12. About education: the law of Ukraine from May 23, 1991 № 1060-XII // Facts of Verkhovna Rada Ukraine. - 1991. - № 34. - Art. 451. [in Ukrainian]
13. Shpagina A. Specificity of distance learning in higher educational institutions of Ukraine / O. Shpagina // Teaching Process: Theory and Practice. - 2013. - Vol. 4 - P. 209 - 213. [in Ukrainian]

Поступила в редколлегию 11.06.2014.

UDC 37.091.313:004.5

GRYBYUK O., PhD, senior researcher

National Pedagogical Dragomanov University
Institute of Information Technologies and Learning Tools
National Academy of Pedagogical Sciences of Ukraine

THE DEPLOYMENT OF CLOUD ENVIRONMENTS OF EDUCATIONAL INSTITUTIONS: SUPPORTING NETWORK SECURITY

Introduction. The main difference between traditional data centers and cloud environment is in the physical location of educational materials on servers that don’t belong to the user (e.g., for schools), but to the outside organizations. It is clear that the use of outsourcing and MCP provider’s services will reduce some of the problems that appear between the physical infrastructure of information-communication technologies and cloud environment [1]. The user develops emotional problems at using cloud services which consist in the failure of visual perception of server, where the user data are kept.

Setting of the task. The problem of implementing computing infrastructure Cloud Computing is explored by B. McConnell, group Beyond Contact, R.L. Krutz, R.D. Vienes, J. Ransome, J. Rittinghouse, J. Rhoton et al. They all stress an important principle – the question of security in Cloud-systems. Hypothetically, it is recommended to use additional levels of identification in security systems, encryption, secure data transmission, restricting access to data of different users and other mechanisms. It is important to understand that security requirements do not change regardless of the calculations in the "cloud," or out of "the cloud."

Obviously, from a formal point of view, there is a set of specifications to ensure safety. During the deployment of cloud environment of the institution particular attention should be paid to applied security, because users perform their tasks using common equipment. Hence, the work in this mode should not be interrupted by failures, otherwise all this will contribute to violations of ideology behind cloud computing. This is how the problem of security is solved in Cloud Computing.

An important problem is to limit access to educational materials (data), e.g. the inability of chosen cloud provider to protect the components of its infrastructure. The necessary measures are data encryption and remote backups (including backup encryption and network communications on a different cloud unit, encryption of network traffic with web-traffic). It is recommended to attach an additional cloud provider to perform the automatic backup procedures, providing a guaranteed recovery of all data and their history, even in case of physical destruction of the main cloud provider. In addition, it’s necessary to set up the level of control for using own data in cloud environment and data centers. To form sets of data backup it’s recommended to use cryptographically secure algorithms, like Pretty Good Privacy, which enables you to save messages (data) even in an unprotected network environment. You should encrypt on individual backup server, which facilitate the creation of a single system with the saving of all accounts (all data) for access to cloud storage.

Results of research. When choosing the cloud provider it's reasonable to consider all options of its physical protection of data and ways of network security realization, including individual hosts. It is impossible to determine the exact location of the cloud provider, i.e. the physical location of virtual storage of relevant data. In addition, the means of cloud provider are provided by declared standards of security and procedures of data saving.

The data of cloud service's user can be found inside of particular guest operating system that runs on a virtual machine. Necessary mechanisms of monitoring users' access to data are available with public access options. The network traffic, which is necessary to exchange virtual packs is always invisible to other virtual hosts.

The ability to create ephemeral storage devices using virtual server is important during deploying cloud environment, although, for example, lack of ephemeral encryption devices in the environment of ES2 is threatening in connection with the erasure of ephemeral devices by recording zeros at the shutdown of the system. Caution while encrypting file system will help prevent conflicts arising from the requirements for efficiency of particular applications and data protection.

The secure approach of data use in a cloud environment is to mount block store devices and ephemeral devices using Encrypted File System. The control of cloud server launch aided by encrypted file systems in cloud environments becomes easier and requires higher security. It's more rational to store passwords for system protection in unencrypted root file system rather than in the cloud environment. Such saving of passwords doesn't present any problems, because the purpose of encrypting file system is protection from physical access to disc image. The process of launching a virtual server using passwords can be presented on Fig.1.

