive Survey on Security in Cloud Computing" and published by Gururaj Ramachandra et. all [20] in 2017. This report gives an examination of the situation with virtualization security in Cloud Computing. They present current endeavors, arising best practices and realized security holes, examining the effect the last have on conditions dependent on virtualization innovations. It additionally gives the premise to get issues and difficulties identified with virtualization security, just as a conversation on normal prescribed procedures for security assurance in virtualized conditions and holes that should be filled in to execute a protected virtualized climate.

METHODOLOGY

We are taking a VM sample code snipped and we will analyze this code to find out the different vulnerability points.

VM Configuration File

VM or Virtual Machine Configuration file is the file which contains the information of the virtual machine settings, memory, network, Mac address, Hard Disk Drive, Hardware Version and other information related to the VM Configuration.

We have taken a sample VM Configuration code for our analysis that is given below:

```
<domain>
<domain type = “KVM”>
<name>alice</name>
<uuid>61a813ba-3c4c-11e4-b048-
005056a85388</uuid>
<memory>1047856</memory>
<current memory>1047856</current memory>
<vcpu>1</vcpu>
<05>
        <type>hvm</type>
        <boot dev = “cdrom”/>
</05>
<features>
        <acpi/>
</features>
<clock offset = “utc”/>
<on – power off> destroy </on – power off>
<on- reboot> restart </on - reboot>
<on - crash> destroy </on - crash>
<devices>
        <emulator>/users/bin/kvm</emulator>
        <disk type = “file” device = “disk”>
                <drivername = “queue” type = “raw”/>
                <sourcefile = “/home/lamw/alice.ing”
                />
                <target dev = = “vda” bus = “virtio”/>
                <address type = “pci” domain =
                “0*0000” bus = “0*00” slot = “0*04”
                function = “0*0”/>
        </disk>
        <disk type = “file” device = “cdrom”>
        <driver name = “queue” type = “raw”/>
        <source file = “/home/lamw/ubuntu-14.04.1-
        desktop-amd64.iso”/>
        <target dev = “hdc” bus = “ide”/>
        <readonly/>
        <address type = “drive” controller = “0” bus =
        “1” target = “0” unit = “0”/>
        </disk>
        <controller type = “ide” index = “0”>
                <address type = “pci” domain =
                “0*0000” bus = “0*000” slot = “0*01”
                function = “0*1”/>
        </controller>
        <interface type = “bridge”>
                <mac address = “52:54: aa:00: fa:51”/>
                <source bridge = “br0”/>
        <interface/>
        <input type = “mouse” bus = “ps2”/>
        <graphics type = “vnc” port = “-1” autoport =
        “yes”
        Listen = “172.30.0.207”/>
</devics>
</domain>
```

We have assessed this sample code that resides in a Virtualization Configuration File. While assessing those codes, we have found some vulnerability points that an attacker can use for malicious activities like attacking other Virtual Machines present in the host. We have assessed each line of code separately so that we can find out the maximum number of possibilities that an attacker can use to attack a client in the host. So, we have broken up the whole code into parts and presented as vulnerability points as following:

(1) Assessing UUID of a VM in a VM Configuration File (Mentioned in above Code)

"<uuid>61a813ba-3c4c-11e4-b048-005056a85388</uuid>"

In the above code that has marked as red is the first vulnerability point, we have found during our assessment. This point is called Universal Unique ID or uuid. An attacker can mask an uuid of any client in the host to use in their malicious activities. In the above code we have assessed that an attacker can mask a user unique id in the host and can use that to their malicious activities like attacking another Virtual Machine present in the host. In simple words, if a malicious or non-malicious user is using the identity of any other user for hiding her own identity, then this activity can be termed as masking. It's extremely useful for hijacking nodes in an open system.

(2) Assessing "memory" of a VM in a VM Configuration File (Mentioned in above Code)

<memory>1047856</memory>

The next vulnerability point that we have found during our assessment is "memory" or memory size that has marked in the above code. Attackers can use the value of the tag "current memory" (i.e., C800:5H) as a vulnerability by modifying the allocated and unallocated memory size. If a client is allocated 50% of total memory of his system and remaining 50% is unallocated then the attackers can modify the memory allocation by changing to 100% and that unallocated 50% memory will be stolen and be used by the hackers unknowingly.

