VIRTUALIZATION SECURITY: A GATEWAY TO SECURE CLOUD COMPUTING

Ranabhat Saugatdeep
Moscow Institute of Physics and Technology (MIPT), Moscow, Russia, ranabkhat.s@phystech.edu

Alexey N. Nazarov
Federal Research Center Computer Science and Control of Russian Academy of Sciences, Moscow, Russia, a.nazarov06@bk.ru

Tuleun Terhemen Daniel
Moscow Institute of Physics and Technology (MIPT), Moscow, Russia, tuleun.t@phystech.edu

DOI: 10.36724/2664-066X-2022-8-6-2-9

ABSTRACT

Lately, the most efficient solution for an organization and individual of internet based distributed computing platforms is cloud computing. Processing, storage, and data management are just a few of the useful services that end users can get from cloud computing. However, it raises a lot of issues with privacy and security which needs to be resolved. Major component of cloud computing is virtualization technology, which helps to develop complex cloud services based on the externalization and composition of these resources. The primary concern with cloud computing security is virtualization security. The collective measures and methods that ensure the safety of a virtualization environment are referred to as virtualization security. It tackles the security risks that virtualized components encounter, as well as techniques for mitigating or preventing them. In recent days, attacks are mainly aimed either to the virtualization architecture or the infrastructure. We prefer to examine the security holes associated with virtualization in this paper and how concentrating on virtualization security might ultimately result in safeguarding cloud computing platform. Through this paper we tend to highlight the recent progress and an overview of the existing works performed on various dimensions of the cloud security. We conclude our paper by making several recommendations with respect to the attack vector for supporting cloud protection with a mathematical LP model. .

KEYWORDS: *Secure Cloud Computing, Virtualization Technology, Vir-tualization Security, Virtual Machine (VM), Data Privacy and Integrity.*

1. ntroduction

The provision of on-demand computer services, including applications, storage, and processing power, often over the internet on a pay-as-you-go basis, is known as cloud computing (CC). The location of service and other factors, like the operating system and underlying hardware on which it is running, are key concept in cloud computing, which are mostly irrelevant to the user. As an evolving computing model based on the Internet, it offers consumers quick and convenient data storage and network service, with the ability for computing resources to be dynamically deployed and shared in a scalable data center. CC is clearly superior to traditional self-hosting approach in terms of cost, speed of deployment, and flexibility; as a result, it is well suited to provide infrastructure services, platform services, software and storage services, among many other services. One of the primary concerns with CC has always been data privacy because the data needs to be secure from outside parties or malicious actors. Since cloud computing is used to share data, data theft is still a major danger that affects both consumers and cloud service providers (CSP) and is highly widespread.

Virtualization is a major technology for cloud computing services, facilities, and the consolidation of several standalone systems onto a single hardware platform by virtualizing computational resources (e.g., network, CPUs, memory, and storage). Virtualization is made possible by hardware abstraction, which conceals the complexity of controlling the physical computing platform and facilitates computing resource scaling. Hypervisors are used to implement it. A hypervisor is in charge of isolating Virtual Machines (VMs) so that they do not directly access the virtual disks, memory, or programs of other VMs on the same host. These two features are important aspects of cloud computing because they enable resource sharing and pooling in order to improve agility, flexibility, lower costs, and increase business value. CSP make substantial efforts to secure virtualization techniques by attempting to eliminate or reduce vulnerabilities, threats, and attacks. However, given the features of virtualization, cloud computing is today facing many new security concerns which can jeopardize personal privacy, company interests, and even state security. The cloud computing instances, such as Amazon's Simple Storage Service's service outrage and Google customers' documents leakage, have prompted concerns about the security of CC technology. In reality, the security issue has become a major impediment to the growth of cloud computing. Only by building a comprehensive information security defense system based on a detailed examination of all types of security problems can we ensure the healthy and sustainable development of CC. The most significant distinction between cloud computing and traditional IT environments is the virtual computing environment, which makes security more difficult. Through virtualization technology, different levels of application systems, such as server, software, data, network, and storage, can be segregated from one another, removing the reliance on physical devices for traditional IT architecture and transforming infrastructure into virtual resources that can be flexibly adjusted on demand. However, typical security tactics and strategies begin to fail in the virtual environment, resulting in new security challenges such as attacks between virtual machines or between the VM and the host, DDoS attacks, anti-virus, data or application security isolation, and so on.