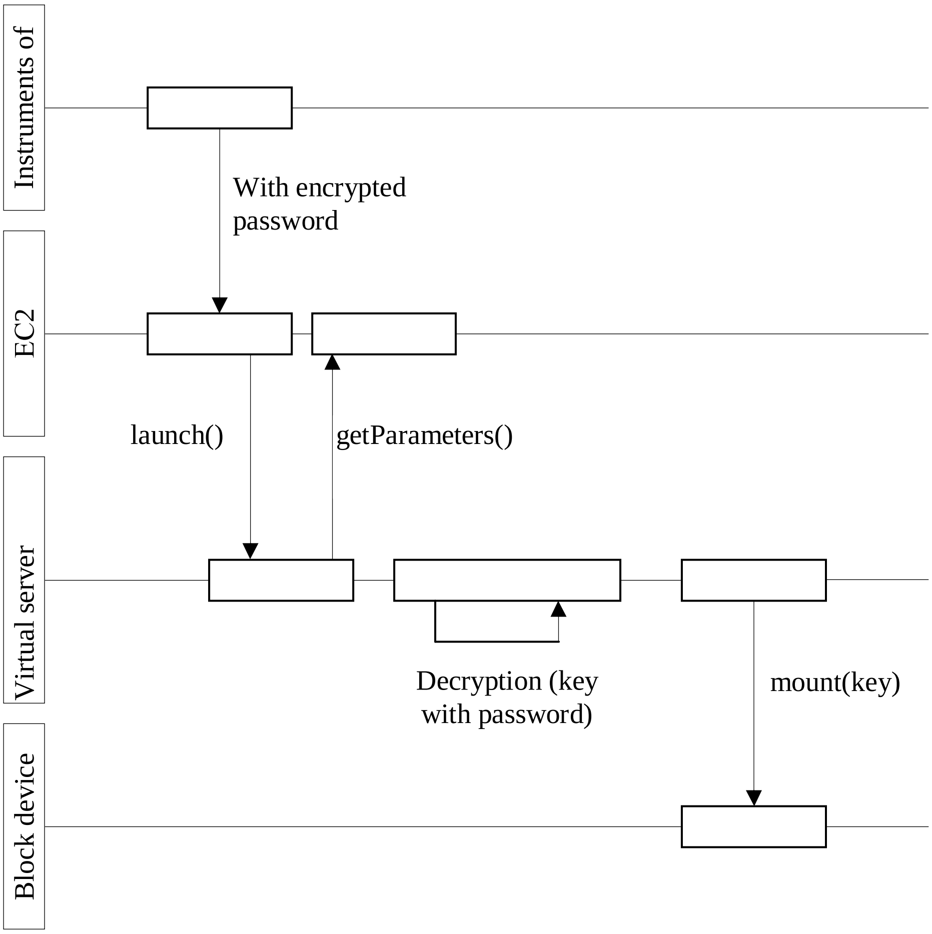

Figure1 – The launch of a virtual server

Most problems with the inconformity of regulations and existing standards, related to the fact, that legal documents are issued before the widespread use of deployed applications in the cloud infrastructure. Certainly, the specification of system deployment in cloud environments can be reduced by the mixed architecture that consists of physical elements and some virtual items. Cloud infrastructure that specializes on hybrid solutions is the best option.

The private information is not saved in the cloud infrastructure of mixed environment, because their processing is performed in physical data processing servers controlled by the user. The protection of the perimeter of one or more network segments is performed by a firewall (Fig.2). A firewall protects the outer perimeter of network traffic letting through only http, https, ftp. There exist intermediate systems between a protected network segment and the outer perimeter – load balancers which is directing traffic to a special district where the application servers are situated. They send requests to the database through another firewall to secure internal network with internal databases of confidential data. The proposed structure (Figure 2) is used to obtain access to data with increasing levels of secrecy, and at that a few levels (perimeters) of network security are organized using firewalls. Compromise of any internal server within a particular segment automatically provides full access to the other servers in the same segment, which stands as a flaw of such infrastructure.