(3) Assessing memory address or location of a VM in a VM Configuration File (Mentioned in above Code)

<current memory>C800:5</current memory>

When the memory size becomes vulnerable, there one more vulnerability arises that memory address or location. The code that we have analyzed for this vulnerability is highlighted above. An attacker can change the address or location of the memory of a Virtual Machine in the host and due to this the client may suffer from the loss of his data or information. We all know that the data stored in the memory is stored with a specific address or location and there exist a link in between the data and the memory address or location. If the address of the memory changed the link between the previously stored data and the existing address gets break and then the data may be lost. For these reasons we have spotted this portion of the code as the vulnerability point.

(4) Assessing Virtual CPU or VCPU of a VM in a VM Configuration File (Mentioned in above Code)

<vcpu>1</vcpu>

All the processes and the tasks done in a system with the help of VCPU (Virtual Centralized Processing Unit) in a Virtual Machine. Code of this vulnerability point is given above.

So, the next vulnerability point that we have analyzed is VCPU. In the above code we can clearly see that the client assigned 1 VCPU for his system. Here the attackers can modify the number of VCPU assigned to steal the unassigned VCPUs and utilize all the VCPUs present client's system. As a result, the processes running in the client machine will be hampered or may be destroyed.

(5) Assessing "cdrom" of a VM in a VM Configuration File (Mentioned in above Code)

<boot dev = "cdrom"/>

The next vulnerability point that we have found throughout our assessment is "cdrom". "cdrom" is the location from where the Operating System (OS) starts its booting process. In this case, the attacker modifies the location of the code and sets her own malicious system code. As a result, the code will follow the path of attacker's malicious OS and original OS will be replaced. Once the malicious OS is placed in the client machine, she can install lots of malicious software, viruses, and worms with the effected OS. Thus, the whole physical or virtual machine will be corrupted and the attacker will gain full access of the client machine. Then the attacker can do lots of malicious activities like stealing information, occupying unallocated memory, CPU and corrupt the whole network also.

(6) Assessing "destroy" of a VM in a VM Configuration File (Mentioned in above Code)

```
<on – power off> destroy </on – power off>
```

In the process of rebooting or power-off, there one more vulnerability arises that is highlighted in the above code. Power-off is the process of destroying or closing all the tasks running in CPUs, RAM and hard disk drives by removing the power supply from them. Here in the code <on – power off> destroy </on – power off>, "destroy" is the vulnerable point. The word "destroy" instructs the system to destroy or remove the power supply from all the components running in the system. But attackers can modify the code by changing the word "destroy" to "pause" or "sleep" and the system will go to sleep mode and pause all the processes running in the system instead of destroying. Next time whenever the attacker wants to turn the malicious activities, she does not need to reboot the system again. Instead, she just needs to awake the machine from sleep mode or pause mode.

(7) Assessing "Address/location of emulator" of a VM in a VM Configuration File (Mentioned in above Code)

```
"<emulator>/users/bin/kvm</emulator>"
```

One of the major components that is used in virtualization is emulator. Emulator is a software or hardware program that enables one computer system (Host System) to imitate the functions of another computer system (Guest System). Emulator enables the host system to run software, peripheral devices, tools and other components which are designed for the guest operating system. In the code <emulator>/users/bin/kvm</emulator>, the highlighted part (i.e/users/bin/kvm) is the vulnerable point. This code indicates the location of the emulator from where it will be installed in the client system. The attackers change this location with their malicious emulator's location to be installed in client machine. When the malicious emulator gets installed in the client system, the whole control of the VM goes to attackers' hand and they can perform any malicious task including the hardware resources.

(8) Assessing "Address /location" of a VM in a VM Configuration File (Mentioned in above Code)

```
<source file = "/home/lamw/ubuntu-14.04.1-desktop-amd64.iso"/>
```

This vulnerability is same as the emulator vulnerability. The location of the source file can be changed by the attackers and exchanged by their own malicious iso file's location. When the client wants to install the iso file the attacker's malicious iso file will be installed. As a result, they will get all the controls over the Operating system and can do any kind of malicious activity like installing malicious software, viruses, worms, stealing information, memory, CPU etc.