This article presents the widely used virtualization technology, analyses the security risks associated with virtualization in cloud computing and based on their categories, recommends appropriate mitigation strategies.

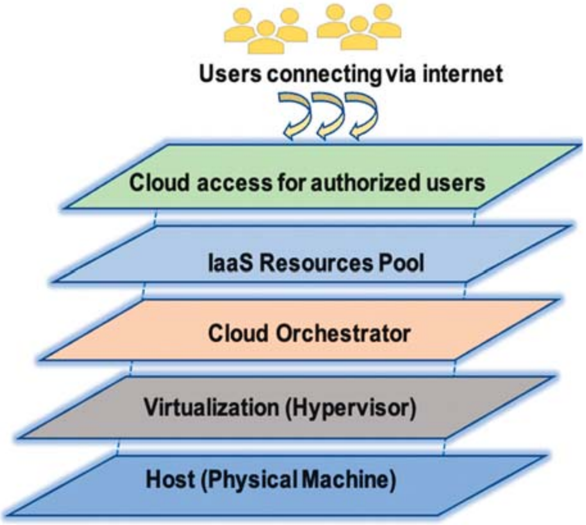
Users connecting via internet
Cloud access for authorized users
IaaS Resources Pool
Cloud Orchestrator
Virtualization (Hypervisor)
Host (Physical Machine)

Fig. 1. Cloud computing stack

2. Virtualization components

By adding a second layer of execution, including their own administrator job, virtualization techniques and virtualized architectures call for effective management and security protection. This layer consists of a number of different aspects, each of which contributes a specific part in the virtualization process as shown in Table 1 and thus could be a fresh target for malicious attack. The attack surface is increased by the virtualization layer's introduction of a complex mix of software elements at various levels of the computing architecture (such as the operating system, communication, administration, and interface), each with its own administrator credentials. While there is no doubt that virtualization approaches improve security, they also come with higher security concerns that must be considered while implementing a robust and safe virtualized infrastructure.

Table 1

Core components of virtualization

No.	Virtualization Components	Purpose
1	Host Machine	The physical device hosting the virtualized environment and its host operating system. The hypervisor operates on the host operating system, which also controls the physical hardware underlying the virtualized environment.
2	Hypervisor	Serves as a bridge between virtual machines and the underlying physical equipment. By sharing physical resources, it mediators all hardware requests made by virtual machines to physical hardware.
3	Virtual Machine Monitor	It records the actions taken by virtual machines. hardware requests are forwarded to actual resources and resource sharing across various virtual machines is supported.
4	Management Server	In charge of controlling virtual machines directly, combining services, assigning resources, moving virtual machines, and ensuring high availability.
5	Management Console	The core element of the virtualization software that gives users access to a management interface for setting up and controlling virtual machines.
6	Guest Machine	Utilizing the hardware abstraction offered by the virtual machine monitor, instantiate the virtualized (encapsulated) system composed of the operating system and applications, commonly known as virtual machines.
7	Network Component	Facilitate the creation of virtual networks where virtual network equipment (such as switches and routers) are entirely managed by software and the network stack and protocols are emulated to closely resemble actual ones.
8	Virtual storage	Provides every element needed to abstract physical storage in a single storage device that may be accessed directly or across a network.

3. Survey of related work

According to Sumter, L.Q. et al., [1] the creation of a system that tracked the movement and processing of data stored in the Cloud. There is a need for a security captured device on the cloud to ensure that users' data is secure and safe from security threats and attacks. Based on a case study, the proposed implementation was incorporated in a small Cloud computing environment. This proposal is only for the small-scale cloud framework not for large scale cloud domain. It is definitely used for provide security assurance to the users while communicating through the cloud domain or environment.

Hocenski [2] gave a broad overview of the security issues, requirements, and complexities that many CSP face. They characterized twenty recommended security approaches and their Cloud computing requirements that CSP should strongly consider as they develop or refine their compliance programmes.

