VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2021, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 9, Number 2, April-June 2021 *pp:44- 49*

Malware Injection Attacks in Resource Virtualization of Cloud Computing Environment

Mamoona Majid, Mansoor Ahmd Rasheed, Mannan Ahmad Rasheed

University of management and technology, Lahore, Pakistan
Corresponding author Email: mansoorahmadrasheed@gmail.com

ABSTRACT
Cloud computing is a procedure which gives us a large, reliable and scalable infrastructure and service. Cloud computing have some features of distributed system, according to these features cloud computing also uses the features of networking. In this technique, there is large number of data sets on the internet. These data sets can be stored and accessed by a remote server. Some common and basic examples of cloud computing are Amazon, Google's application etc. This technique provides the user to build an online application and to access that from any remote server hosted on internet. We know cloud computing system usually operate on an open network (public) so there comes security issues. The critical part of cloud computing technology is Virtualization. Virtualization refers to creating new system on the machine that is not actual but acts and performs like the actual ones. Cloud Computing and Virtualization give different services by working together. -This paper describes the malware injection attack on virtual systems working in cloud computing environment and their solutions as well. Cloud computing based on sharing technique therefore, the security is the leading crisis of this system. In this paper we discussed the diverse types of malware injection attacks and their possible solutions. Virtual machine emulators have turn out to be conventional in the examination of malicious code. This paper presents notorious attacks for the most extensively used virtual machine emulators. This paper also demonstrates newly exposed attacks on Bochs, Hydra, QEMU, and Xen (other virtual machine emulators), and describes how to protect from them.

KEYWORDS
Malware injection attacks, security attacks, virtualization or virtual machines (VM).
JOURNAL INFO

HISTORY: Received: April 20, 2021 Accepted: June 15, 2021 Published:.June 30, 2021.

INTRODUCTION

In everyone's life Cloud computing is involved. We make use of cloud computing services every day. To exchange messages email systems (Yahoo and Google) is used, to share information with friends social sites are used (Facebook and Twitter), cloud storages (e.g. Dropbox), teamwork tools (e.g. Google docs) and backup tools to backup data on cloud servers. Cloud computing also involved in business.

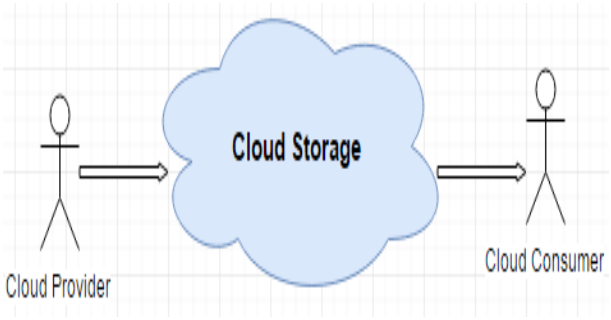

Figure 1. Cloud Deployment Models, Characteristics, and Infrastructures

National Institute of Standards and Technology (NIST) described three service model of cloud computing[1]Infrastructure, software and platform. It also lists four deployment models (hybrid, community, private and public). NIST also defined five features of cloud computing on-demand self- service, resource pooling, rapid elasticity, broad network access and measured service. Cloud computing environment can be shown by Figure 1.

*A. Infrastructure **as-a-service (IaaS)***

IaaS includes computational resources like storage, memory and network devices. IaaS offers virtual machines to help the customers to build infrastructures of complex network. This model restricts the cost as well as eases the load of network administration. Amazon's EC2 is the pattern of cloud computing service provider of IaaS.

Platform-as-a-Service (PaaS)

PaaS provides a stage to users to design particular applications and integrate it into their existing IT environments. It reduces the cost because User does not need to buy software development tools. One of the paradigms of cloud computing service provider of PaaS is GoogleApps.

*B. **Software-as-a-Service (SaaS)***

In SaaS, instead of purchasing applications user rent applications running on clouds. A paradigm of a cloud computing service provider of SaaS is grouped on four deployment model of Cloud Computing can be briefly discussed as below:

1) ***Private cloud***

It provide services to specific group of customers and these services are not available for public.

2) ***Public cloud***

It provide services to general public or large group of industry.

3) ***Community cloud***

It provide services to particular community that has shared common interests.

4) ***Hybrid cloud***

It is a mixture of one or more deployment models. It permits load balancing between clouds and portability of application and data.

