

## E-university cloud information security issues

Firudin Aghaev<sup>1</sup>, Gyulara Mamedova<sup>2</sup>, Esmira Aleskerova<sup>3</sup>  
AMEA, Institute of Information Technologies, Baku, Azerbaijan  
agayevinfo@gmail.com, gyula.ikt@gmail.com, aleskerova-66@mail.ru

**Abstract:** This article identifies various security problems of electronic education in the provision of cloud services and proposes solutions to ensure security measures. Various types of attacks on e-learning platforms are also discussed. Various models of the usage of cloud technologies in electronic education, threats and security requirements when using these models are investigated.

**Keywords:** ELECTRONIC UNIVERSITY, CLOUD SERVICE DELIVERY MODELS, IDENTIFICATION AND AUTHENTICATION CONTROL, CLOUD SERVER PROTECTION, MITM ATTACKS, DDOS ATTACKS, INSIDER ATTACKS.

### 1. Introduction

Cloud-based e-learning is one of the fastest growing information technologies that offers powerful cloud-based e-learning products [1-2]. Cloud technologies have numerous advantages over existing traditional e-learning systems, but at the same time, security is a serious problem in cloud e-learning. To prevent the loss of valuable user data due to security vulnerabilities, appropriate security measures must be followed. Cloud-based e-learning products must meet customer security needs and address various security threats. In this paper, we consider key security issues when using cloud computing in e-learning systems.

### 2. E-learning cloud architecture

The cloud architecture of e-learning is mainly divided into five levels [3] called: the level of hardware resources, the level of software resources, the level of resource management, the server level and the application level. The cloud architecture of e-learning is illustrated in Fig. 1.

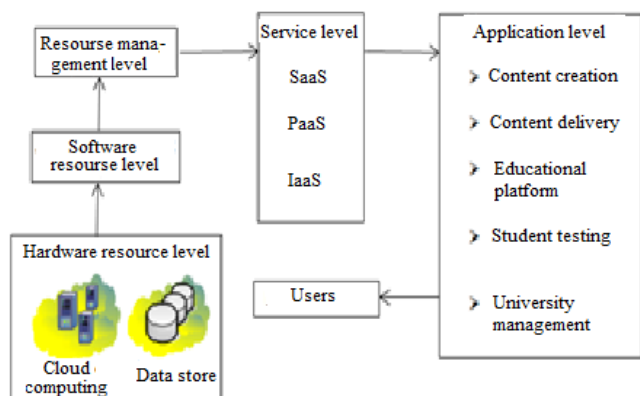


Fig. 1. Cloud architecture of e-learning.

The level of hardware resources is the lowest level of cloud infrastructure, which provides the computing power of electronic education. To ensure the smooth operation of cloud services for e-learning systems, physical memory is dynamically expanding, and is scaled at any time to add additional memory.

The software resource level includes an operating system and application software for developers and users of the cloud infrastructure.

The level of resource management plays an important role in the weak relationship of software and hardware resources. Using the idea of virtualization, it provides uninterrupted distribution of software on demand for various hardware resources of the cloud infrastructure.

The service level is divided into three levels: IAAS (Infrastructure as a Service), PAAS (Platform as a Service) and SAAS (Software as a Service). These service levels help cloud clients use various types of cloud services, such as software, hardware, and infrastructure services.

The level of applications differs from all other levels in the cloud-based e-learning architecture, as it forms the basis of components for e-learning and serves to create training content, content delivery, educational platform, assessment of learning and education management.

### 3. Problems of ensuring services of cloud calculations for electronic education

As was shown above, there are three models of cloud service delivery: 1. Software as a service (SaaS), 2. Platform as a service (PaaS), 3. Infrastructure as a service (IaaS). This article addresses security issues in each of these groups.

Software as a Service (SaaS) - allows multiple users to work together with ready-made software. Therefore, in SaaS, the user is completely dependent on the software vendor. To ensure proper security measures, the software vendor must ensure the security of the training data so that it is not possible for several users to see each other's data. The educational institution must be sure that the cloud service provider will only process data in accordance with its instructions, that it will take appropriate measures to exclude unauthorized access to the data, its modification or destruction.

Platform as a Service (PaaS) provides a computing platform and system software as a service. PaaS provides services for software developers. These include platforms such as Google App Engine, Salesforce, Windows Azure and others, which allow you to create programs and corporate sites in Java and Python. PaaS providers provide services for application development, deployment, team collaboration, web services integration and testing [4].