All cloud computing services are linked to the virtualization technique. Iaas, PaaS, SaaS, NaaS (network as a service), and one more service that is entirely dependent on virtualization is known as virtualization as a service. The author of [3] stated that the security challenges how to effect cloud virtualization and what kind of security issues users and customers of cloud environment face. The security of virtual machines has already been prioritized and prioritized. The risk is a critical asset in cloud computing virtualization, and its mitigation at that virtualized level is being monitored by those people surveyed. In her paper, various security flaws are identified as existing or occurring now, and different algorithms by protocol and rules are applied to provide security to the virtualization layer.

Two types of controls in the cloud computing domain: physical control and virtual control were put forward in [4]. Encryption techniques must be implemented and used in the cloud. Encryption techniques can be used to encrypt data or information and secure and protect communication media that exists between the client and the cloud server. One main benefit of encrypted data is that it prevents data loss. We can use prevention policies to prevent data loss. Access control policies are also available to verify user authentication and protect against unauthorized access. Allow for the safe migration of data from a private cloud environment to a public CSP.

The fundamental problem, problems that users have while attempting to use the cloud computing virtualization application and how cloud computing has been successful in dealing with some issues such as data loss, data access, and data storage are explored in [5]. CC is the use of scientific knowledge to the reduction of some critical assets like cost reduction, hardware reduction, and money reduction. Only these notions are used in CC. Virtualization is mostly used in CC to share resources and create an isolated image, often known as a virtual image because it is not real. Another reason why virtualization is employed in CC is for dynamic resource allocation. The author discussed several virtualization challenges such as an infected application, data accuracy and mass data loss in cloud computing in this study. These challenges can be addressed by utilizing scientific knowledge that is virtualized.

Sabahi, F. et al., [6] discussed about Hyper-visor which helps to safeguard the environment of cloud computing technology and proposed a virtualized architecture for cloud security as well. The author attempted to explain various terminologies that aid in the security of virtualization in CC such as, reduce workload, decentralized security tasks between hypervisor and virtual machines and distribute the centralized security system When compared to a decentralized system, a centralized system has fewer flaws. One advantage is that defining the distributed system is beneficial for fault tolerance. According to the author, anything built by humans in this digital age is potentially breakable. However, the essential idea or concept is that decentralized application access presents a security concern in the cloud computing environment, which can cause a huge issue or problem while moving data in the cloud. So, from a security standpoint, it is necessary to control the security of the cloud computing environment as well as virtualization in the cloud environment.

With the use of Security Oriented Architecture, the challenges to networking environment in cloud computing domain can be evaluated [7]. The Security Oriented Architecture domain can carry out a number of tasks. As a result, it reduces the operation of information technology, saves money for cloud users giving a higher quality of flexibility and delivers needed services. This paper discussed the dangers of utilizing virtualization in cloud computing.

Security metrics are proposed in [9] that providers could use to evaluate the security of their services describing necessary policy rules and required procedures. In general, they emphasized to systematize in great detail, structure them according to the proposed levels and summarize the threats and vulnerabilities of the most common SaaS cloud model.

4. Security risk in virtualization

A hypervisor is used to virtualize resources, which allows for the dynamic allocation of resources to virtual computers (VMs). In cloud virtual systems, cryptography is used to safeguard data in transit from user to the cloud, but data must be decrypted in memory. This opens the door to privacy violations because virtualization improves an instance's memory pages virtually transparently, allowing a hostile provider to get data.

