International Journal of
Science and Engineering Investigations vol. 8, issue 91, August 2019
Received on August 21, 2019 ISSN: 2251-8843

# Proactive Approach for Security of the PAAS Model of Cloud System Based on Vulnerability Assessment

Maryna A. Yevdokymenko[1], Anastasiia S. Shapovalova[2], Olena Nevzorova[3]
[1,2,3]Infocommunication Engineering Department, Kharkiv National University of Radio Electronics
([1]marina.ievdokymenko@nure.ua, [2]anastasiia.shapovalova@nure.ua, [3]olena.nevzorova@nure.ua)

***Abstract-*** A proactive approach to the quantitative assessment of the security of cloud systems is proposed, which allows assessing the risks at the user and network level, which significantly affect the security of the cloud system under consideration in the PaaS model. The novelty of the approach is that the risk assessment of the cloud system is carried out taking into account the separation of vulnerabilities in two groups: with existing countermeasures and without them, as well as in assessing the spread of the attack at the network level, taking into account the free address space. This allowed us to assess in more detail the possible risks in the cloud system to minimize vulnerabilities, which in turn will lead to minimization of the damage that can be caused both to the user and the provider of the cloud system.

***Keywords-*** *Cloud, PaaS, Security, Vulnerability, Virtualization, Risk Assessment*

## I. INTRODUCTION

The main directions of the development of information and communication networks, which have appeared in recent years and have significantly influenced the global computing infrastructure, are the development of cloud technologies, the growth of mobility, as well as the intensive growth of traffic and a change in its structure. In this regard, telecommunication equipment and data transmission channels are experiencing constantly increasing loads, often exceeding the nominal performance. Also, a number of factors arise that require increased flexibility of network resources, which include prioritization of various types of traffic, unpredictability of congestion of end devices, insufficient flexibility of network protocols and limited bandwidth of the physical data transmission medium. Attempts to solve such problems by traditional means of traffic balancing cause the consumption of resources of network channels and devices for transmitting many service messages of routing protocols, the complexity of reconfiguring the network in overload mode, and the limitations and complexity of setting up various scenarios for the operation of network devices. At the same time, one of the most important tasks in building and configuring info-communication networks, as before, is to provide the necessary level of quality of services to the end user. Providing the flexibility of managing traffic flows bypassing the above difficulties is possible using software-configured networks and cloud systems built using them [1, 2].

It is known that one of the basic principles of cloud computing is the ability to use the same computational resources by different users (either simultaneously or at different times), on the one hand, economically beneficial to companies that provide resources, and on the other hand, causes increased attention to security, isolation of data and software products, differentiation of rights.

Moving data and applications to cloud storages implies a transition from ensuring the security of the perimeter of the information and communication network, on which all protection of classical systems is based, to ensuring the protection of information itself. Now security issues concern not only the user / client - how the provider will handle his data, but also the provider - how much one can trust the user from what external and internal threats it is necessary to protect the cloud infrastructure. At the same time, the main share of data protection risks lies with the provider - the service provider. In this regard, there is a need for a detailed analysis of information security threats arising from the use of cloud computing systems.

## II. FEATURES ANALYSIS OF THE CONSTRUCTION AND OPERATION IN THE CLOUD SYSTEMS

As is known, in comparison with classical info communication networks, cloud technologies are characterized by a faster implementation process with lower upfront costs, the ability to scale at any moment in time and dynamically change the provided power of computing resources [3]. The architecture of deployed cloud systems directly depends on the goals of its use, the services provided, and also on the requirements of the users themselves.

At the heart of the creation of a cloud system is the virtualization technology that allows the user to provide computing resources, abstracted from their real hardware. Thus, it improves the adaptability virtualization, flexibility and efficiency of use of computing power, sharing resources with different hardware devices serving a multi-user customer. In addition, virtualization speeds up the deployment of workloads, increases their productivity and availability, and also makes it possible to automate many processes. Depending on this, cloud systems are classified on the model of the provided service and deployment model (Fig. 1).

