[1] **Vagif Gasimov ***
[2] **Shahla Aliyeva**
[3] **Maryam Asadova**
[4] **Sema Bayramova**
[5] **Hasan Pashayev**

Cloud Computing, Virtualization and Security Issues

Abstract: - The most significant challenge in cloud computing is the security and privacy issues associated with the infrastructure, sensitive data and critical applications, which may be accessed from external sources. This article examines the security issues associated with cloud computing, including potential attacks and risks that can be perpetrated against cloud technologies. It also considers methods of preventing and minimizing these risks.

Keywords: Cloud Computing, Virtualization, Virtual Machines, Cloud Security.

I. INTRODUCTION

In the contemporary business environment, organizations tend to favor the utilization of cloud computing services due to their cost-effectiveness Cloud computing services perform a range of functions, including data storage, calculation, memory array clustering and virtualization, through the use of network and communication technologies. These services provide network users with flexible, cost-effective and configurable computing and storage resources that can be used to provide information services such as application, storage, search and exchange over the cloud.

The utilisation of virtualisation technologies for cloud computing is regarded as a significant factor due to its prevalence in the processing of large volumes of data. This technology enables users to create and share copies of computer resources (processors, storage devices, etc.) by virtualising them. This allows multiple independent virtual machines to run on a single physical device.The utilisation of virtualisation technology enables the creation of numerous virtual machines within a single physical machine. This allows for the loading and running of different operating systems on individual virtual machines, with the distribution of memory resources between virtual machines being facilitated as required. This approach has the potential to result in significant savings in terms of energy, technical equipment, work area, service personnel, and so forth.

In cloud computing, virtualisation technology organizes a virtual platform for the server operating system and physical equipment. The technology permits the concurrent use of multiple virtual machines, the sharing of memory resources, and the distribution of one physical copy of software applications among multiple users. Cloud computing virtualisation enhances the scalability, cost-effectiveness, and efficiency of traditional computing, thereby facilitating the management of workloads and the rapid integration of core computing.

One of the most significant concerns in cloud computing is the issue of information security. The introduction of a new level, which is necessary to protect, into the counting environment in conjunction with virtualisation renders the system vulnerable to hacking. In light of the above, it can be argued that the security of virtual machines is just as important as that of physical computers and that the vulnerabilities that exist in both cases affect each other. Although the security measures implemented in cloud computing infrastructure are not significantly different from those applied to traditional information technology (IT) infrastructure, cloud computing does present a greater risk than traditional IT due to the information services and infrastructure offered [1].

In order to guarantee the security of the cloud platform, it is of the utmost importance to consider the significance of virtualisation. The vulnerability of virtualised environments to attack is greater than that of traditional

[1] Computer Technologies / Azerbaijan Technical University, Baku, Azerbaijan. gasumov@yahoo.com

[2] Computer Technologies / Azerbaijan Technical University, Baku, Azerbaijan. shahla.aliyeva@aztu.edu.az

[3] Information Technologies/ Mingachevir State University, Mingachevir, Azerbaijan. maryam.asadova@mdu.edu.az

[4] Department of İnformation Technologies, Western Caspian University, Baku, Azerbaijan. sema.bayramova@wcu.edu.az

[5] Cybersecurity / Azerbaijan Technical University, Baku, Azerbaijan. hesen.pashayev@aztu.edu.az

* Corresponding Author Email: gasumov@yahoo.com

infrastructures. In this context, the issue of ensuring security in the virtual cloud environment is a significant challenge. The introduction of virtualisation creates a multitude of access points and communication channels, which significantly complicates the operation of the system. For this reason, the issue of security should be accorded the highest priority in the virtualisation process, as it represents one of the most pressing concerns in this context.
In consideration of the aforementioned factors, the present article is devoted to the examination of the security challenges associated with virtualization in cloud computing, a topic of paramount importance in the contemporary era [2]**.**