Table 2

Category of virtualization security risk

No.	Risk Type	Description
1	Virtual machine migration	VMs can be moved to another physical machine via "VM hot migration," which is done without shutting down the virtual machine. VM migration can be done for a variety of purposes, including load balancing or preserving fault tolerance. Data privacy and integrity may be lost as a result of the transfer, which exposes the VM's contents to the network.
2	Virtual machine escape	Users can achieve mutual isolation and resource sharing on a virtual computer. In a virtual computer, a software typically should not interfere with other virtual machines. VM escape is the term for when applications operating in a virtual machine are able to get beyond isolation limits and execute directly on the host machine in some circumstances due to technological restrictions and flaws in virtualization technologies. If the virtual machine escape attack is successful, the host and the hypervisor are both in extreme threat.
3	Rookit attack	A specific type of malware called a rootkit conceals itself on the installation target and targets certain files, processes, and network links. What is more typical is that rootkits are frequently used in conjunction with other harmful software like Trojans and backdoors. Rootkits conceal information by loading unique drivers and changing the kernel of the operating system.
4	Denial of service attack	VM uses shared resources from a physical machine. A denial-of-service attack will occur in the virtual environments if an attacker uses one virtual machine to take full control of the host computer's resources, causing other virtual machines' resources to be disturbed or even crash due to a lack of resources.
5	Virtual machine monitor problem	The key component of virtualization is the virtual machine monitor, which generates or manages virtual resources as well as manages and isolates virtual machines. If the virtual machine monitor is penetrated, the attacker will have access to all other virtual machines it maintains as well as the metadata it stores about those virtual machines.
6	Decoupling attacks on virtualization platforms	In the conventional working context, just the physical machine with the system vulnerability is vulnerable, and the attack reach is very constrained. A single virtual machine can be used to attack the entire virtual vulnerability platform by several rent users using a cloud computing virtualization platform to share information across the entire system.

5. Counter measures

This section may each be divided by subheadings or may be combined. Following the classification of security risks, we provide several countermeasures and recommendations. The overall virtualization security protection model is shown in Figure 2.

a. Virtualization deployment planning, design, management

Administration of the infrastructure should be more rigorously organized than that of a physical one because it is far more important. In fact, the virtual infrastructure should be seen as a full machine in and of itself, housed in a single physical location with strict security constraints. Planning contributes to assuring security and adherence to all essential organizational policies. To maximize security while minimizing costs, organizations should address security from the outset of the systems development life cycle. Organizations must follow basic ICT security recommendations and practice such as keeping software up to date using host-based firewalls, antivirus, and IDS, to mention a few.

b. Restric and protect administrative access

The security of the entire virtualization infrastructure is dependent on the virtualization management system, which manages the hypervisor and supports operations on guest operating systems as well as other administrative tasks. Organizations should limit access to the virtualization management system or any other console interface, allowing only authorized administrators to access the hypervisor.

c. C trols against Hypervisor-based Attacks

Some of the strategies used to protect against hardware-based assaults are also successful in protecting hypervisors. Hardware-assisted Virtualization (HaV) is an efficient method that provides hypervisor security. HaV protects hypervisor integrity and improves isolation of system hardware resources. Hardware physical memory virtualization is possible with HaV; memory addresses are transformed from guest virtual to guest physical, then to system physical [8]. The system also includes a secure Input Output Memory Management Unit (IOMMU), which enables virtual machines to access peripheral devices directly. As a result, cyberattacks from malicious devices that could compromise the hypervisor's integrity are avoided.

On top of virtual machine migration, software-based security solutions secure virtual machines where tenants live. These solutions safeguard virtual computers both internally (at the operating system level) and externally (hypervisor level). Memory isolation, device isolation, and network isolation can all help to secure VMware's hypervisor.