In cloud computing, cloud actors (cloud agent) play a vital role [2]. Here, cloud consumer and cloud provider are used as actors. Cloud provider provides cloud services to cloud consumers. He offers owned IT resources to the cloud consumers for lease. Cloud provider is also known as data owner and Cloud consumer is also known as a client.

In cloud infrastructures virtualization is a core technology. It provides elasticity to move virtual machines to any location for resource optimization. DOS, virus, memory leaks and malware are most common security threats in virtualization [3].

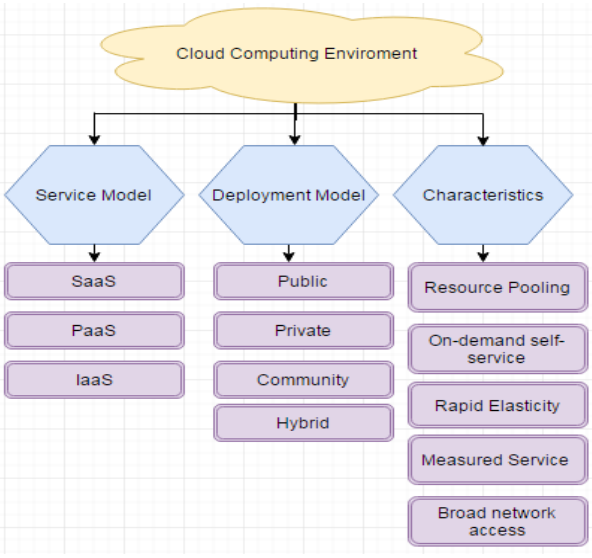

Figure 2. Cloud Computing Envirnoment

The following Figure 2 shows that client can use the services from the cloud storage with the help of internet and other devices and data owner hosts the services in the cloud storage.

Today network security is a challenging task and becomes very difficult to control specially in the cloud computing environment because in this environment becomes more dynamic and demanding. The key objective of cloud computing is to provide shared resources, storage, memory and services, etc. to minimize the cost of resources. This helps the user to not worry about resources so much to fulfill their desired tasks. In cloud computing environment, remote servers are public to the network and are much more demanding and provide many approaches of parallelism and distribution of resources. According to the security point of view, there are many types of attacks in cloud computing systems such as malware injection attack, flooding attack, browser attack, denial of service (DOS), theft of serves, man-in-middle etc. but here we discuss malware injection attacks. There are five feature of security.

1. **Availability**: Data must available on the remote server always and at any time for its users.
2. **Confidentiality:** Data on the server must be kept secret and available only to the eligible users.
3. **Integrity:** Data should not replicate or modified during travelling on network.
4. **Authentication:** Unauthorized access of data is prohibited.
5. **Accountability:** No user can refuse to participate in data transfer process.

We can classify attacks related to the security of cloud computing in five categories, which are mentioned in Table 1 [4].

Table 1: Categories of cloud security

Category	**Description**
Security Standards	To prevent attacks, it describes the standards for precaution in cloud computing
Network	It include network attacks e.g. DoS
Access Control	It include authorization, authentication and identification attacks
Cloud Infrastructure	It is associated with the virtualization environment
Data	It include data related problems such as integrity, confidentiality etc.

A lot of data is transferred between the cloud provider and the consumer in the cloud computing so authorization and authentication is necessary. The attacker can initiate malicious code between these actors while transferring data. This refers to malware injection. Considering the above issues, security is one of the main focuses in cloud computing. As we mention above there are many type of attacks that affect cloud security but our observation in this paper will be on malware injection attacks. We try to identify root cause of malware injection attacks and propose some solution.

In next section we describe some literature review in cloud computing. Section III presents comparison between several attacks. Section IV is attacks on VM. Section V is about software emulators and section VI is about discussion and future work. Section VII concludes the paper.

II. LITERATURE REVIEW

In malware injection attack an intruder breaches the security by injecting a malicious code into the system. In this