II. MATERIALS AND METHOD

The virtual machine and its associated security concerns

Hypervisors, also known as virtual machines' (VM) monitors, possess a number of capabilities, including reconstruction, initiation, termination, resource switching, management, and configuration of virtual machine communication channels with each other or with the Internet. The implementation of a hypervisor permits the segregation of distinct virtual machines (VMs), situated on a common physical host, thereby averting the risk of data theft or malevolent actions perpetrated by other VMs. The isolation mechanism serves to preclude the possibility of the utilization of resources for each virtual machine being influenced by others. It allows end users to access only their own resources, such as hardware, software, and data, while the isolation mechanism allows them to limit their access to other resources (Fig. 1)

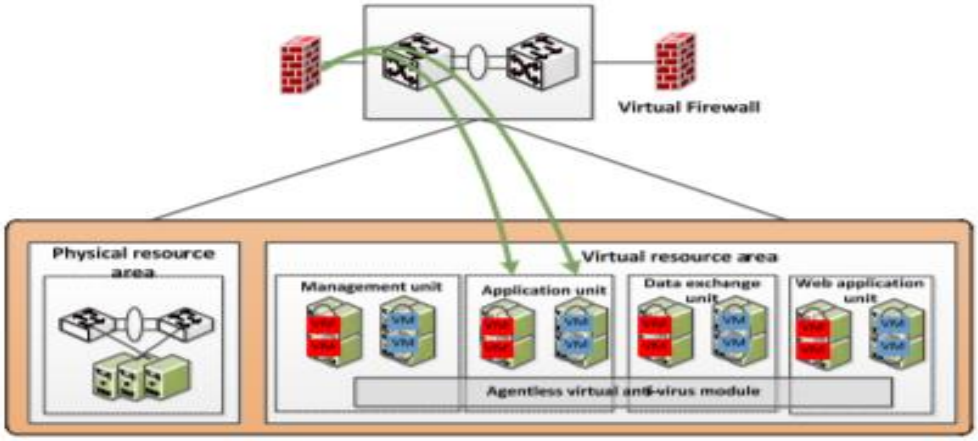

Fig. 1. A virtual machine security solution

In the context of cloud computing infrastructure, virtualization technology serves to enhance both computing power and storage efficiency by optimally managing any unused computing resources. While this solution is undoubtedly convenient, it is important to recognize that it can also pose significant security risks. This renders virtualization more susceptible to cyber-attacks in terms of internet access. Consequently, there is a possibility that hackers may gain access to these types of systems and thereby interfere with their functionality. To protect online systems from the attacks such as SQLi, XSS, LDAP Injection, Session Hijacking, DoS, DDoS, etc. professionals and developers are compelled to continuously enhance their security policies in order to reduce the associated risks [1, 2].
In this context, it is possible to utilize firewalls to prevent unauthorized access and to protect data privacy. Furthermore, firewalls can serve to safeguard data from malicious software, including computer viruses and other forms of cyber-attack. Consequently, the client is able to transfer his data to a virtual environment and create a backup copy on any cloud server, where it can be stored. Although virtualization is a highly beneficial technology due to the VMs, it is important to recognize that it can also present a number of potential risks in terms of data privacy and security. These risks include the possibility of system data corruption, loss, leakage, virus infection, and traffic theft. Figure 2 presents a hierarchical structure that encompasses the various threat and attack levels that have been identified in the context of the virtualization infrastructure.
A three-layer cloud security model, comprising an authentication layer, an encryption layer, and a recovery layer, has been proposed by Pooja Sharma and colleagues [3]. The authors claim that each of these levels is responsible for the security of data in the cloud. It is proposed that some security policies be applied between the provider and users in order to enhance the level of security. The idea is to apply some encryption methods and robust protection methods, such as multi-factor authentication, in order to achieve complete (end-to-end) encryption of data in transit,

storage and processing. This will prevent hackers from understanding the actual data during an attack. In this manner, it is possible to empower different administrators within the cloud according to their functions, apply SIEM and SOC technologies, detect attacks on the system at an early stage and take the necessary measures.