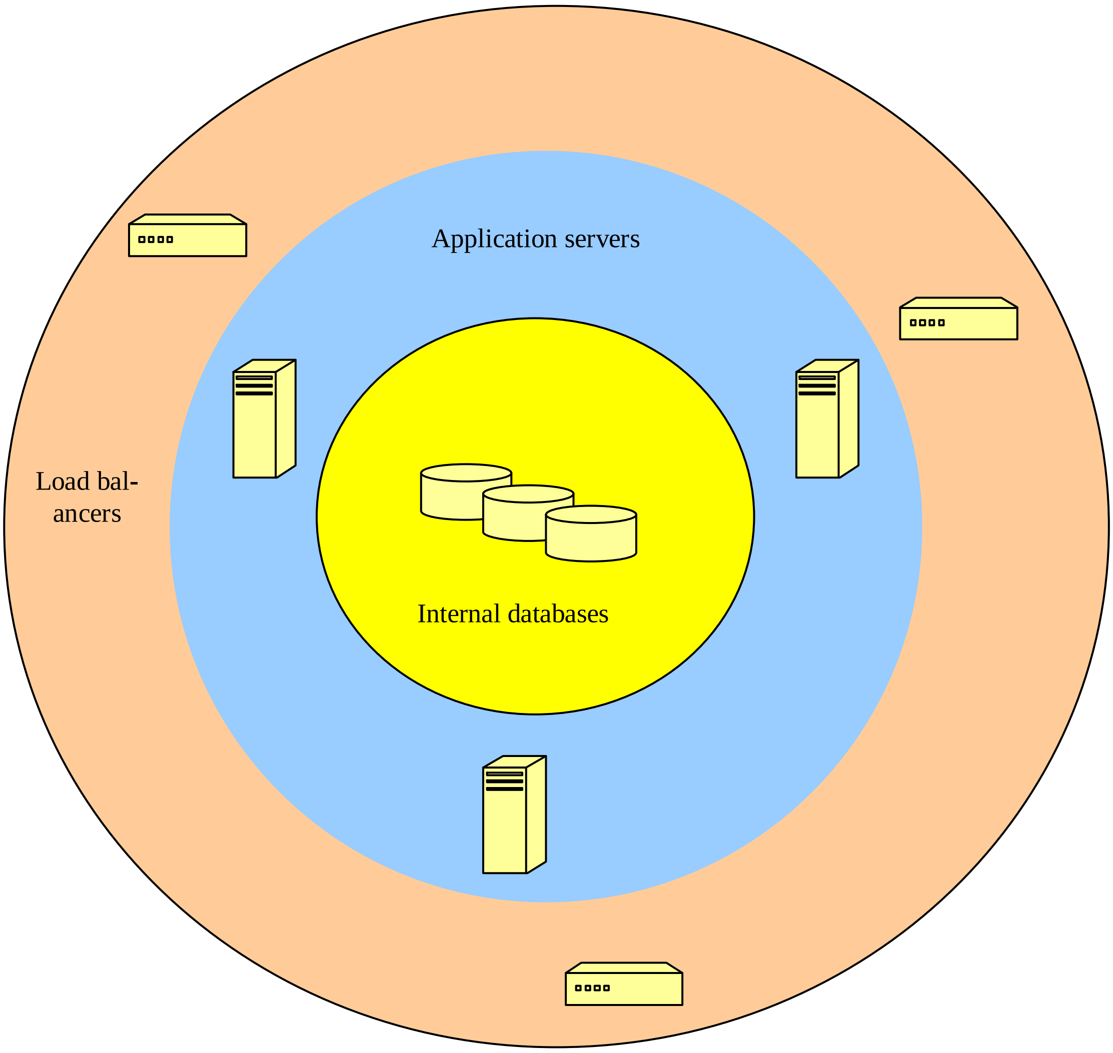

Figure 2 – The protection of networks' perimeter by firewall

There are no perimeter network segments in cloud environments. All virtual servers are at the same level in the network, and traffic is controlled by means of security groups

(Fig.3). An individual server can belong to different groups and security rules for an individual server can combine the rules for all groups to which this server belongs.

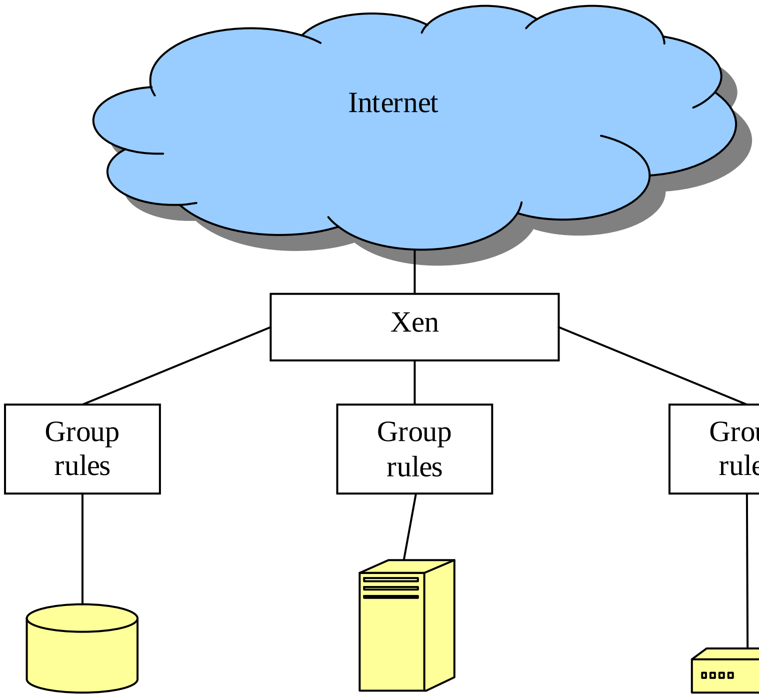

Figure 3 – Vizualization of the concept of firewall rules in cloud environment

The efficiency of the network security in the cloud environment depends on many factors. For example, it's advisable to run only one network application on each virtual server and services intended for administration,. Focusing on a single server multiple services will lead to a virus attack vectors that determine access to data on the server, or using the server as a buffer zone for receiving access rights to the network.