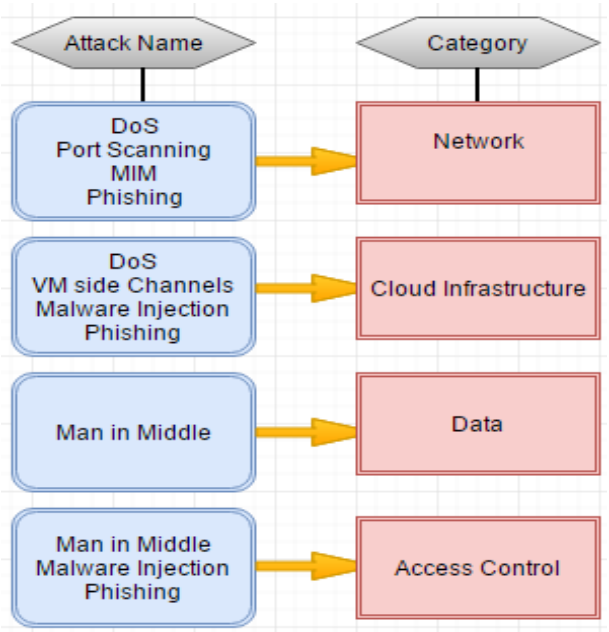

Figure 3. Attacks on Cloud and Respective Categories

type of attack, the attacker builds its own service that contains harmful viruses such as (SaaS or PaaS) or a virtual machine such as (IaaS) and injects these into the target system. After attack, intruder behaves like it is a valid and authenticated service or some new service. In this malware attack, attacker may delete the user account or modify its access right. So whenever user makes the request, it passes the request to its own created service rather than to execute the command as it is. If the attacker succeeds to do it, user request will automatically be directed toward the attacker malicious service implementation and attacker's code starts to execute. In malware injection attack, the core intention of attacker is to achieve the access to the user request. Once achieved, it can access, control and modify user's data on the cloud. So this will actually disclose the user account to the attacker.We can see various clouds attacks and their respective categories [5] in Figure 3.

Previous researches purpose many solutions against malware injection attack. As in cloud computing environment all system are running their application publically in highly efficient way. To prevent attack, they focus more on hardware. In some system they combine the integrity with the hardware because it is difficult to breach the security hardware (IaaS) level. Manitou is a system that is designed to execute the code of only authenticated users by computing hash of each memory page.

In our recent system, Firewall and Web Application Firewalls (WAFs)is designed to check the incoming connection either they are valid or not. It is used for port scanning. Firewall first scans the port of system that wants to access or store data that whether it is authenticated or it is some malicious malware containing system.

Intrusion Detection System (IDS) architecture is used to discover Malware Injection attacks[5, 6]. This system recognizes intrusion detection, alert or record detected information. This system composed of Console to observe events, Sensors and Central Engine to record events. In the IaaS Layer of the cloud, Intruders can get victim machine information [7]. By using this information he can attack cloud users and collocate affected VM with victim's VM. Intrusion Detection System investigates user behavior, log files and network traffic[8]. It gathers information from various points to analyze protection measure.

Intrusion detection (ID) is divided into two classes Misuse Detection & Anomaly Detection. Misuse detection compares user input with preceding inputs by identical user. On contrary anomaly detection used to stores user activities in database, which compared with existing activities. Invasion occurred, if there is huge difference in comparison. There are two types of IDS, one that analyze behavior on single host is host based IDS (HIDS) and other that monitor behavior on network is network based IDS (NIDS)[9]. A third type known as hybrid IDS that combines the characteristics of both type is also discussed in [10].

Host-based Intrusion Detection Systems installed in a computer system to detect intrusion and notify the nominated authority. It works like an agent that analyzes any internal or external activity that is against the security.

Network-based IDS (NIDS) observe network traffic, detect any malicious activity and unconstitutional access to network to block it[5]. Another solution to tackle the malware injection attack is to perform integrity check for arriving requests. Hash values[11]are used for comparison between

new service instance images with stored hash value of the original service instance's image. If there any variation is done in valid instance, hash value will also update and this signifies the presence of malicious activity [12]. Thus, to inject harmful attacks into the Cloud system, attacker has to trick hash value comparison which is very difficult approach for him.

File Allocation Table (FAT) system architecture can also be used to prevent Malware Injection Attacks in cloud environment [13, 14]. Client code or application can be recognized in advance using FAT. To determined integrity of the new instance, it can be compared with previous ones that already executed. Usually when user opens the system or makes a request, cloud creates an image of the user's virtual machine in the image repository. Some systems utilize FAT table for this purpose because it determine validity and integrity of system that want to access remote system in cloud computing environment. In FAT architecture we know all

about the system what is currently running on the system by which user etc. in FAT table we can also check the integrity by the previous executing task etc. For this purpose we have to provide hypervisor at the user's end. Hypervisor is responsible for integrity purposes and to check all the instances[15].

Hash Value Comparison It is one more method to avoid malware injection attacks. A hash value is used to store the original image file of the instance and this value is compared with the values of new instances. The integrity check between original and new instance can identify the hateful instances [16].