(9) Assessing "MAC Address" of a VM in a VM Configuration File (Mentioned above as Code1)

```
<mac address = "52:54: aa:00: fa:51"/>
```

MAC address is also known as Media access control address is a unique identifier assigned to a System NIC (Network Interface Controller) for use a network address in communication. Virtual Machine has such kind of facility that it can be transported anywhere by using Mac Address. This facility has become the vulnerable point for virtualization since the Mac Address can be changed by the attackers. If the attacker changes the Mac address with their malicious system's MAC Address, then the host will also be changed. That means, the attacker's malicious system will be the host then and the client system will be divested from his all the tasks and processes. Then the client will not be able to run his own Virtual Machine in his system.

(10) Assessing "Mac Address" of a VM in a VM Configuration File (Mentioned in above Code)

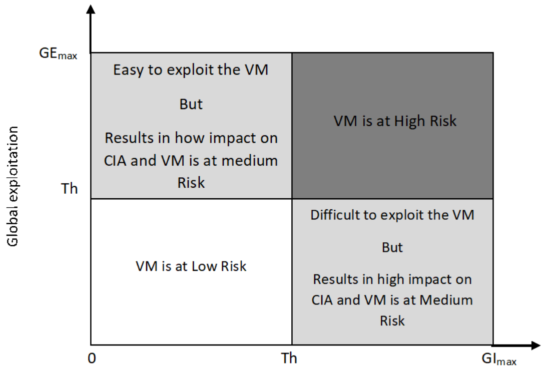
```
<graphics type = "vnc" port = "-1" autoport = "yes"
        Listen = "172.30.0.207"/>
```

The next vulnerability point that we have found while we assessing the configuration file code is "listen". Listen is a Restful API command that handles some kind operations like socket connection, port connection etc. With listen command one IP address is used which signifies to establish the communication with that IP address only. Here the attacker can change the IP address with their malicious system IP address and can establish a connection with the client system. After getting connected with the client system, they can use this port as a backdoor for their malicious activities.

These are some vulnerable points that we have found during our assessment. We have explained all the vulnerable points above and after assessing these vulnerabilities, we have proposed some mitigation framework.

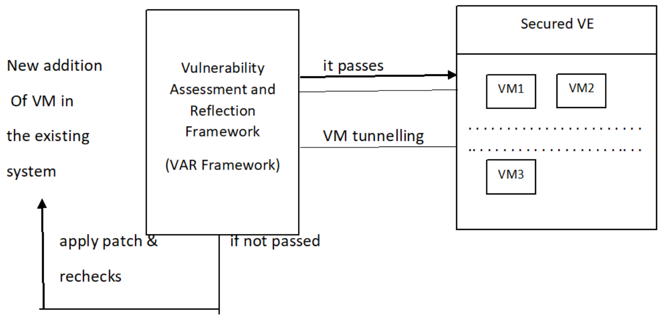
After finding these vulnerability points throughout our assessment, we have proposed some mitigation techniques and frameworks. We have tried to consider the maximum possibilities to mitigate the vulnerabilities which we discussed above. Our approach is providing some frameworks and algorithms to counter the existing problems in VM Configuration file.

The first framework that we have defined is Global Impact:


GE$_{max}$
Th
Global exploitation
Easy to exploit the VM
But
Results in how impact on CIA and VM is at medium Risk
VM is at High Risk
VM is at Low Risk
Difficult to exploit the VM
But
Results in high impact on CIA and VM is at Medium Risk
0
Th
GI$_{max}$

When the global exploitation and global impact reach the "Th" level then the VM remains at low risk. When global exploitation reaches maximum, the global impact remains at the "Th" level. Then the VM becomes easy to exploit but it results in how impact on CIA and VM is at medium risk. When global impact reaches maximum and global exploitation reaches "Th" then the VM becomes difficult to exploit but it results in high impact on CIA and the VM is at medium risk. When both the global impact and the global exploitation reach maximum then the VM remains at high risk.