The main security threats to the PaaS layer are data location and privileged access. In the United States and many EU countries, universal safety standards and data privacy laws have been set for data placement problems. For example, the General Data Protection Regulation (GDPR) of April 27, 2016, valid in all EU countries, they never allow sensitive data to move from the country [5-6]. For violation of the rules for processing personal data, fines reach millions of euros.

Based on the location of the data, the PaaS model provides reliability for its customers. To ensure reliable data storage at the PaaS level, the user must choose a reliable encryption method for accessing data, maintain high standard data confidentiality, require legally executed contractual obligations of security mechanisms from the cloud provider. The cloud service provider must have technical solutions to prevent unauthorized access for users and support the principle of separation of duties for privileged users in order to prevent and detect malicious insider activity.

When storing encrypted data in a cloud storage, decryption keys must be stored securely in other disintegrated systems [7-8]. If the cloud user system allows the cloud service provider to process unencrypted data, the cloud service provider must ensure that the data is protected from unauthorized access, both inside and outside.

Infrastructure as a Service (IaaS) allows you to use many resources, such as servers, storage, networks, and other computing resources; it is hosting for a virtual machine. In the event that IaaS provides complete control and management of resources, users can

safely run any software on dedicated resources. In this case, an agreement is reached between the user and the cloud provider on the SLA (Service Level Agreement), which describes the services provided, the rights and obligations of the parties. This agreement contains a detailed description of the services, methods and controls provided to ensure the security of information.

The main types of threats in electronic education when providing IaaS services are DDoS attacks (Distributed Denial of Service Attack), MITM attack (Man In The Middle), DNS attacks, etc. The purpose of a DDoS attack is to make a cloud service unavailable for an auto-customized user. In this case, the cybercriminals use SYN flood (TCP connection requests), in which the entire server channel is simply clogged with connection requests. SYN flood is one of the types of denial of service network attacks, which consists in sending a large number of SYN requests, overflowing the connection queue on the cloud server.

Another common threat while providing IaaS services is the MITM attack, when an attacker introduces himself between two legitimate users of the network. An attacker establishes a connection between two users and tries to take possession of the information sent by them to each other [9].

Recently, in a cloud environment using the IaaS service, hackers have used this kind of

instantly change the parameters of the transaction, as well as the pages of the user's request, is completely transparent to the victim.

#### 4. Safety measures of cloud computing services for electronic education

While providing cloud services for an electronic university, to ensure the security of information, special attention needs to be paid to protecting hardware and virtual data processing devices, as well as communication channels. It is necessary to provide the following safety criteria [10-11]:

- Control of identification and authentication of subjects and access objects;
- Protection of computer storage media;
- Ensuring the necessary level of cryptographic and anti-virus protection of stored and transmitted information;
- Protection of the cloud server, communications and data transmission;
- Adoption of firewall measures.

In order to protect data from confidential information leakage, it is necessary to use strong encryption methods for network traffic to control data flow in the network: Secure Socket Layer (SSL) and Transport Layer Security (TLS). These security levels will help protect against traditional network problems such as MITM attacks, IP spoofing, port scans, sniffing packages, etc.

Attacks today have become complex and multi-level, evil-wills choose specific targets and take a long time to prepare for an attack in order to hit precisely the most vulnerable elements. The evolution of Internet threats has naturally influenced the development of a means of countering them. Today, the most effective tools for protecting cloud resources from external attacks from the network are Cloud Access Security Broker (CASB) solutions aimed at satisfying new security requirements. CASB is a unified tool for monitoring all cloud applications, resources and services, controls the interaction between cloud applications (access, traffic, downloading and data storage), the server and external users, allows you to identify potential threats and is focused on a high level of protection cloud environment [12-13]. CASB prevents unauthorized actions of users, detects abnormal activity, including those associated with the actions of various malicious programs. According to data published by Gartner in 2019, the leaders in the

cloud security market are: Skyhigh Networks, Netskope, Symantec [14-15].

And the recently appeared CloudSOC Security for Cloud Apps software package [16] monitors in real-time transactions with authorized (permitted) and unauthorized cloud applications; implements a visualization of user activity maps for quick analysis of their actions; protects against threats based on extensive analytics of user behavior. It provides rich visibility, data movement control and sophisticated analytics to identify and combat cyber threats in all of your cloud services.