Figure 4 represent possible solution of Malware Injection. In next section we will discuss the comparison of these solutions.

III. ANALYSIS AND COMPARISON OF POSSIBLE DEFENSE MECHANISM

The comparison between the four techniques of solution malware injection attack is present in Table 2.

Table 2: Comparison of Existing Techniques

FILE ALLOCATION TABLE (FAT)	WEB APPLICATION FIREWALL (WAFS)	INTRUSION DETECTION SYSTEM (IDS)	HASH VALUE SYSTEM
HYPERVISOR S ARE USED	Port scanning is used	PIDs are used	HASH VALUES ARE USED
BASED ON PREVIOUS INSTANCE'S VALIDITY AND INTEGRITY	Based on new Instantiation of VM	Based on MAC Address and IP.	BASED ON COMPARISON BETWEEN NEW AND PREVIOUS INSTANCE
MIGHT ACCESS IAAS, PAAS, SAAS	No Access to IaaS, PaaS, SaaS	Access to IaaS, PaaS, SaaS	ACCESS TO IAAS, PAAS, SAAS
SECURITY CAN'T BE BREACHED	Possible to attack (VM)	Possible to attack the management/ services of the system	INTEGRITY CHECKS IDENTIFY SECURITY
FIREWALL IS NOT IMPLEMENTED IN FAT	Firewall is implemented (to prevent placement of new VM to target VM	Firewall and port are implemented.	FIREWALL IS NOT IMPLEMENTD .
NO LAYERED TECHNOLOGY	NO LAYERED TECHNOLOGY	USE OF LAYERED TECHNOLOGY OF IDS.	NO LAYERED TECHNOLOGY

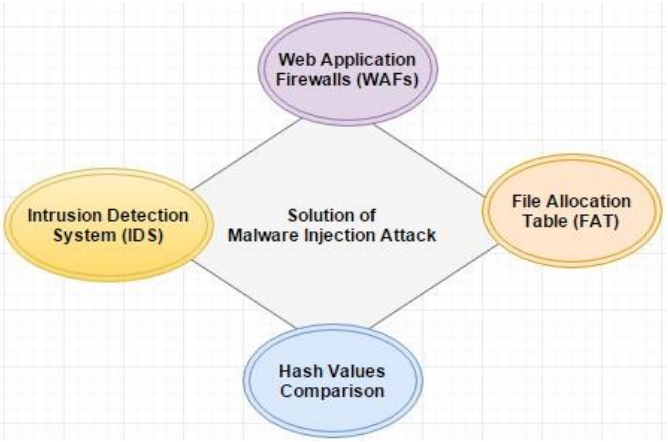

Figure 4. Possible Solutions of Malware Injection Attack

FAT design is a simple technique and supports all existing virtual operating systems. As Hypervisors is used in FAT technique, it provide high reliability and security cannot be breached by any means. Plus point of FAT is that it supports larger file sizes. It is no layered technology. Intrusion Detection System (IDS) detect intrusions by integrating knowledge and observing behavior. The main limitations in IDS are network load overhead, redundancy and trust management. Trust management requires collaboration with different clouds, which does not exist in IDS [6].

Hash Value System provides high protection by making comparison of instances. To breach security in this technique intruder have to guess hash calculation tricks, which is highly difficult.

Web Application Firewall (WAFs) Block malware trying to enter network and all "evil packets". This technique consume more time as it continually analyze network activities. The limitation of WAFs is firewall maintenance because of its complex nature.

IV. ATTACKS ON VIRTUAL MACHINE EMULATOR

There are many hardware and software assisted virtual machine emulators. HYDRA, QEMU, BOCHS and XEN are some of popular machine emulators. XEN is hardware emulator machine and QEMU and BOCHS and HYDRA is software based emulator.

A. XEN

Xen 3.x, Virtual Server exists as hardware-assisted virtual machine emulators. Virtuozzo may also act as a hardware-assisted virtual machine emulator. Hypervisor is the main appealing thing as regards of hardware-assisted virtual machine emulators. To detect currently running machine, hypervisor is mostly used. There are efficiently two copies of the OS; host machine is suspended whereas the other guest machine execute liberally in the fresh state. When an appealing event (an intercept, interrupt, or exception) occurs, the host operating system regains control, handles the event, and then restarts the guest operating system [17]. Once the host machine is active, it become difficult to detect virtual machine unless it release all sensitive information to CPU e.g; CPUID. When CPU saw the copy of these sensitive information, it suggest to hide the presence of hypervisor e.g; clear the CPUID flag.