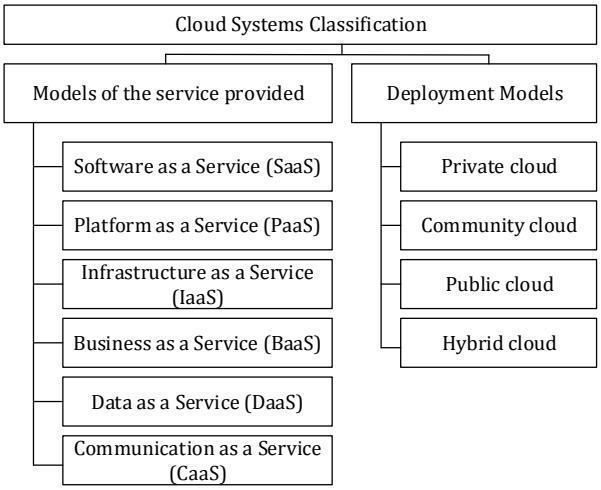



Figure 1. Classification of cloud systems

There are two virtualization approaches for creating a cloud system: using a hypervisor that separates virtual machines from a server with dynamic allocation of computing resources (Amazon, Azure, VMWare) and isolated containers (OpenVZ, LXC (Linux Containers), Docker). However, from the point of view of ensuring the security of the cloud system, these two approaches are quite vulnerable. So, for example, by hacking one of the containers in the cloud, a malicious user can gain privileges to the main system, and thereby neighboring containers and, accordingly, other users will be compromised.

Based on the foregoing and in accordance with a document published by IEEE "ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing", specifications of the European Telecommunications Standards Institute (ETSI) and the National Institute of Standards and Technology (NIST) [4 - 6] for the successful provision of services and computing resources to end users, the requirements for the cloud system are shown in Fig. 2.

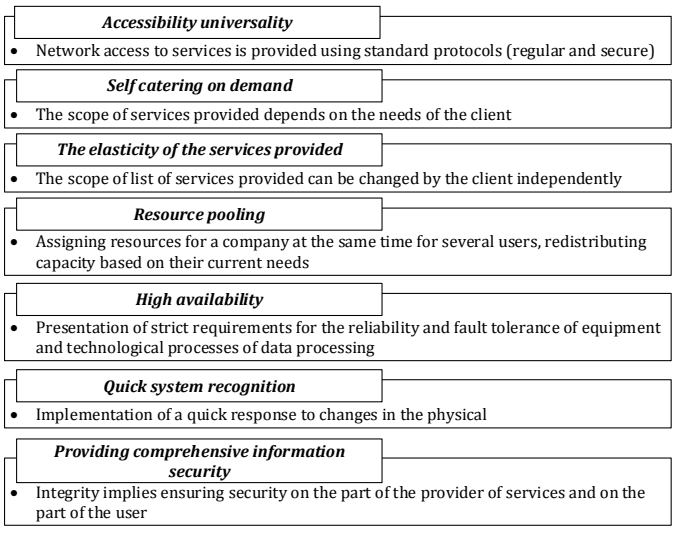



Figure 2. Requirements for developing cloud systems

However, even if the cloud system meets the requirements to the fullest extent possible, it is almost impossible to ensure complete data security. This is due to a decrease in the level of controllability of information processing processes and the dynamism of the resource allocation model. So, for example, the user does not have the ability to use additional means of limiting physical access to equipment. And on the other hand, a number of influences on the part of the users themselves can lead to a sharp reduction in the number of available computing resources on the provider side. In this regard, an urgent scientific task arises of providing comprehensive protection of the information of the cloud system both from the side of the provider and from the end user.