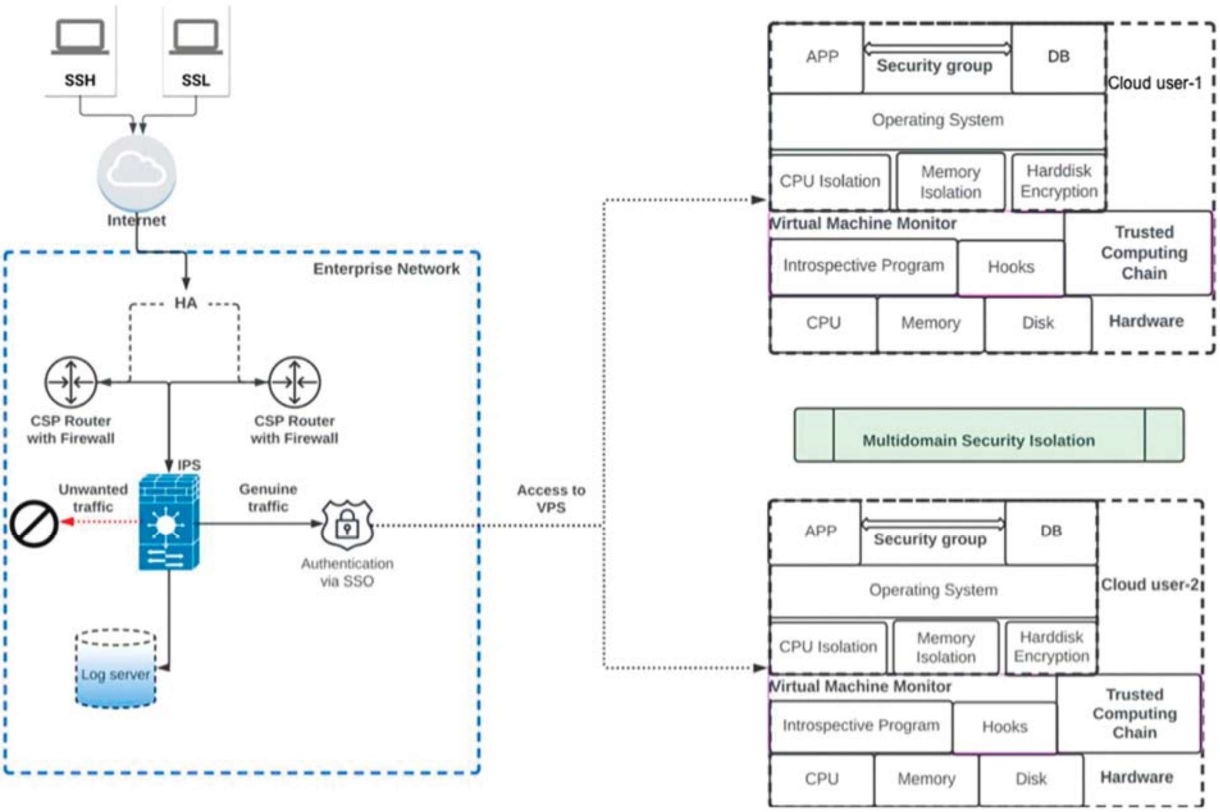

Fig. 2. Architecture of virtualization and cloud computing security

d. Access control for virtual network

The virtual network access control method can be accomplished using the Open vSwitch (OVS) technique, which inspects network data packets moving in and out through the security agent. The kernel driver layer's security agent enables virtual ports in the data flow route to load control function and accompanying security policy. This security agent mode can perform operations like security control optimization and policy synchronization. Furthermore, the Open vSwitch approach can be used to achieve several functionalities such as access control between vLANs, security domains, or virtual machines, as well as dynamic construction and migration of security policies.

e. S pshots and image management

Passwords and personal information may be concealed in images and snapshots. A company gains considerable security and operational benefits from proper image management. Images must be properly safeguarded against unwanted access, alteration, and replacement. Keeping a limited known good images of guest OSs is a recommended approach. Snapshots are more dangerous than images since they carry the RAM memory state. This could contain critical information that was not even kept on the drive itself, such as clear text passwords.

f. C trol the access to VMs

Limited access to virtual environments and effective privilege locking are required to reduce code exploitation via malicious software.

g. Isolate guest OS and perform partitioning

Policies for physical and logical partitioning should also be implemented for hypervisors. Partitioning prevents unauthorized access and reduces the possibility of code injection from one VM into another, as well as the risk of denial of service due to resource saturation. Side-channel attacks are also mitigated by VM separation. Isolation strategies have been used in this context to limit:

- access to VMs;
- communications between VMs
- communications from VMs to hypervisor.

h. Monito the resources

The hypervisor or VMM can be configured to monitor running virtual machines, network traffic, memory, and processes (introspection). Introspection also has auditing features as well as security controls like firewall policy, intrusion detection, and access control. Network-based security policies should not hinder traffic in a typical network arrangement. Active monitoring detects changes in system status and allows hook functions to be embedded in the monitored virtual machine.

Enhancing the virtualization security protection in cloud computing through the aforementioned features in Figure 2 will effectively boost cloud computing virtualization security, hence improving the security and reliability of cloud computing services.

6. Security-policy based model

A security policy based on rules (criteria) is proposed based on the proposed security measures related to the above-mentioned threats and protection measures. The considered measures and rules are essentially protection functions, used both to identify and prevent attacks and to assess the risk of attacks and intelligent monitoring of information security of modern info communications, including on a cloud model. The types of information attacks listed in the table are due to the technological features of VMs and the cloud resources used in specific systems. In general, for the calculation justification of cloud resources through which these attacks can be carried out, you can use the following methodological results.