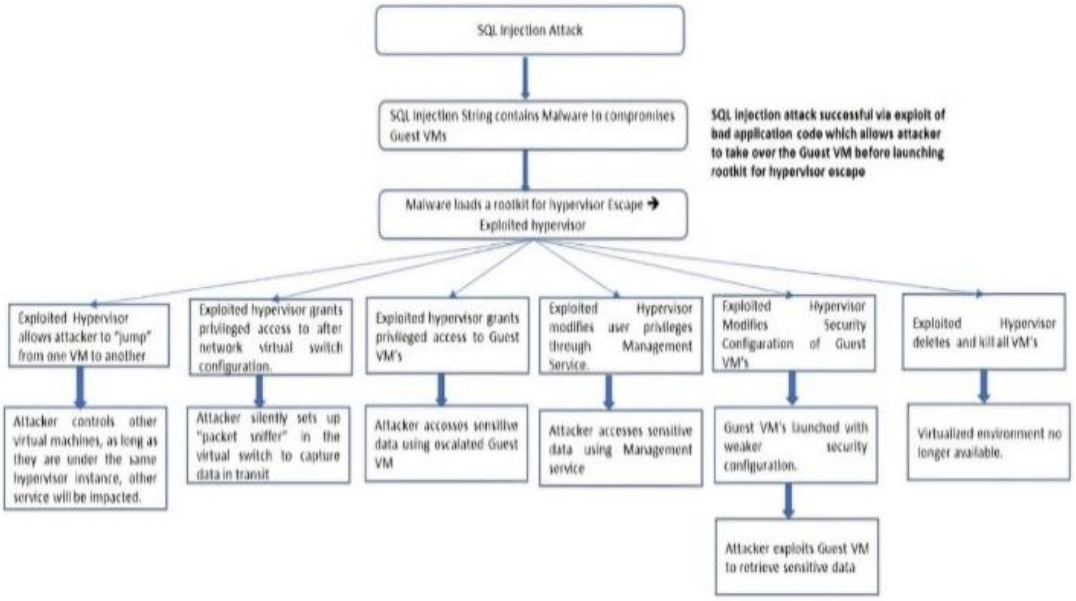

Fig. 2 illustrates the hierarchical structure of different threat and attack levels in virtualization infrastructure.

In [4], Chandrakala et al. proposed a transition-based approach, such as the Discrete Time Markov Chain (DTMC) distribution, to assess the security of individual VMs and predict the potential for danger. This approach also alleviates the performance burden, thereby enhancing the performance of the cloud platform.

As stated by R. Velumadhava Rao et al. [5], the transition to a virtual cloud model necessitates a heightened focus on data security and privacy, as the potential for data leakage can have a profound negative impact on an organization's business, brand, and credibility. It is observed by researchers that there are a number of security issues associated with the cloud, including those pertaining to privacy, authenticity, availability, location, separation, and so forth. A number of solutions have been proposed to address the security concerns associated with cloud computing. These include the encryption of data prior to its storage in the cloud and the authentication of certain group members. In particular, prior to storage in the cloud, data owners must ascertain that the data has not been changed by calculating hash values that serve to guarantee data integrity.

In Darwish et al. [6], the primary risks to cloud systems are identified as distributed denial of service (DDoS) attacks, IP spoofing, SYN flooding, Smurf attacks, and buffer overflows. The authors describe the attacks and propose defensive measures to mitigate their impact. The use of hop count filtering at the PaaS level and a trust-based approach at the IaaS level are presented as methods to protect against IP attacks. In the context of SYN overflow, the SYN Cache approach at the PaaS level, the SYN cookie protection approach, the reduction of SYN time achieved at this level, the active monitoring mechanism along with filtering and firewall mechanisms at the IaaS level are recommended. Virtual machines (VMs) are configured at the Platform as a Service (PaaS) level, while network resources are configured at the Infrastructure as a Service (IaaS) level, in order to prevent a Smurf attack. For SYN overflow defense, it is ensured through the implementation of SYN Cache, SYN cookie, and SYN timeout reduction mechanisms at the PaaS level, alongside filtering and firewall mechanisms with active monitoring at the IaaS level.

Iyengar and Ganapath [7] put forth a three-module overload classification mechanism for network traffic analysis, anomaly detection, and request feature verification using chaotic theory against DDoS attacks.