The Second framework that we have proposed is Vulnerability Assessment and Reflection Framework or VAR framework:



Abstract model of proposed solution

VAR Framework

$$Risk=\begin{cases} High, & if\ (GE > Th\ and\ GI > Th)\\ Medium, & if\ (GE \le Th\ and\ GI \ge Th)\ or\\ & (GE \ge Th\ and\ GI \le Th)\\ \longrightarrow & \\ Low & otherwise \end{cases}$$

Vulnerability assessment and reflection refers to the process of identifying risks and vulnerabilities in virtual machine. Our proposed Vulnerability Assessment and Reflection Framework (VAR Framework) shows how it provides security to the virtual machines. Actually, it acts as a vulnerability scanner tool. When users try to add new VM in the existing system, the VAR Framework checks the system whether is malicious or not. That means, VAR Framework will assess and rectify the vulnerabilities. After checking and assessing the vulnerabilities, the new VMs are allowed to enter the existing secured Virtual Environment (VE).

Following are the assessments and strategies that we are following to implement our defined framework.

Vulnerability Assessment: Finding the influences of the VM vulnerabilities once they've been discovered is a huge challenge. One of the biggest drawbacks of existing vulnerability databases is that they do not include information on cloud infrastructure, which is required to determine the total exploitability, impact, and risk level of VMs. As a result, vulnerability attributes such as exploitability, impact, and exploit likelihood position can be used to extract this information. Each vulnerability is examined in terms of the source of potential exploitation. To determine the severity level of a vulnerability, we calculate the exploit likelihood class, vulnerability exploit rate, and vulnerability impact rate for each vulnerability.

Vulnerability Exploit Likelihood Class: The likelihood of a vulnerability being exploited is calculated by taking into account the attacker's privileges and network connectivity. To exploit the vulnerability, it is assumed that an attacker has particular privileges on the cloud infrastructure. It also takes into account the level of difficulty and user engagement required to exploit the flaw. We map found vulnerabilities to three classifications, namely virtual network, internal network, and external network, which correspond to cloud network infrastructures, using a likelihood estimate. It examines the vulnerability and the exploitability parameters associated with it and determines the cloud network infrastructure from which the vulnerability is most likely to be exploited.

We utilise CVSS V.2 for vulnerability evaluation because it covers all vulnerabilities discovered to date, whereas CVSS V.3 includes vulnerabilities released after June 2015. The CVSS vector in NVD defines the seven-base metrics for qualitative vulnerability assessments. These seven indicators are divided into two categories: exploitability measurements and impact measures.

The complexity of gaining access to the target VM is defined by the access metric. Attack Vector (AV), Attack Complexity (AC), and Authentication (Au) are three sub-metrics. The attacker's ability to exploit the vulnerability without requiring physical access to the VM is defined by AV. The amount of effort necessary to exploit the vulnerability in order to attack the target VM is represented by AC. The number of times an attacker is authenticated to a target for the purpose of exploiting a vulnerability is shown in Au.

Confidentiality Impact (CI), Integrity Impact (II), and Availability Impact (AI) are three sub-metrics in the impact metrics (AI). The impact of a successfully exploited vulnerability on VM information leaking is presented in CI. The influence of the VM on information modification is shown in II, while the influence on VM resource accessibility is shown in AI.

Vulnerability Exploit Rate: Equation 1 shows how to calculate the vulnerability exploit score using NVD's established formula. The exploit score is a decent way to quantify vulnerability's exploitability; however, it ignores advanced exploit techniques or the availability of attack code for the related vulnerability. Exploit Code Maturity (ECM), an NVD metric, is used to characterize it. High (H), Functional (F), Unproven (U), and Not-defined (X) are the possible ECM metric values, with ECM numeric values (ECMNV) of 1.0, 0.97, 0.91, and 1.0, respectively. Equation 2 is used to determine the general exploit score (GES). The GES is a scale of one to ten that is used to determine the vulnerability exploit rate (VER). It is then mapped to the qualitative ratings as follows:

$$\text{Exploit\_score} = c1 * AC * Au * AV \quad (1)$$

$$GES = \text{Exploit\_score} * ECMNV \quad (2)$$

Vulnerability Impact Rate: The impact score is generated using a predetermined NVD algorithm as shown in equation 3 to evaluate the vulnerability impact on a VM. For CI, II, and AI, NVD defines three possible values: High, Low, and None, with values of 0.56, 0.22, and 0, respectively. The impact score is a useful tool for estimating the impact of vulnerability on a virtual machine. It does not, however, take into account the presence of a fix for the associated vulnerability.
If a patch is available, the cost of restoring the virtual machine after successful exploitation is lower. As indicated in equation 4, we analyze patch availability using a temporal metric called Remediation level (RL) and construct the cost associated impact score (CAIS). Unavailable (U), Temporary Fix (T), Official Fix (O), and Not-defined (X) are the potential values for the RL metric, with RL numeric values (RLNV) of 1.0, 0.96, 0.91, and 1.0, respectively. The CAIS is a one-to-ten scale that is translated to qualitative ratings to determine the vulnerability impact rate (VIR).

$$\text{Impact score} = c2 * (1 - (1 - CI) * (1 - I\,I) * (1 - AI)) \quad (3)$$

$$CAIS = \text{Impact\_score} * RLNV \quad (4)$$

Vulnerability Severity Level: It's vital to decide which vulnerabilities need to be repaired right away before implementing the updates. This decision might be made based on the vulnerability's severity level. Although certain methodologies for estimating severity levels are available, the infrastructure-wise chance of a given vulnerability must be considered. Based on their VIR, VER, and probability class, we create an algorithm to map vulnerabilities to distinct sternness levels. The algorithm takes ELC, VIR, and VER values as input for each vulnerability and translates the relevant vulnerability to a certain sternness level, as shown in the Algorithm below.

Algorithm: Vulnerability sternness level estimation.

Require: Exploit Probability Class, ELC; Vulnerability Influence Rate, VIR; Vulnerability Feat Rate, VER

Ensure: Vulnerability sternness level, VSL;

```
if ((ELC = VN or ELC = IN or ELC = EN) and VER =High and VIR = High) or (ELC = VN and VER= Medium and VIR = Medium) then
    VSL = High;
end if
if ((ELC = IN or ELC = EN) and ((VER = High and VIR = Medium) or (VER = Medium and VIR =High) or (VER = High and VIR = Low) or (VER = High and VIR = Low))) then
    VSL = Medium;
end if
if ((ELC = VN or ELC = IN or ELC = EN) and ((VER = Medium or VER = Low) and (VIR = Medium or VIR = Low))) then
    VSL = Low;
end if
```

VM Risk Analysis: The threat of a newly joined VM is determined by the number of unpatched vulnerabilities. This aids in prioritizing the VM for continuous monitoring in the event that many VMs are joined. When an unpatched vulnerability linked with the VM is exploited, risk is defined as the likelihood of an attack and its impact on the target VM. We use a Wooden Barrel Theory (Cask Theory) to determine global exploitability and impact, GE and GI, as indicated in equations 6 and 7. In equation 6, we take into account the vulnerability's exploit rate as well as the port.

Thus, the number of unpatched vulnerabilities with low, medium, and high VER is n1, n2, and n3, accordingly. Similarly, the total number of open ports with low, medium, and high PER are represented by m1, m2, and m3, respectively. The vulnerability's impact rate is taken into account in equation 7. The number of unpatched vulnerabilities with low, medium, and high VIR, respectively, is q1, q2, and q3.

$$\text{GE=max}\left\{\sum_{i=1}^{n1} GESi * \sum_{j=1}^{m1} PESj, \sum_{i=1}^{n2} GESi * \sum_{j=1}^{m2} PESj, \sum_{i=1}^{n3} GESi * \sum_{j=1}^{m3} PESj\right\} \quad (5)$$

$$\text{GI=max}\left\{\sum_{i=1}^{q1} CAISi, \sum_{i=1}^{q2} CAISi, \sum_{i=1}^{q3} CAISi\right\} \quad (6)$$