## III. Cloud Information Security Threat Analysis

To build cloud systems, it is proposed to use the concept of multi-level security (Fig. 3), which allows increasing the time of hacking the system, which, in turn, will track the attempt to hack and block the attacker.er. Do not number text heads-the template will do that for you.

| | | | | |
|---|---|---|---|---|
| Services level | Service and Application Security | | Data protection | |
| Controls level | Identification and authentication | Access control | User data protection | Audit and Security Management |
| Virtualization level | Virtualization Environment Protection | | | |
| Equipment level | Network Perimeter Protection | Security operating environment | Infrastructure security | |

Figure 3. Simplified architecture of a cloud information security system

The main difference between security in the cloud system and traditional information and communication networks is the need to use additional protection mechanisms that are unique to cloud systems [7], for example:

1. Difficulties in moving conventional servers to the computing cloud. The security requirements for cloud computing are no different from the security requirements for data centers. Access via the Internet to the management of computing power is one of the key characteristics of cloud computing, therefore, delimiting access control and ensuring transparency of changes at the system level are one of the main protection criteria.

2. The dynamism of virtual machines. Due to the fact that virtual machines in the cloud system can be moved and copied between physical servers, which affects the development of the integrity of the security system. However, vulnerabilities in the operating system or applications in a virtual environment spread unchecked and often manifest after an arbitrary period of time (for example, when restoring from a backup). In a cloud computing environment, it is important to securely capture the security status of the system, regardless of its location.

3. Vulnerabilities inside the virtual environment. In the development of cloud systems, as a rule, the same operating systems are used, which causes a high probability of infection with malicious software. In addition, with the growth of virtual machines used, the “attacked surface” of the cloud system also grows. And considering that inactive virtual machines are also at risk of infection and it is impossible to run security software, it is recommended to use intrusion detection and prevention systems capable of detecting malicious activity inside virtual machines, regardless of their location in the cloud, and at the hypervisor level.

4. Perimeter protection and network demarcation. The expansion of the perimeter of the info communication network when using cloud computing leads to the appearance of "bottlenecks" while ensuring security, i.e. protection of a less secure part of the network determines the overall level of security. Therefore, to distinguish between segments with different levels of trust in the cloud, virtual machines themselves must provide protection by moving the network perimeter to the virtual machine itself [8].

5. The impact on the cloud from the user. When users access the cloud system through a browser, it becomes possible to implement many attacks, such as Cross Site Scripting, SQL injection, intercepting web sessions, the "man in the middle" and many others. Therefore, it is recommended to use secure authentication mechanisms and the use of an encrypted connection with mutual authentication.

Based on the foregoing, in order to ensure multi-level security of the cloud system, a proactive approach is proposed in the work, with the help of which it is possible to assess vulnerabilities and subsequent risks.

## IV. Proactive Approach For Security Of The PAAS Model Of Cloud System Based On Vulnerability Assessment

The main criterion for the security of the cloud system is the assessment of existing vulnerabilities and risks. The paper proposes a method for providing multi-level security for the PaaS model, where the user has the right to deploy the created or acquired application created using programming languages, libraries, services and tools supported by the service provider, as well as use databases. At the same time, the user does not manage the basic infrastructure of the cloud, including networks, servers, and operating systems, but has control over the deployed services / applications and can deploy the databases in the cloud storage himself, which, in turn, complicates the process of providing security.

As you know, any cloud system can be visualized both from a physical point of view and from a security point of view. From a physical point of view, such a system can be considered as consisting of several computers, servers and other components of the system, interconnected via a high-speed local area network or WAN. However, when the same system is visualized from a security point of view, it can be divided into user level / service level and network level, which includes various devices (switches, routers, servers, access points, etc.). Therefore, a solution is proposed based on the breakdown of the process of safe user access to the cloud system at the user level and the network level (Fig. 4).

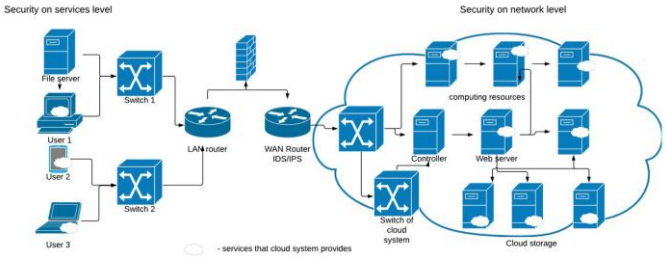



Figure 4. Architecture of a cloud system divided into user and network levels

### A. *User-level vulnerability risk assessment.*

The security of the cloud system depends on factors such as the security of the computer (tablet, smartphone, etc.) of the user who is allocated the necessary applications / services according to the PaaS cloud model, the lack of vulnerabilities in the applications / services provided to the user and the procedures user authorization when accessing the cloud system. Accordingly, if there are vulnerabilities at the user level (lack of anti-virus programs, insecure connection to local networks and the Internet, authorization errors, etc.), then their use by an attacker poses a risk to the cloud system.