Kishu Gupta et al. [8] highlight the crucial role of data in any organization, emphasizing the importance of implementing a robust data security policy to prevent the leakage of data to unauthorized third parties. The authors put forth a data leakage detection (DLD) module, which is employed to identify instances of data leakage as a data distribution strategy.

In the current era, virtual machines are logically distinguished according to their virtualization capabilities. In the context of virtualization, as resources are in distribution mode, there is a heightened risk of information leakage. These security factors are accorded greater consideration when virtualizing infrastructure within a private cloud

environment. A private cloud is a model that can be influenced by external factors when deploying an application that is located within a single organization, serves different structural units of the organization, and has access to the Internet.

The most reliable method for establishing a connection between virtual machines (VMs) and a host computer is to utilize dedicated VMs. Furthermore, network administrators utilize virtual networks to facilitate direct and effective communication [9, 10].

III. RESULTS

The configuration of secure virtual machines

The results obtained from the structure shown in Figure 2 indicate that the optimal security design would be as follows.

As previously stated, it is possible to configure multiple independent virtual machines (VMs) on a single physical machine. This approach can address the challenges associated with the distribution and optimal utilization of machine resources, as well as enhance parallel processing and computing capabilities. An abstraction level exists that conceals all key details from users, is considered more secure than modern architectures, and its high availability feature allows for easier disaster recovery. In general, this architectural approach is considered a more favorable choice for enterprises and organizations, given the importance of cloud technology to all organizations. In light of these considerations, researchers and manufacturers are striving to enhance security measures in any instances [8, 9, 10].

The present study employed three virtual machines (VMs). The VM-Web machine assumes a pivotal role in this context. It is assumed that the VM-Web machine is the primary computing virtual machine and that the majority of the data is stored on this machine. The primary objective is to enhance the security of the virtual computing machine, which is situated within the cloud infrastructure.

The instruments employed for this purpose are illustrated in Figure 3.

The initial stage of the process entails establishing a connection to the VM-Web machine on the VM1 machine, however the user is not aware of this connection. In other words, the user should be unaware that they are accessing a VM-Web machine. In order to maintain privacy, as illustrated in the accompanying figure, the user is presented with the (VM1) VM-Web machine (Figure 4).

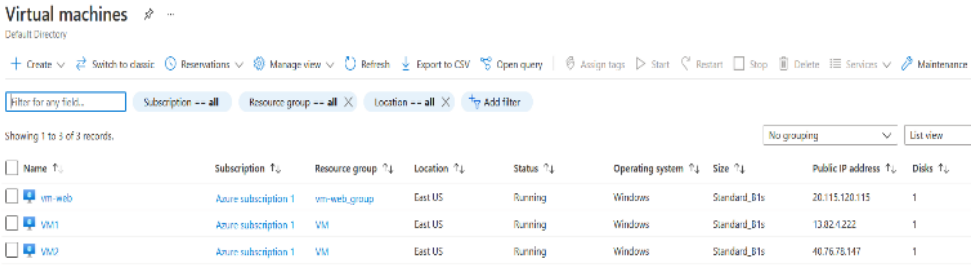

Fig. 3. Virtual machines were employed

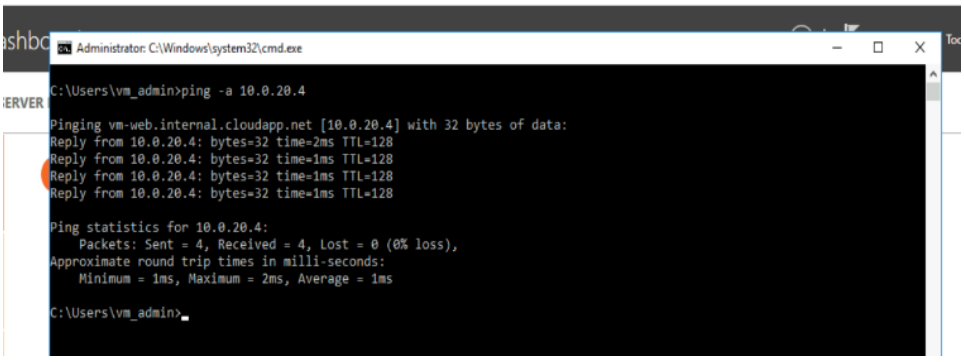

Fig. 4. The interconnection between the VM1 and VM-Web machines

Prior to any further action, it is necessary to ensure that the VM-Web machine is isolated from all caches.