Vulnerability Patching: The proposed framework discovers security patches, applies them to VMs, and then checks the patch installation after the severe vulnerabilities in VMs have been found. It's an SSH-based service that transfers, installs, and keeps virtual machines up to date. Patching extremely dangerous flaws. Let S = (v1, v2, v3, ..., vm) be a set of m highly severe vulnerabilities in a virtual machine. The framework works in the following phases for each highly severe vulnerability in the set S:

Step 1 It takes the vulnerability's CVE number and matches it to a fix in the patch repository (PR). PR stores the most recent patches and is updated with advanced patches on a regular basis.

Step 2 It looks for the patch's availability. It establishes an SSH connection to the target VM and transfers the patch file from the host PC to the VM if patch is available.

Step 3 It deploys the patch to the target VM and restarts it (if required).

Step 4 Finally, it scans the same VM to ensure that the updates were installed correctly.

It changes the record of the related VM in VMD for patching information such as patched date and time, number of patched vulnerabilities, and patch duration after successful patching. A cloud security administrator receives the report on open ports. He or she makes the decision to block unused ports and modifies firewall rules to blacklist those ports.

RESULT & ANALYSIS

We proposed so me frameworks and mathematical models which help us to mitigate the VM security concerns. We performed the following analysis and we got the relevant results.

How we analyzed vulnerability exploit rate:

Following are the equations that are used to assess the vulnerability exploit rate,

$$\left.\begin{aligned} &\text{Exploit score} = c1 * AC * Au * AV && (1)\\ &\text{GES} = \text{Exploit score} * ECMNV && (2)\end{aligned}\right\}$$

In above two equations, equation 1 helps to calculate the vulnerability exploit score by using NVD's established formula. The vulnerability exploit score specifies the amount or quantity of vulnerability's exploitability; however, it neglects the advanced exploit techniques or the availability of attack code for the related vulnerability. Equation 2 is used to determine the general exploit score (GES). The GES is a scale of one to ten that is used to determine the vulnerability exploit rate (VER).

How we analyzed Vulnerability impact rate:

Following are the equations that are used to assess the vulnerability impact rate,

$$\text{Impact score} = c2 * (1 - (1 - CI) * (1 - I\,I) * (1 - AI)) \quad (3)$$

$$CAIS = \text{Impact score} * RLNV \quad (4)$$

The impact score is generated using a predetermined NVD algorithm as shown in equation 3 to evaluate the vulnerability impact on a VM. For CI, II, and AI, NVD defines three possible values: High, Low, and None, with values of 0.56, 0.22, and 0, respectively. The impact score is a useful tool for estimating the impact of vulnerability on a virtual machine. It does not, however, take into account the presence of a fix for the associated vulnerability.

If a patch is available, the cost of restoring the virtual machine after successful exploitation is lower. As indicated in equation 4, we analyze patch availability using a temporal metric called Remediation level (RL) and construct the cost associated impact score (CAIS).

How we analyzed VM risk analysis:

Following are the equations that are used to assess the VM risk:

$$GE=\max\left\{\sum_{i=1}^{n1} GESi * \sum_{j=1}^{m1} PESj, \sum_{i=1}^{n2} GESi * \sum_{j=1}^{m2} PESj, \sum_{i=1}^{n3} GESi * \sum_{j=1}^{m3} PESj\right\} \quad (5)$$

$$GI=\max\left\{\sum_{i=1}^{q1} CAISi, \sum_{i=1}^{q2} CAISi, \sum_{i=1}^{q3} CAISi\right\} \quad (6)$$

The threat of a newly joined VM is determined by the number of unpatched vulnerabilities. an unpatched vulnerability linked with the VM is exploited, risk is defined as the likelihood of an attack and its impact on the target VM. We use a Wooden Barrel Theory (Cask Theory) to determine global exploitability and impact, GE and GI, as indicated in equations 6 and 7. In equation 6, we take into account the vulnerability's exploit rate as well as the port.