When a vulnerability is detected on the user side, it takes time before an appropriate countermeasure is introduced (denial of access, updating the application provided, etc.) During this time, the cloud system and the services themselves are vulnerable to an external attack. To determine the risk of exploiting an existing vulnerability, we use an exponential distribution to quantify the worst-case scenario when an attacker exploited a vulnerability and damaged the cloud system. According to [13], there are the following indicators of potential damage (Table 1):

TABLE I. Vulnerability exploitation potential indicators

| Indicator | Description |
|---|---|
| Absent | Successful exploitation has no loss |
| Low | Successful exploitation of the vulnerability results in a slight decrease in performance, minimal damage |
| Low to medium | Successful exploitation of the vulnerability results in a decrease in the performance of the cloud system, user requests are processed longer than defined in the SLA, which may lead to a decrease in revenue from the use of cloud services |
| Medium - High | Successful exploitation of the vulnerability results in a significant decrease in productivity; serious financial damage |
| High | Successful exploitation of the vulnerability causes catastrophic damage to user data and the cloud. |

Let $S$ be the set of services provided to the user of the cloud system, and $V(y_i)$ be the set of vulnerabilities that are discovered in the services, i.e. $y_i \in S$. $C(y_i)$ is vulnerability criticality indicator of $y_i$, which is understood as the damage caused to the cloud system. Let's divide $V(y_i)$ into two subsets: $V_p(y_i)$ a set of vulnerabilities with existing countermeasures and $V_u(y_i)$ a set of vulnerabilities that do not have protective measures. Then, to calculate the risk $R(S)$, the expression proposed in [8] is

$$R(S) = a_1 \ln \sum_{y_j^p \in V_p(S)} e^{C(y_j^p)} + a_2 \ln \sum_{y_j^u \in V_u(S)} e^{C(y_j^u)}, \quad (1)$$

where $a_1$ and $a_2$ are weights that are used to model the difference in risks created by these two sets of vulnerabilities.

Unfortunately, from a practical point of view, to ensure the security of the cloud system, PaaS models often analyze vulnerabilities at the user level after the cloud system has been exposed. There are also situations where all the most critical vulnerabilities have been fixed, but after some time the cloud system is again affected by the user. This is due to a lack of security analysis of the proposed service / application (especially for open source applications and exploit techniques). This situation necessitates the prediction of risks in the event of new vulnerabilities at the user level. However, most of the approaches used do not predict the future security state of the cloud system in terms of the emergence of new vulnerabilities [10-12]. Therefore, in this paper, it is proposed to evaluate the security of the cloud system not only at a given moment in time, but also in the future. Then let $P_f(y_j^n)$ is the probability of detecting a new vulnerability $y_i^n$, and $y_i^n \in S$ in the services/applications provided, which will give an idea of the risks that the cloud system will face in the future, $C_n(y_i^n)$ is expected indicator of the criticality of the vulnerability, and $P_f(y_j^n)$ is the probability of an attacker using the new vulnerability. Then, to calculate the expected risk $R_n(S)$, we use the following expression:

$$R_n(S) = P_f(y_i^n) \cdot \sum_{y_j^n \in S}^{\infty} C_n(y_i^n) \cdot P_z(y_i^n), \quad (2)$$

*B. Network-level vulnerability risk assessment.*

An analysis of existing studies showed [9, 12-15] that it is network policies that determine the network's susceptibility to the influence of external factors, as well as the intensity of the attack on the network (that is, how widespread the attack can be). A quantitative risk assessment (attack intensity) at the network level includes an assessment of the spread of a possible attack ( $RA$ ) and impact factor ( $IF$ ), i.e. the influence coefficient of an attack through one network element on another.