In order to achieve this, it is necessary to disable all additional ports and resources on VM-Web, which is the main computing machine, via the firewall.
The primary parameters for debugging are defined as follows:

- Each port connection is disabled;
- All programs are selected;
- All IP addresses are selected as wildcards.

It should be noted that such adjustments to parameters may occasionally prove to be impractical. The primary rationale for this is the potential for complete disconnection with the computing machine on the cloud server. As a consequence of its isolation, a network administrator may be unable to connect to the computing server in order to manage it. This issue can be addressed in two distinct ways.
The connection is established through the command line interface (CLI) provided by the cloud service. In the event that the cloud service provider is unable to provide this service, option 2 can be selected.
For a static IP address, a predefined port remains accessible. This will permit access to the management of the compute server.
Upon completion of the aforementioned steps, the transition to the subsequent phase is initiated.
In this instance, the VM2 server is employed as a router. Due to the routing capabilities provided by VM2, incoming requests are processed according to specific routes, and functions or controllers assigned to these routes are invoked. This methodology allows for the proper organization of application functions and the routing of requests. In order to achieve this objective, it is necessary to register the network address of the router server VM2 on the VM-Web server in the firewall, thus allowing the main computer to connect to the server (Figure 5).

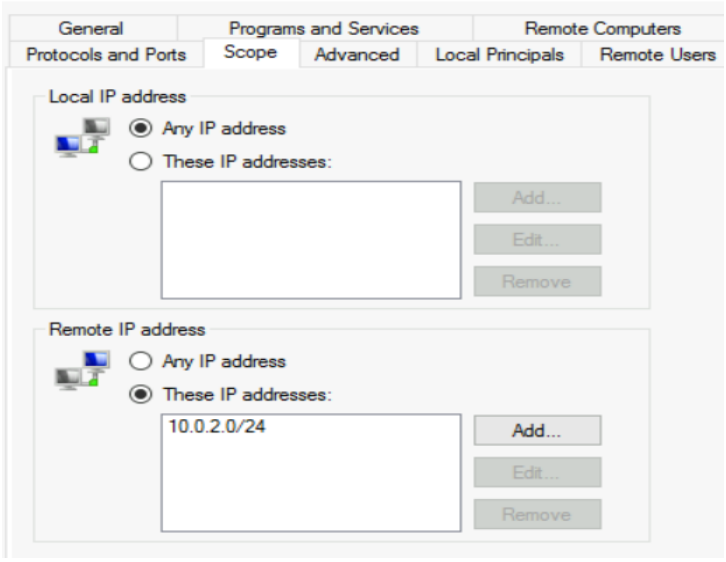

Fig. 5. Recording the server's network address in the firewall

Upon completion of the aforementioned steps, the VM-Web compute server will only respond to requests originating from the VM2 router server. The next stage of the process requires the VM2 router server to undergo tuning in order for it to be able to perform the forwarding function in its entirety. The routing parameters of the VM2 routing server are as follows (Figure 6).