The use of CASB tools in electronic education will make it possible, by analyzing the logs of "registration" and "geolocation", data on the time of performing certain actions in the "cloud", to track user actions, identify threats in real time, and identify unsafe applications. Machine learning tools are built into these packages, which provide the ability to track user behavioral actions and their deviation from the norm. By analyzing risk indicators, such as: insecure IP addresses, registration failures, activity level, inactive accounts, "impossible travel" scenarios and their location, timely detection of intruders on the network.

#### 5. Conclusion

The problem of data accessibility in electronic education is the main obstacle to ensuring the security of cloud data. A literary study clearly shows the risks in e-learning based on cloud computing, as well as its service delivery models and effective solutions for each attack. The listed security issues are important for management and the new methodology for developing secure e-learning based on cloud computing in the future.

The main goal of the work is to elucidate the key security problems that arise when implementing cloud computing for e-learning systems. The development of e-learning systems should be carried out using safety methods and internationally recognized standards. The system must implement security services, such as authentication, encryption, access control, user management and their permissions.

#### 6. References

- [1] N. Antonopoulos, L. Gillam. Cloud Computing: Principles, Systems and Applications. London: Springer-Verlag, 2010. 379 p
- [2] H Skleyter. Oblachniye vichisleniya v obrazovanii. Analiticheskaya zapiska/perevod s angliyskogo. Institut YUNESKO po informazionnim texnologiyam v obrazovanii [Elektronniy resurs] // IITO YUNESKO: 2010. URL: <http://iite.unesco.org/pics/publications/ru/files/3214674.pdf>.
- [3] K.Fogarti. Oblachniye vichisleniya: opredeleniya i resheniya. [Elektronniy resurs] // Izdatelstvo Otkritiye sistemi. <http://www.osp.ru/>: URL: <http://www.osp.ru/cio/2011/03/13007508>.
- [4] V.F. Shagin. Informaionnaya bezopasnost kompyuternix sistem I setey / V.F. Shagin. – M.: IZD «FORUS»: Ivfra-M, 2008. – 416 s.
- [5] [https://ec.europa.eu/info/law/law-topic/data-protection\\_en](https://ec.europa.eu/info/law/law-topic/data-protection_en)
- [6] A. Pazyuk, M. Sokolova. Zashita personalnix dannix: mejdunarodniye prinzipi i standarti. <https://www.researchgate.net/publication/281459857>
- [7] A.V. Erigin. Analiz effektivnosti sistem predotvrasheniya utechek konfidencialnoy informazii iz lokalnix setey. Vestnik SibADI, vipusk 2 (20), 2011, s. 40-47.
- [8] M.Jensen, J.Schwenk, N.Gruschka, & L.Iacono, Year. On technical security issues in cloud computing. In, 2009. IEEE, pp.109-116.
- [9] Callegati, Franco; Cerroni, Walter; Ramilli, Marco. IEEE Xplore - Man-in-the-Middle Attack to the HTTPS Protocol (англ.) // [ieeexplore.ieee.org](http://ieeexplore.ieee.org) : journal. — 2009. — P. 78—81.
- [10] E. B. Fernandez, Nobukazu Yoshioka, and Hironori Washizaki, "Patterns for cloud firewalls", Procs. of AsianPLoP (AsianPattern Languages of Programs) 2014, Tokyo, Japan, March 2014
- [11] E.A .Isayev., D.V. Dumskiy., V.A. Samodurov., V.V.Kornilov. Obespecheniye informazionnoy bezopasnosti oblachnix sistem Matematicheskaya biologiya I bioinformatika , 2015. T. 10. № 2. s. 567–579.

- [12] Hassan Reza, Madhuri Sonawane, "Enhancing Mobile Cloud Computing Security Using Steganography", Journal of Information Security, July 2016, Page no. 245-259.
- [13] [https://www.anti-malware.ru/analytics/Market\\_Analysis/cloud-access-security-broker](https://www.anti-malware.ru/analytics/Market_Analysis/cloud-access-security-broker)
- [14] <https://www.gartner.com/reviews/market/cloud-access-security-brokers/co-mpare/symantec-blue-coat-vs-skyhigh-networks>
- [15] C. Lawson, S.Riley Magic Quadrant for Cloud Access Security Brokers. Gartner. 29 October 2018.  
<https://www.bsigroup.com/globalassets/local-files/enie/csir/resources/whitepaper/1810-magic-quadrant-for-casb.pdf>
- [16] <https://www.symantec.com/content/dam/symantec/docs/dashboards/cloud-soc-gateway-en.pdf>