Thus, the number of unpatched vulnerabilities with low, medium, and high VER is n1, n2, and n3, accordingly. Similarly, the total number of open ports with low, medium, and high PER are represented by m1, m2, and m3, respectively. The vulnerability's impact rate is taken into account in equation 7. The number of unpatched vulnerabilities with low, medium, and high VIR, respectively, is q1, q2, and q3.

Analyzing Vulnerability Security Level:

Using the following algorithms, we have assessed the security level of a VM. To assess the security level required some components like Exploit Probability Class, ELC, Vulnerability Influence Rate, Vir, Vulnerability Feat Rate, VER.
The algorithm used is as follows:

```
if ((ELC = VN or ELC = IN or ELC = EN) and VER =High and VIR = High) or (ELC = VN and VER= Medium and VIR = Medium) then
    VSL = High;
end if
if ((ELC = IN or ELC = EN) and ((VER = High and VIR = Medium) or (VER = Medium and VIR =High) or (VER = High and VIR = Low) or (VER = High and VIR = Low))) then
    VSL = Medium;
end if
if ((ELC = VN or ELC = IN or ELC = EN) and ((VER = Medium or VER = Low) and (VIR = Medium or VIR = Low))) then
    VSL = Low;
end if
```

CONCLUSIONS

VM hardening plays a vital role in providing a secured computing platform. Recently many researchers provided many ways to mitigate the vulnerabilities found in virtual machine configuration file. Here we have found some vulnerability in virtual machine configuration file and also, we have proposed some frameworks to mitigate those problems. Our main consideration was to assess the maximum number of vulnerabilities and propose their mitigation policies. In this research paper, we have defined some frameworks and mathematical algorithms to the problems we countered during our assessment.

ACKNOWLEDGEMENT

In all respects doing of this research paper, we have received a distinguish assistance and clinch. We would like to applaud and appreciate our mentor, Professor Nirmalya Mukhopadhyay, whose experience and expertise was invaluable in formulating the research questions and methodology. His insightful feedback pushed me to sharpen my work to a higher level. We could not have completed this dissertation without his support and the stimulating discussions as well as happy distraction to rest our mind outside of this research.

REFERENCES

[1] Maria Sichkova, Biao Li, Lachlan, Like Mason, Yelyu, Yi Weng,"VM2: Automated Security Configuration and Testing of Virtual Machine Images", Published by Elsevier B.V. in 2020.

[2] Kenta Ishiguro, Kenji Kono," Hardening Hypervisor Against Vulnerabilities in Instruction Emulators", Published by EuroSec'18, April 23–26, 2018, Porto, Portugal.

[3] Darshan Tank, Akshai Aggarwal, Nirbhay Chaubey," Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison" Published by Bharati Vidyapeeth's Institute of Computer Applications and Management 2019.

[4] Pablo Martín Zamora, Michal Kwiatek, Vincent Nicolas Bippus, Eneko Cruz Elejalde," Increasing Windows security by hardening PC configurations" Published by EDP Sciences in 2019

[5] Sabiyyah Sabir," Security Issues in Cloud Computing and their Solutions: A Review", Published by (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 11, 2018.

[6] Rohan Jathanna, Dhanamma Jagli," Cloud Computing and Security Issues" Published by Rohan Jathanna. Int. Journal of Engineering Research and Application ISSN: 2248-9622, Vol. 7, Issue 6, (Part -5) June 2017, pp.31-38.

[7] Varsha, Amit Wadhwa, Swati Gupta," Study of Security Issues in Cloud Computing", Published by IJCSMC, Vol. 4, Issue. 6, June 2015, pg.230 – 234.

[8] Abhinav Mishra, Rishabh Mishra," Virtualization Security", Published by GRD Journals- Global Research and Development Journal for Engineering, Volume 1, Issue 12, November 2016 ISSN: 2455-5703.

[9] Ahmed Albugmi, Madini O. Alassafi, Robert Walters, Gary Wills, "Data Security in Cloud Computing", Published by Fifth International Conference on Future Generation Communication Technologies (FGCT 2016).

[10] S. Rama Krishna and B. Padmaja Rani, "Virtualization Security Issues and Mitigations in Cloud Computing", Published by Springer Science + Business Media Singapore 2017 S.C.