Based on the analysis of [10] known cloud deployment models and the IaaS dynamic traffic model, the IaaS resource allocation model was developed. It is used to evaluate resources and tasks for the entire IaaS structure. The model can be used as a base for automating practical methods for multivariate calculation justification of necessary investments in IaaS design solutions with optimization of information flows. Developed on the basis of the entropy approach, the IaaS model of the system" information sources - boundary nodes " describes the most likely distribution of data from information sources over IaaS boundary nodes fixed in space, and all its coefficients have a certain physical meaning. The model allows you to get the values of the upper and lower estimates of the number of virtual connection (VC) as a function of the bit rate values of information sources. Based on the analysis of a stepwise bit dynamic model of content traffic of different categories of IaaS, resource allocation model of IaaS, a method has been developed for distributing the required resource of an IaaS fragment between all content categories in the interests of all resource tenants. The problem of conditional optimization in the "entropy setting" is formulated and solved by the method of undetermined Lagrange multipliers to find the distribution matrix of virtual connections between all tenants of the IaaS fragment resource, which are supplied with different categories of content.

Based on the results of solving this problem of conditional optimization, an optimization model for the distribution of virtual connections from content sources of different categories by service tenants in the IaaS fragment was obtained. The model reduces to solving a complete system of linear equations, and all its coefficients have a certain physical meaning. The model allows you to get the upper and lower estimates of the number of virtual connections as functions of the values of bit or packet speed of content sources of different categories. The conditions of model applicability, accuracy and stability of decisions on estimating the number of virtual connections in the IaaS fragment are determined.

The results obtained in [10] can be useful in solving the problem of structural-topological synthesis of IaaS at the pre-project stage.

Risk- an object of system of virtualization (SV) are being attacked by the intruder, consists of two components:

a) The probability of failure counter attack against the user (hereinafter - the failure of the object) or the probability of a successful attack.

b) Evaluation (e.g., financial, material, time to repair the damage, etc.) scale consequences (damage) of a successful attack.

The object of risk is considered to be sufficiently protected if given the opportunity to overcome potential barriers probability of a successful attack (the probability of the risk, the probability of failure or vulnerability of the object of risk) $P_A^Y = \left(1 - P_З^Y\right)$ than minimum value $P_{А-ДОП}^Y$, i.e., $P_З^Y \geq 1 - P_{А-ДОП}^Y$ – the condition of the feasibility, (1) where $P_З^Y$ - the probability of a successful counter attack (immunity, the success of the object of risk) subject to risk.

For any object risk of SV in the general case there is a complete system (list) security functions or attributes, each of which is in Table 3, denote the binary logic variable with the appropriate subscript.

Table 3

Security Features

Designation of security functions	**Appointment of security functions**
X_1	Preventing the occurrence of conditions conducive to the generation of (occurrence) destabilizing factors Preventing the occurrence of conditions conducive to the generation of (occurrence) destabilizing factors
X_2	Warning immediate manifestations of destabilizing factors
X_3	Detection manifested destabilizing factors
X_4	Prevention of exposure to risk in the manifested and revealed destabilizing factors
X_5	Prevention of exposure to risk on the manifest, but the undetected destabilizing factors
X_6	Detecting the impact of destabilizing factors on the subject of risk
X_7	Localization (restriction) found the impact of destabilizing factors on the subject of risk
X_8	Localization of undetected exposure to risk by destabilizing factors
X_9	Dealing with the consequences of the localized impact of the detected object on the destabilizing factors risk
X_{10}	Dealing with the consequences of undetected localized exposure to risk by destabilizing factors

The result of each of the Security Functions, or the outcome is a random event and can take two values – success or failure. It is assumed that a binary logical variable X_j, $j = 1 \div n$, $n = 10$ is equal to 1 with probability P_j if the execution of the $j-$ Security Functions has led to the failure risk of the object, and this binary logical variable equal to 0 with a probability $Q_j = 1 - P_j$ otherwise.