V. SOFTWARE BASED VIRTUAL MACHINE EMULATORS

For any given CPU instruction, pure software virtual machine emulators work by executing identical operation in software. Over hardware-bound virtual machines, main advantage of pure software virtual machine emulators is that there is no need to match the original CPU and guest environment can liberally be in motion between machines of different architectures Hydra, Bochs and QEMU are best example of pure software virtual machine. CPU and operating system both can be emulated. Atlantis and Sandbox are two examples that let a malicious file to execute, and capture its behavior in a totally nontoxic mode. Sandbox supports Windows only and Atlantis supports DOS, Windows, and Linux When the required CPU is not known Atlantis, Hydra and Bochs support various CPUs to more reliably emulate an environment. The main problem of emulator is that for same instruction different behaviors is display on different generations of CPUs. Emulated software might not perform properly, if a pure software virtual machine emulator is Created for one particular CPU [17].

A. BOCHS

Bochs. is pure software virtual machine emulator and also Open Source,. It behaves like a stand-alone machine because it does not sustain guest-to-host or host-to-guest communication. It is exposed to a number of detection methods. Device support is one of the simplest methods. For example, Bochs only support standard size of floppy disk. Non-standardized floppy size can cause kernel panic.

B. HYDRA

HYDRA is pure software virtual machine emulator and also closed-source. It is supposed to act like a stand-alone machine and also supports guest-to-host communication. It does not purposely support host-to-guest communication. Plug-ins can modify the environment and manage the execution flow. Therefore, guest-to-host communication channel exists.

Plug-in do not communicate with the guest machine. Therefore, Hydra uses a specific port for guest-to-host communication but still there is a possibility of an exception , thus it is better to hide the communication. No Hydra-specific information is returned by the port access as host-to-guest communication does not happen.

C. QEMU

QEMU is pure software virtual machine emulator and also Open Source,. It is supposed to act like a stand- alone machine and also supports guest-to-host communication. To advance the performance of the CPUs it supports dynamic translation of code. When non-spontaneous CPU behavior occurs, like self- overwriting then in the presence of self-modifying code, the use of dynamic translation is constantly unsafe. Double Fault exception is not supported in QEMU. CPU is not capable to create the General Protection Fault so Double Fault exception is raised. The General Protection Fault is raised frequently in QEMU [17].

Bochs, Hydra, and QEMU, are the pure software virtual machines that are used to detect diverse types of attacks on virtual layer of cloud computing. All of these machines experience bugs and limitations that allow their detection but these troubles can be fixed easily. Pure software virtual machine emulators can come close to absolute lucidity. It should be achievable to reach the position where detection is unreliable because it can also be attributed to anomalous behavior of a real CPU.

VI. DISCUSSION

As we know that cloud computing is very vast field and is on arise. So we can anticipate a lot number of data protection and vulnerabilities. Malware injection attacks in cloud computing are very fatal. Cloud security issues are active area of research and experimentation. Cloud security, virtualization, data protection and isolation of resources are the main concerns on which lot of research is going. This paper gives first step towards the detail version of existing techniques and then provides the brief

comparison of all details. In this paper we discuss malware injection attacks of cloud computing and also provide some possible solutions against this attack. High volume of data could be handled by IDS, FAT, and Web Application firewall etc. To prove or controvert the attacks and to find the solution of all these, we can continue with the malware injection (SQL Attacks) attacks and vulnerabilities. It will become necessary for anti-malware researchers to find behavior to sense the virtual machine emulator, if malicious code occurs.

VII. CONCLUSION

As discussed throughout this paper cloud computing is in consistent advancement and malware injection attacks on client machines in virtual environment. Cloud computing has a lot of benefits but security in cloud computing environment is a key test. Weakness in cloud computing still exists and systems analyst keeps on exploiting these security gaps. To provide better environment of administration to cloud clients, security defects must be distinguished.

This paper reviews the malware injection attacks on cloud and the consequent alleviation dealings. We have depicted crucial and well known security attack malware injection and have some potential solutions in this paper, such as utilizing the FAT table, Hash Value System, Intrusion Detection System (IDS). We also compare these solutions to making them more concrete and improving their analysis. Two VMs in the same network may communicate by covert channel. Shared clipboard maybe used secretly for communication between VMs. Hypervisor is responsible for all the interaction between hardware and the virtual machines (VM's).A malicious Hypervisor can change any virtual machine code to run it in a way attacker wants, and can access or tamper all data in the virtual machines. XEN, BOCHS, HYDRA and QEMU are the machine used to detect malware injection attack.