[11] Boubakeur Annane, Osman Ghazali, "Virtualization-Based Security Techniques on Mobile Cloud Computing: Research Gaps and Challenges", Published by IJIM – Vol. 13, No. 4, 2019.

[12] Adnaan Arbaaz Ahmed, Dr. M. I. Thariq Hussan, "Cloud Computing: Study of Security Issues and Research Challenges", Published by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4, April 2018, ISSN: 2278 – 1323

[13] Roberto Di Pietro, Flavio Lombardi, "Virtualization Technologies and Cloud Security: advantages, issues, and perspectives", Published by From Database to Cyber Security, 166 – 185, 2018-Springer.

[14] Nadiah M. Almutairy, Khalil H. A. Al-Shqeerat and Husam Ahmed Al Hamad, "A Taxonomy of Virtualization Security Issues in Cloud Computing Environments" Published by Indian Journal of Science and Technology, Vol 12(3), DOI: 10.17485/ijst/2019/v12i3/139557, January 2019.

[15] Abid Shahzad, Alan Litchfield, "Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable", Published by Australasian Conference on Information Systems 2015, Adelaide, South Australia.

[16] Ahmad Fayez S. Althobaiti, "Analyzing Security Threats to Virtual Machines Monitor in Cloud Computing Environment", Published by Journal of Information Security, 2017, 8, 1-7.

[17] Sebastian Biedermann, Stefan Katzenbeisser, Jakub Szefer, "LeveragingVirtualMachineIntrospectionforHot-HardeningofArbitrary Cloud-UserApplications", Published by 6th {USENIX} Workshop on Hot Topics in Cloud Computing (HotCloud 14),2014.

[18] Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Muhammad Nawaz, Brohi, Rukshanda Kamran, "Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures", Published by International of Cloud Computing,

Technologies, Applications & Management 978-1-4673-4416-6/12/$31.00 ©20121EEE in 2012.

[19] Yubin Xia, Yutao Liu, Haibo Chen, Binyu Zang, "Defending against VM Rollback Attack", Published by IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012),1-5,2012.

[20] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing", Published by Elsevier B.V, The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017), Procedia Computer Science 110 (2017) 465–472.

BIOGRAPHIES

Mr. Golam Mostafa is pursuing Bachelor of technology from Assam down town University, Guwahati, Assam, India since 2017. He will be graduated in July, 2021. He is currently a web developer, Content writer, Graphic designer, Digital Marketer. He is also doing a research how to publish research papers on different topics and what are the future scopes of doing research paper. He completed some certifications like "Workshop on Python Programming", "Digital Marketing" and "Ethical Hacking Basics". He is also trying to build his own start up.

Mr. Ananta Uzir is pursuing Bachelor of technology from Assam down town University, Guwahati, Assam, India since 2017. He will be graduated in July, 2021. He is currently a web developer, Graphic Designer, Web Designer. He is also trying to build his own start up with his friends. He completed different certifications like AWS Certified Solutions Architect -Associate 2020.

Mr. Nirmalya Mukhopadhyay pursued Bachelor of Technology in CSE from MAKAUT, India in 2009 and Master of Technology in CSE from MAKAUT, India in 2012. He is currently doing his research work in Cloud domain and working as Assistant Professor in Department of Computer Science & Engineering, Assam down town University, Guwahati, India since 2019. He is a member of ACM, CSTA, IEEE, IAENG, CSI & AACSIT since 2013. He has published 14 research papers in reputed International Journals including UGC Care Listed Journals, Ebsco Indexed Journals and Copernicus Indexed Journals. He has been a Google Scholar since 2012. His main research work focuses on Virtualization, Cloud Resource Allocation, Cloud Scheduling, Cloud Load Balancers, Cloud Algorithms, Virtualization Security, Cloud Security and Privacy, High Performance Computing, Cloud Performance Analytics, Docker & Containerization, Edge Computing, Optimization Problems, Grid Computing, Genetic Algorithm, IoT and Computational Intelligence Elucidation. He has 10 years of teaching experience and 6 years of Research Experience.