Then the extent to which the policy allows the spread of attack within the network and the cloud system will be determined by the metric of the spread of attack ( $RA$ ). Attack propagation is estimated by how difficult it is for an attacker to spread an attack over a network in a cloud system using vulnerabilities of the provided services, as well as security policy vulnerabilities.

When analyzing vulnerabilities at the network level, we determine that $N$ many nodes in the network that perform at least one service, $K$ many communication channels connecting nodes in the network. Then $S_n$ the set of services on the node $n$; $P_n$ indicator of vulnerability for the service $S_n$. Based on this, the service that is transferred from one node to another will be defined as $S_{n_1 n_2}$

For further analysis, we introduce an estimate $L_{s_i}$ that determines the vulnerability of the service $s_i$ to an attack. So, $L_{s_i}$ is calculated from $P_{s_i}$ a combined indicator of service vulnerability $s_i$, as:

$$L_{s_i} = -\ln(P_{s_i}) \quad (3)$$

$L_{s_i}$ has a range $[0, \infty)$ and is used to measure the ease with which an attacker can spread an attack from one node to another using the service $s_i$. Thus, if the node $n_2$ can connect to the node $n_1$ using only the service $s_i$, then $L_{s_i}$ is measured as the resistance of the node $n_1$ to the attack initiated by the node $n_2$.

Impact factor assessment is defined as the set of services $S_{n_1 n_2}$ that a node $n_2$ can use to connect to a node $n_1$:

$$IF = -\ln(P_{S_{n_1 n_2}}) \cdot F, \quad (4)$$

where $F$ is level of protection. For protection using a firewall $F = 1$ and implies the highest protection. For protection using attack detection systems (SOA), protection is a value from 0 to 1.

To assess the spread of attacks from the $n$ th node with the disruption of other nodes that are within reach of the $n$ ith node, we construct the minimum spanning tree according to the Prim algorithm for a network segment, i.e. of all those nodes that will be susceptible to attack through the $n$ th node. The weight of this minimum spanning tree will determine how vulnerable this network segment is to attack. The more vulnerable the system, the higher this weight will be. To determine the weight, we use the following expression:

$$W_n = \sum_{n \in T} (\prod P_{s_{mn}}) \cdot \cos t_n, \quad (5)$$

where $\cos t_n$ reflects the cost of damage when a node $n$ in the network is compromised, and $T$ is the set of nodes present in the spanning tree. Then, the attack propagation score is determined by the following expression:

$$RA = \sum_{n \in T} P(n) \cdot W_n. \quad (6)$$

Where $P(n)$ denotes the probability of a vulnerability in the $n$ th node.

The calculation of the risk assessment by external factors (External Factor,) is based on the share of the address space on which the service operates, because it is the address space that is the most "bottleneck" in ensuring the security of the cloud system from external influences. External influences $s_i$ on the service take into account the number of ports $Ports(s_i)$ and IP addresses $IP(s_i)$, while the total number of IP addresses is $2^{32}$, and the total number of ports is $2^{16}$. Thus, the range of this coefficient will begin with a minimum value of 1 for a service completely hidden from the network and reaches a maximum value of 2 for a service that is completely affected by the entire address space. Then the assessment of the influence of external factors on the network is determined as

$$EF(s_i) = 1 + \frac{\log_2(IP(s_i) \cdot Ports(s_i))}{\log_2(2^{32} \cdot 2^{16})}, \quad (7)$$

assuming that the risk from the external network is evenly distributed. The high value of this rating indicates that the network should be divided to minimize network connectivity and the spread of attacks. Possible mitigation measures that can be taken at the network level include:

1) Network redesign (implementation of virtual local networks);

2) The rearrangement of the network so that machines with equivalent risk are in the same area;

3) An increase in the number of control points (Firewalls, IDS);

4) Increased security around active points on the network.