References

[1] Final Version of NIST Cloud Computing Definition Published. 2015.

[2] International Journal of Advanced Research in Computer and Communication Engineering **3**(10, October 2014).

[3] Mohamed Al Morsy, J.G.a.I.M., An Analysis of the Cloud Computing Security Problem. (January 2010).

[4] Issa M. Khalil, A.K.a.M.A., Cloud Computing Security: A Survey **3**.

[5] Omar Achbarou, M.A.E.k., and Salim El Bouanani, *Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems.* Indian Journal of Science and Technology, (May 2017).

[6] Issa M. Khalil , A.K., Muhammad Azeem, *A Survey of Cloud Computing.* (3 February 2014).

[7] Tupakula, U.V., V Akku, *Intrusion detection techniques for infrastructure as a service cloud.* IEEE Ninth International Conference on Dependable,Autonomic and Secure Computing (DASC), (2011).

[8] Kleber Vieira, A.S., Carlos Becker Westphall, Carla Merkle Westphall *Intrusion detection for grid and cloud computing.* (2010).

[9] Van athi, G., *Comparison of network intrusion detection systems in cloud computing environment.* International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, (January 2012).

[10] Roschke, C., Meinel, Intrusion detection in the cloud, in International Conference on Dependable, Autonomic and Secure Computing.

[11] Ajey Singh, D.M.S., *Overview of Attacks on Cloud Computing.* International Journal of Engineering and Innovative Technology (IJEIT) **1**(4, April 2012).

[12] B.Sumitra, C.R.P., M.Misbahuddin, , *A Survey of Cloud Authentication Attacks and Solution Approaches.* International Journal of Innovative Research in Computer and Communication Engineering. **2**(10, October 2014).

[13] Chou, T.-S., *Security Threats on Cloud Computing Vulnerabilities.* International Journal of Computer Science &Information Technology (IJCSIT) **5**(3, June 2013).

[14] Venkatesa Kumar, M.N., Improving security issues and security attacks incloud computing, International Journal of Advanced Research in Computer and Communication Engineering. International Journal of Advanced Research in Computer and Communication Engineering. **3**(10, October 2014).

[15] Priyanka Chouhan, R.S., *Security Attacks on Cloud Computing With Possible Solution.* international journal of Advanced Research in Computer Science and Software Engineering. **6**(1, Junary 2016).

[16] KaziZunnurhain, S.V.V., *Security attacks and Solution in clouds.***6**(1, January 2016).

[17] Peter Ferrie,Attacks on Virtual Machine Emulators. (01, September 2007).

[18] Vistro, D. M., Rehman, A. U., Farooq, M. S., Abid, A., & Idrees, M. (2020). CLOUD BASED CRYPTOGRAPHY BY USING QUANTUM KEY DISTRIBUTION. *Journal of Critical Reviews*, *7*(9), 1680-1686.

[19] Vistro, D. M., Rehman, A. U., Abid, A., Farooq, M. S., & Idrees, M. (2020). Analysis of cloud computing based blockchain issues and challenges. *Journal of Critical Reviews*, *7*(10), 1482-1492.

[20] Vistro, D. M., Rehman, A. U., Farooq, M. S., Abid, A., & Idrees, M. (2020). A SURVEY ON CLOUD COMPUTING SECURITY WITH CROSS PLATFORM. *Journal of Critical Reviews*, *7*(10), 1439-1445.

[21] Vistro, D. M., Rehman, A. U., Abid, A., Farooq, M. S., & Idrees, M. (2020). CLOUD BASED ARCHITECTURE FOR SMART EDUCATIONAL SYSTEM USING MODERN TECHNOLOGY. *Journal of Critical Reviews*, *7*(10), 1493-1503.

[22] Vistro, D. M., Rehman, A. U., Farooq, M. S., Abid, A., & Idrees, M. (2020). A survey ON the role OF security and integrity issues IN cloud. *Journal of Critical Reviews*, *7*(10), 1456-1469.

[23] Abid, A., Manzoor, M. F., Farooq, M. S., Farooq, U., & Hussain, M. (2020). Challenges and Issues of Resource Allocation Techniques in Cloud Computing. *KSII Transactions on Internet and Information Systems (TIIS)*, *14*(7), 2815-2839.