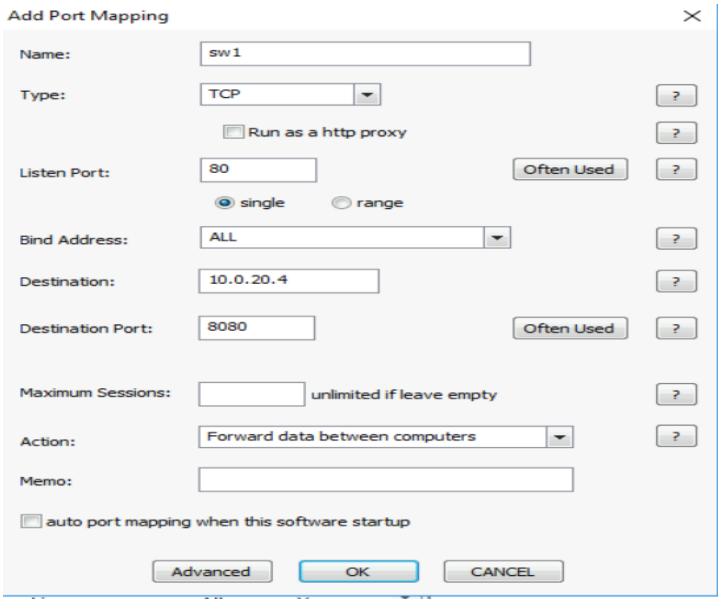

Fig. 6. VM2 Server Router Settings

The results obtained are presented in Figures 7 and 8 below.