Also, valid IP addresses and ports must be carefully checked so that the IP address or port is not resolved unintentionally. As an optimization problem, we choose the following objective function

$$f(MY, PY, L_{s_i}, IF, RA, EF) \to \min, \quad (8)$$

whose physical meaning is to minimize the number of vulnerabilities at the user level, which will lead to an increase in the level of security of the PaaS model cloud system.

### *C. Experimental study of the proposed approach*

According to this approach, an experimental research on the basis of a simulated network consisting of several types of terminal devices and integrated communication services was carried out. The attack is simulated at the application level through the service port 80 that uses the TCP (Fig. 5). For each device, vulnerabilities with different weights were selected that characterize the criticality of the vulnerability itself.

If we consider the state in which the network is exposed to an attack propagating from one endpoint or several terminal devices, according to (5)-(6), knowing the weights of existing vulnerabilities, it is possible to assess the expected risk of data transfer routes that depends on the weight of the vulnerability on the node.

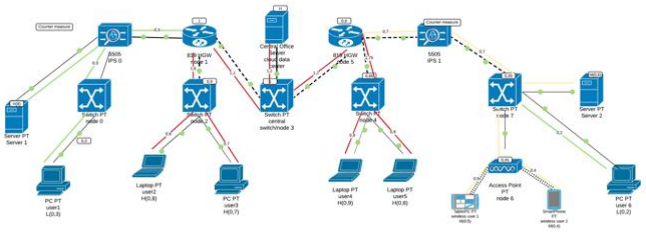


Figure 5. The experimental scheme of the network

As a result of the experiment in Fig. 5, the ways of attack propagation in the network from the user to the data center were obtained in this case. Influence and loss are directly dependent on the weight of the vulnerability (criticality) at the end user level. Therefore, from different users with different vulnerabilities in the event of the intruder intervention, the attack will spread by the shortest path to the data center. As a result, the network was divided into segments according to the criticality of future losses under the attack propagation, which was shown in Fig. 5 in different colors. Hence, the green color shows the paths of the attack propagation, which will cause minimal losses; yellow and red denote more critical attacks, which are implemented due to existing vulnerabilities that have a critical weight for the network.

Suppose that the risk from the external network is distributed evenly. The high value of this assessment indicates that the network must be divided to minimize the network connection and the attack propagation. However, at the network level, the following preventive measures can be taken:

1) Implementation of virtual local area networks;

2) Rearranging the network, so that devices with equivalent risk are located in the same area;

3) Increasing the number of control points (firewalls, IDS);

4) Increasing the security around "active" points in the network.

In addition, valid IP addresses and ports must be thoroughly checked to ensure that the IP address or ports will not be unintentionally resolved.

TABLE II. CLIENT-SIDE SERVER VULNERABILITY WEIGHTS

| Users | Weight of vulnerability |
|---|---|
| 1 | 0.3 |
| 2 | 0.8 |
| 3 | 0.7 |
| 4 | 0.9 |
| 5 | 0.8 |
| 6 | 0.2 |

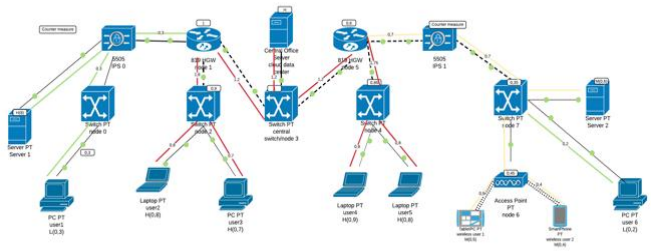


Figure 6. The experimental scheme of the network

As a result of the experiment in Fig. 6, the ways of attack propagation in the network from the user to the data center were obtained in this case. Influence and loss are directly dependent on the weight of the vulnerability (criticality) at the end user level. Therefore, from different users with different vulnerabilities in the event of the intruder intervention, the attack will spread by the shortest path to the data center. As a result, the network was divided into segments according to the criticality of future losses under the attack propagation, which was shown in Fig. 5 in different colors. Hence, the green color shows the paths of the attack propagation, which will cause minimal losses; yellow and red denote more critical attacks, which are implemented due to existing vulnerabilities that have a critical weight for the network.