It is inappropriate to grant users access to data with high level of security, and others will have to overcome three different vectors of virus attacks to obtain unauthorized data. Obviously, protecting each server requires a particular port to support a particular service, amplification while some particular service may be running on it. It is advisable to restrict access to services for external users, except for personalized users. Even with restricted use of load balancer they recommend to use a reverse proxy server. Reverse proxy server relays user's requests from outside environment to one or more servers, which are logically located in the internal network. Usually the reverse proxies are located before the web-servers and are used as applied firewalls for load balancing in the network between multiple web-servers and the improvement of their security.

To automate the elimination of security problems in the network it's recommended to thoughtfully apply dynamization of the cloud environment. Network systems of intrusion detection are designed to prevent attacks before they start and to reflect attacks that began and continue. Intrusion in the network is detected by routing all traffic through the system that is used for its analysis, or respectively by passive monitoring of the traffic from one computer of the corresponding LAN. In the cloud environment, additional system of virus attack detection is effective due to opportunities of rapid detection and neutralization of harmful content of network packets.

An original approach to run and use a remote server for NIDS with a load balancer is to install it on the server before the network (Figure 4), owing to this all incoming traffic is monitored.

Having found a way to compromise load balancer a viral attacker not only invades occupies load balancer, but also gets the opportunity to suspend the process of intrusion detection. An alternative approach is to implement the intrusion detection system on a server in the position behind the load balancer, which acts as an intermediary between the load balancer and other system components. In traditional data centers or cloud infrastructures, intrusion detection systems are installed in accordance with clearly thought-out algorithm. A minimum required set of software is established on each host in the cloud environment.

Conclusions. In the cloud environment, the deploying of individual applications supported by the security system presupposes security updates to all AMI, testing of results, restarting all virtual servers, minimizing various operations in the cloud, making it practically impossible for a human error to occur. It can be possible to experiment with different configurations and restructuring of images of the computer in the cloud environment. Having selected the configuration for the particular service profile, you can pre strengthen protection of the system before the deployment of image in the cloud environment. But it's recommended to delete user accounts and passwords, which are kept in the configuration file beforehand.

Convenience and consistency of such computer infrastructure as Cloud Computing will over time increase the level of user confidence, particularly in the educational process and administering of educational institutions.

It's advisable to determine the requirements for choosing the antivirus software before the deploying of the cloud. Obviously, the number of viruses increases according to the geometric progression every day, so it is logical that the developers of anti-virus software can't ensure the protection against each of them, so their product provides protection only against existing viruses. Network systems of intrusion detection monitor network traffic, detecting anomalous activity. Accordingly, network systems of intrusion detection operate similarly to anti-virus system at the host (HIDS) and additionally research the system, if there are any signs of the discrediting, report about all cases of changing of the system services and operating system files. It is not recommended to deploy servers in the cloud environment without network systems of intrusion detection at the host (HIDS). In the cloud infrastructure it's advisable to choose a centralized configuration to develop a high level of security profile with a high degree of protection of individual services according to the principle "one server - one service". Segmentation of data according to different levels of confidentiality is the primary way of minimizing the impact of any virus attack on the performance of the system as a whole. It is recommended to provide access to virtual servers by the dynamic delivery of public keys (passwords) to the target server, pasing the keys through the administrative interface, rather than through the user account, that is integrated in the image of the computer. If you change the user it's recommended to create another image of the computer with the necessary changes for the new user.

The fundamental approach is to use already existing control tools to manage cloud infrastructure or to develop necessary tools, so that credentials of users are kept outside the cloud infrastructure and it is possible to dynamically add (delete) user accounts on cloud servers at runtime. This approach requires to create and run the administrative service on each host. During the compromise in the cloud environment it is appropriate to copy the root file system onto one of the volumes, and copy volumes in case of halting of the server and its replacement.

REFERENCES

1. Hryb'yuk O. Prospects for the introduction of cloud technologies in education / O. Hryb'yuk .// Theory and Methods e-Learning :. Collected Works. - Issue IV. - Copenhagen: KMI Publishing Department, 2013. - P. 45 - 58.

Поступила в редколлегию 06.06.2014.