In general, the logic function (L-function), the success of the attack, realizing the impact of destabilizing factors as [11] and [12], $Y = Y\left(X_1, \ldots, X_n\right)$, and the probability function (P-function, P-polynomial) the risk of failure of the object – $P\left(Y = 1/X_1, \ldots, X_n\right) = \Psi\left(P_1, \ldots, P_n\right) = PY$.

According to the general case of [11, 12], L-function of the success of an attack is:

$$Y = X_1 X_2 \left(\overline{X_3} X_4 \vee X_3 X_5\right) \times \\ \times \left(\overline{X_6 X_7} X \ \vee X_6 \overline{X_8} X_{10} \vee \overline{X_6} X_7 \vee X_6 X_8\right) \qquad (2)$$

and the probability of success of an attack can be calculated using the B-polynomial

$$PY = PY\left(P_1, P_2, \ldots, P_{10}\right) = P_1 P_2 \left[\left(1 - P_3\right) P_4 + P_3 P_5\right] \times \\ \times \left[\left(1 - P_6\right)\left(1 - P_7\right) P_9 + P_6 \left(1 - P_8\right) P_{10} + \left(1 - P_6\right) P_7 + P_6 P_8\right]. \qquad (3)$$

The barriers a-h that are created to counteract the negative effects of destabilizing factors on the subject of risk, perform certain security functions that prevent the implementation of the attacks on the subject of risk in SV. Such changes are methodically quite easily and flexibly taken into account by introducing gradations of protection functions (1).

By analogy with the above, we assume that the binary logical variable X_{ij}, *i=1,2,…,n, n=10* corresponding to the *j-th* gradation of the known *j-th* security function, is equal to 1 with probability P_{ij} , if because of it the execution of the known *j*- th security function led to the failure of the risk object, and is equal to 0 with probability $Q_{ij} = 1 - P_{ij}$ otherwise.

In view of above specific a-h barriers to develop constructive solutions to counter its list of security functions in Table 3 appropriate to expand according to Table 4.

New security functions for SV are the logical components of the functions of the Tables 2 and 3:

$$X_i^{SV} = \begin{cases} X_i \vee X_{ij}, \ \forall X_{ij} \neq \Phi, \ i=1,2,\ldots,n, \ n=10, \ j=a,b,\ldots h, \\ X_i, \ \forall X_{ij} = \emptyset, \ i=1,2,\ldots,n, \ n=10, \ j=a,b,\ldots h, \end{cases} \qquad (4)$$

where $\emptyset$ – empty set.

Table 4

Security functions for SV

Designation of security functions i**=1,2,…10**	**Appointment of security functions**
X_{ia}	Virtualization deployment planning, design and management
X_{ib}	Restrict and protect administrative access
X_{ic}	Controls against Hypervisor-based Attacks
X_{id}	Access Control for Virtual Network
X_{ie}	Properly manage images and snapshots.
X_{if}	Control the access to VMs
X_{ig}	Isolate guest OS and perform partitioning.
X_{ih}	Monitor the resources

Substituting (3) into (1) obtained the L-polynomial for SV

$$Y^{SV} = X_1^{SV} X_2^{SV} \left(\overline{X_3^{SV}} X_4^{SV} \vee X_3^{SV} X_5^{SV}\right)*$$
$$*\,(\overline{X_6^{SV} X_7^{SV}} X_9^{SV} \vee X_6^{SV} \overline{X_8^{SV}} X_{10}^{SV} \vee \overline{X_6^{SV}} X_7^{SV} \vee X_6^{SV} X_8^{SV}) \qquad (5)$$

To assess the probability $Q_i^{SV}\ \forall X_{ij} \neq \Phi,\ i = 1,2,\dots,n$, $n = 10,\ \ j = a, b, \dots h$, let 's apply the Bayes formula,

$$Q(X_{jr}^{SV}/X_j^{SV}) = \frac{Q(X_{jr}^{SV})Q(X_j^{SV}/X_{jr}^{SV})}{\sum_{\substack{r=a \\ \forall X_{jr} \neq \emptyset}}^{f} Q(X_{jr}^{SV})Q(X_j^{SV}/X_{jr}^{SV})}, \forall X_{jr} \neq \emptyset. \qquad (6)$$

Using (6), the expression (3) for the B-polynomial and the formula (1) for a new kind of reachability condition are refined. Formula (6) can be used for interactive training (setup, identification) of the B-model (5) based on statistical data in order to clarify the current risk value.