Suppose that the risk from the external network is distributed evenly. The high value of this assessment indicates that the network must be divided to minimize the network connection and the attack propagation. However, at the network level, the following preventive measures can be taken:

- implementation of virtual local area networks;
- rearranging the network, so that devices with equivalent risk are located in the same area;
- increasing the number of control points (firewalls, IDS);
- increasing the security around "active" points in the network;
- improving user registration procedures.
- comprehensive study of network activity of service users;
- tracking the main black sheets for the appearance of a cloud provider network there;
- sing a robust and secure API;
- encryption and protection of transmitted data;
- implement a robust encryption key management system;
- selection and acquisition of only the most reliable media;
- ensuring timely data backup
- ban on transferring accounts
- using two factor authentication methods
- implement proactive monitoring of unauthorized access
- log Disclosure
- full or partial disclosure of system architecture data and installed software details
- using vulnerability monitoring systems.

## V. CONCLUSIONS

The effectiveness of the cloud security metric depends on security measurement methods and tools that allow network administrators to analyze and evaluate security. In this paper, we propose a proactive approach to quantifying the security of cloud systems, which allows us to assess the risks at the user level and at the network level, which significantly affect the security of the PaaS model cloud system under consideration. The novelty of the approach is that the risk assessment of the cloud system is carried out taking into account the separation of vulnerabilities into two groups: with existing countermeasures and without them, as well as in assessing the spread of attacks at the network level, taking into account free address space. Taking into account the fact that each cloud system contains vulnerabilities of different nature and for each system these vulnerabilities have a different level of criticality, it is not possible to use a single approach to assess the level of security for all cloud systems. However, knowing the criticality of a particular vulnerability, using this approach (1) - (7), you can evaluate possible risks and minimize them using expression (8) for a particular cloud system. This allowed a more detailed assessment of possible risks in the cloud system to minimize vulnerabilities, which, in turn, will minimize the damage that can be done to both the user and the cloud system provider. So, for example, if, as a result of risk calculations, the resulting estimates are lower than the permissible within the framework of the security policies used by a particular cloud system, then we need to review the security mechanisms. Based on this, the proposed solutions will be useful for making decisions and will be further integrated into a single metric to display the integrated security level of the cloud system.

## REFERENCES


[1] A. Mohammad Salim, E. Al-Shaer, M. Taibah, and K. Latifur, “Prediction capabilities of vulnerability discovery models,” Reliability and maintainability symposium, 2006, pp. 86-91.

[2] M. Abedin, S. Nessa, E. Al-Shaer, and L. Khan, “Vulnerability analysis for evaluating quality of protection of security policies,” 2nd ACM CCS workshop on quality of protection, Alexandria, 2006, pp. 28-39.

[3] F. Bock, “An algorithm to construct a minimum directed spanning tree in a directed network,” Developments in Operations Research. Gordon and Breach, 1991, pp. 29-44.

[4] “NIST Cloud Computing Program,” National Institute of Standards and Technology. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[5] C. Hewitt, “ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing,” IEEE Internet Computing, 2008, vol. 12, issue 5, pp. 96-99.

[6] “AlertLogic,” CloudSecurityReport:Research on the Evolving State of Cloud Security, 2014. URL: https://www.alertlogic.com/resources/cloud-security-report.pdf.

[7] E. Al-Shaer, and H. Hamed, “Discovery of policy anomalies in distributed firewalls,” IEEE INFOCOM’04, 2004, pp. 84-97.

[8] S. Kamara, S. Fahmy, E. Schultz, F. Kerschbaum, and M. Frantzen, “Analysis of vulnerabilities in internet firewalls,” Network Security, 2003, vol. 22(3), pp. 214–232.

[9] P. Ammann, D. Wijesekera, and S. Kaushik, “Scalable, graph-based network vulnerability analysis,” 9th ACM conference on computer and communications security, New York, USA, 2002, pp. 217–224.