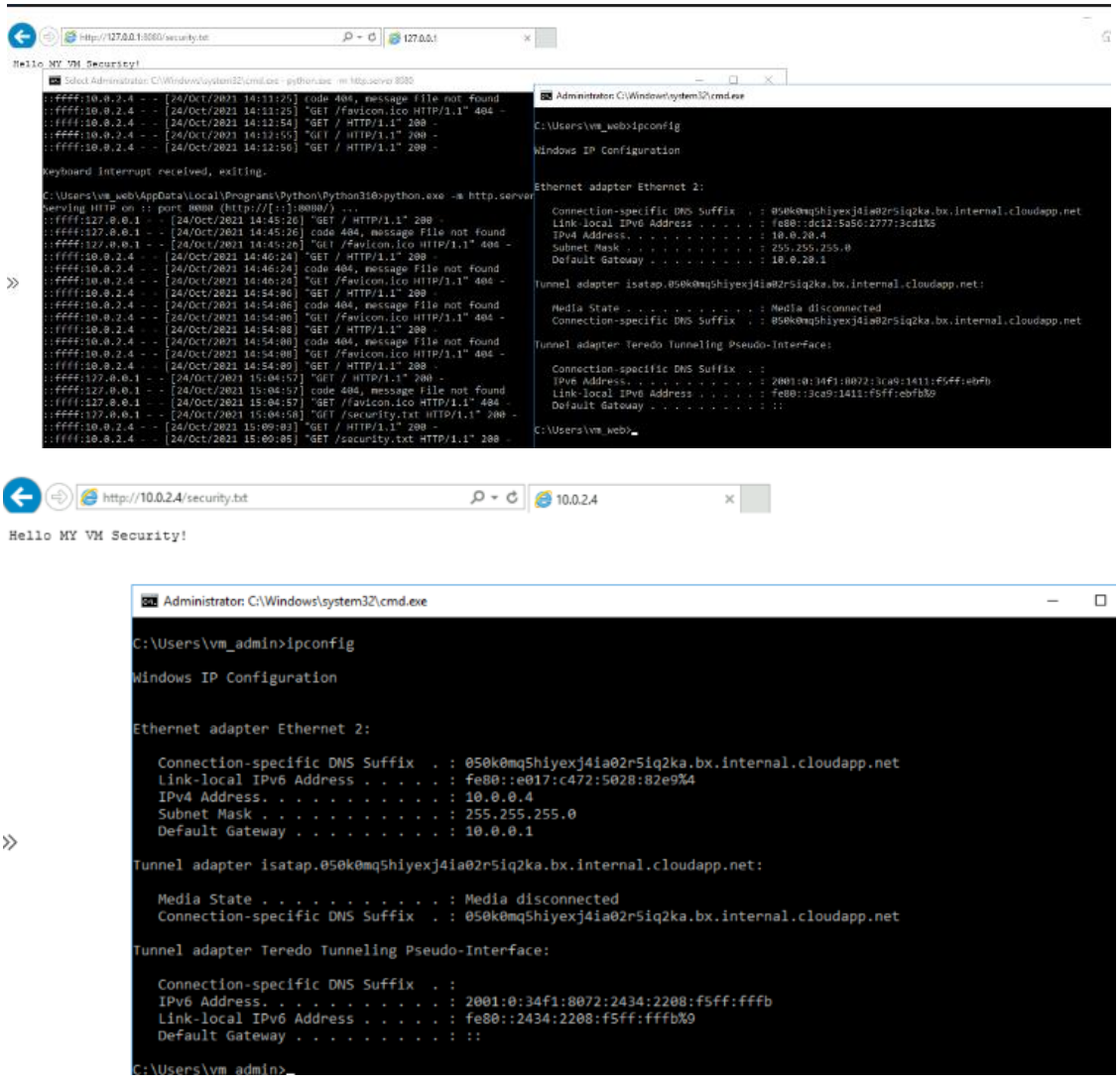

Fig. 7. The forwarding of incoming requests to the IP address and port numbers of the VM2 server

The accompanying image illustrates the configuration of the VM2 server, which has been set up to listen on port 80 and redirect requests to the 8080 port of IP address 10.0.20.4. The necessary debugging has been conducted to guarantee that router VM2 correctly forwards incoming requests to the appropriate IP address and port number. These tests allow the functionality and correctness of the router to be evaluated and, if necessary, provide troubleshooting.

IV. Discussion Conclusion

A review of the literature reveals that security is the most significant concern among users of cloud computing. The present article concentrates on the security of the virtual network, which represents the fundamental technology underlying cloud platforms. To enhance the security of communication between virtual machines placed on physical machines, the issues that may arise when isolating a virtual machine and establishing a connection with it have been examined, and potential solutions have been proposed.

Authors' Contributions

The authors' contributions to the paper are equal.

Statement of Conflicts of Interest

There is no conflict of interest between the authors.

Statement of Research and Publication Ethics

The authors declare that this study complies with Research and Publication Ethics

References

[1] Gasimov V.A., Aliyeva Sh. Kh., Using blockchain technology to ensure security in the cloud and IoT environment. // International Congress on Human-Computer Interaction, Optimization and Robotic Applications, June 11-13, 2021, Turkey

[2] https://www.researchgate.net/publication/352801393_Using_blockchain_technology_to_ensure_security_in_the_cloud_and_IoT_environment

[3] Gasimov V.A., Aliyeva Sh.Kh. Basic components of the digital business: cryptocurrency, blockchain, cloud technologies and internet of things. // "International Journal of 3D Printing Technologies and Digital Industry", Turkey, 2020, pp. 97–105.

[4] Pooja Sharma, Vaibhav Jha, Boosting Security for Cloud Storage // Volume 8 Issue V May 2020 International Journal for Research in Applied Science & Engineering Technology (IJRASET)

[5] Chandrakala N., Thirumala R.B. Migration of Virtual Machine to improve the Security in Cloud Computing. // International Journal of Electrical and Computer Engineering, ISSN: 2088-8708, Vol. 8, No. 1, February 2018

[6] Velumadhava R., Selvamani K. Data Security Challenges and Its Solutions in Cloud Computing. // International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015)

[7] Darwish D., Ouda A., and Capretz L. F., Cloud-based DDoS Attacks and Defenses, Information Society (i-Society), 2013 International Conference, pp. 67-71 2013

[8] Iyengar N. Ch. S. N., and Ganapathy G., Chaotic Theory based Defensive Mechanism against Distributed Denial of Service Attack in Cloud Computing Environment, International Journal of Security and Its Applications, Vol.9, No.9, pp. 197-202, 2015.

[9] Kishu G., Ashwani K. A Review on Data Leakage Detection for Secure Communication. // Volume-7 Issue-1, October 2017 International Journal of Engineering and Advanced Technology (IJEAT)

[10] Gasımov V.A., Aliyeva Sh.Kh. The role of cloud technology in the formation of digital economy. // International Conference "Digital economy: modern challenges and real opportunities", UNEC, Baku, 2020.

[11] Gasimov V.A., Aliyeva Sh. Kh., 3-Tier Architecture for Edge, Fog and Cloud Computing in the Implementation of IoT Technologies. // 5th International Congress on 3D Printing (Additive Manufacturing) Technologies and Digital Industry 2021 3-5 June, 2021 - Antalya, Turkey.