Conclusion

As cloud computing technology advances, security risks and threats will increase in the future. Virtualization, the foundation of cloud computing is vulnerable to security risks, which has slowed down cloud computing's expansion and widespread adoption. However, despite the fact that many features are created with these objectives in mind, it poses a risk to secrecy, integrity, authenticity, and non-repudiation.

To secure user's application and their cloud account, users must enable all risk mitigation rules because security issues can take many different forms. Analysing the primary security risks that virtualization technology faces, enhancing virtualization's security defenses are very important. It is challenging to comprehend all the security concerns and privacy threats with the development of effective solutions. Work must be done to support virtualization and cloud computing, as well as to comprehend the difficulties posed by cloud security issues.

This paper also intends to give this field of study a new direction and assist researchers in identifying potential countermeasures to such risks and threats. Based on new security features that take into account the technological features of the general case of cloud virtualization, a new Security Protection Model has been developed. The proposed LP-models (LP-polynomials) for the general case of an arbitrary risk object SV create prerequisites for assessing the fulfilment of the reachability condition for each specific risk object.

References

[1] R. La'Quata Sumter, "Cloud Computing: Security Risk Classification". *ACMSE Oxford. USA*, pp. 15-17, Apr 2010. https://doi.org/10.1145/1900008.1900152

[2] Kresimir Popovic et.al. "Cloud Computing Security Issues and Challenges" Proc. 33rd *Int'l Convention on Information and Comm. Technology. Electronics and Microelectronics* (MIPRO 10). IEEE Press, pp. 344-349, Jun 2010.

[3] H.M. Anitha, P. Jayarekha, "Security Challenges of Virtualization in Cloud Environment". *International Journal of Scientific Research in Computer Science and Engineering*. Vol. 6, Issue. 1, pp.37-43, Feb 2018. https://doi.org/10.26438/ijsrcse/v6i1.3743

[4] T. Swathi, K. Srikanth, S. Raghunath Reddy, "Virtualization in Cloud Computing". *International Journal of Computer Science and Mobile Computing*, IJCSMC, Vol. 3, Issue. 5, pp. 540-546, May 2014.

[5] L. Malhotra, D. Agarwal and A. Jaiswal, "Virtualization in Cloud Computing". *Journal of Information Technology and Software Engineering,* Dec 2014, 4:2. DOI: 10.4172/2165-7866.1000136

[6] Farzad Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology". *International Journal of Machine Learning and Computing*. Vol. 2. No. 1, Feb 2012. https://doi.org/10.7763/ijmlc.2012.v2.87

[7] Mladen A. Vouch, "Cloud Computing Issues. Research and Implementations". *Journal of Computing and Information Technology*. pp. 235-246, Jun 2008. https://doi.org/10.1109/ITI.2008.4588381

[8] Z. Gilani, A. Salam, and S. Ul Haq, "Deploying and managing a cloud infrastructure: real world skills for the CompTIA cloud+ certification and beyond," *Wiley*, Jan. 2015.

[9] D. Georgiou, and C. Lambrinoudakis, "Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR)," Information, 11(12), p. 586, Dec 2020. Available at: https://doi.org/10.3390/info11120586

[10] A.N. Nazarov et al, Alireza Nik Aein Koupaei, Anshita Dhoot, Asyraf Azlan & Seyed Milad Ranaei Siadat, "Mathematical modelling of infrastructure as a Service," *Systems of Signals Generating and Processing in the Field of on Board Communications*, Mar 2020. Available at: https://doi.org/10.1109/ieeeconf48371.2020.9078629

[11] A.N. Nazarov, & M.M. Klimanov, "Estimating the informational security level of a typical corporate network". *Automation and Remote Control*, no, 71(8), pp. 1550-1561, Aug 2010. https://doi.org/10.1134/s0005117910080059

[12] A. Nazarov, M. Klimanov, "Characteristic analysis of logic and probabilistic model of information security". Sofia, Bulgaria, *Proceedings of International Workshop on Distributed Computer and Communication Computer and Communication Networks*, pp. 154-164. Published by Research and Development Company "Information and Networking Technologies". Oct 2009.