[10] C. Feng, and S. Jin-Shu, "A flexible approach to measuring network security using attack graphs," International symposium on electronic commerce and security, 2008, pp. 278–304.

[11] Ch. Li, and Z. Deng, "Value of Cloud Computing by the View of Information Resources," Network Computing and Information Security (NCIS). International Conference on, 2011, vol. 1, pp. 108–112.

[12] M. Yevdokymenko, M. Manasse, D. Zalushniy, and B. Sleiman, "Analysis of Methods for Assessing the Reliability and Security of Infocommunication Network," 4th International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» PIC S&T`2017, 2017, pp. 199–202.

[13] M. Yevdokymenko, B. Sleiman, S. Harkusha, and O. Harkusha, "Method of fault tolerance evaluation in conditions of destabilizing factors influence in infocommunication network," in Proc. 2018 Fifth International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), 2018, pp. 571-574.

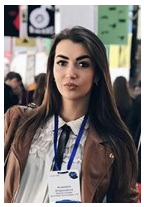
[14] M. Yevdokymenko, A. Shapovalova, O. Voloshchuk, and A. Carlsson, "Proactive Approach for Security of the Infocommunication Network Based on Vulnerability Assessment," in Proc. 2018 Fifth International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), 2018, pp. 609-612.

[15] M. Yevdokymenko, "An adaptive algorithm for detecting and preventing attacks in telecommunication networks," 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), 2016, pp. 175-177.

**M. Yevdokymenko** was born in 1984. In 2007 graduated with honors from Kharkiv National University of Radio Electronics for specialty Telecommunication Systems and Networks and received a Master's degree. She received the degree of candidate of technical sciences (PhD) in 2010. Thesis on the topic «Models and method of channel distribution in multichannel Mesh-networks of the standard 802.11», specialty 05.12.02 – Telecommunication systems and networks.

She took positions of Assistant of the Department of Telecommunication Systems of the Kharkiv National University of Radio Electronics since 2010. Since 2012 she held a position of Senior Lecturer of the Department of Telecommunication Systems, Kharkiv National University of Radio Electronics. In 2016 she held a position of associate Professor of the Department of Telecommunication Systems of the Kharkiv National University of Radio Electronics. Since 2017 she have been held position of doctoral candidate of the Department of Infocommunication Engineering (before telecommunication systems) of the Kharkiv National University of Radio Electronics. Scientific interests are traffic management in infocommunication networks, wireless networks, and security in infocommunication networks.

Ms. Yevdokymenko since 2019 is an IEEE member (IEEE Membership No.: 94598841).



**A. Shapovalova** was born in 1991. In 2014 she finished Kharkiv National University of Radio Electronics for specialty "Administrative management in the field of information security" and received a Master's degree. In a period from 2014 to 2017 she was a postgraduate student in Telecommunication system department Kharkiv National University of Radio Electronics. Since 2017 she is an assistant of department of infocommunication engineering Kharkiv National University of Radio Electronics

Ms. Shapovalova took a scholarship Program of the City Mayor "Gifted Youth", winner of the All-Ukrainian Competition for Scientific Information on "Information Security".

**O. Nevzorova** was born in 1992. In 2015, she graduated from Kharkiv National University of Radio Electronics, specialty «Telecommunication Systems and Networks» and received a Master's degree. She received the degree of candidate of technical sciences (PhD) in 2018. Thesis on the topic «Models and methods of hierarchical-coordinating routing in software-defined telecommunication network», specialty 05.12.02 – Telecommunication systems and networks. Since 2018 she works as an assistant of the Department of infocommunication engeeniring, Kharkiv National University of Radio Electronics.

Ms. Nevzorova since 2019 is an IEEE member (IEEE Membership No.: 95459565).

How to Cite this Article:

Yevdokymenko, M. A., Shapovalova, A. S. & Nevzorova, O. (2019) Proactive Approach for Security of the PAAS Model of Cloud System Based on Vulnerability Assessment. International Journal of Science and Engineering Investigations (IJSEI), 8(91), 167-173. http://www.ijsei.com/papers/ijsei-89119-22.pdf