УДК 811.111

DEVELOPMENT OF CLOUD SYSTEMS SAFETY BY MEANS OF CLOUD COMPUTING. APPLICATION IN MODERN ANTI-VIRUS PROGRAMS

Машукова А.В., Курбатова Е.А.
научный руководитель – ст.преподаватель Курбатова Е.А.
Сибирский федеральный университет

Cloud computing - technology of distributed data processing where some scalable information resources and capacities are provided as service for multiple external clients by means of the Internet technology.

The concept of cloud computing includes a combination of the following notions:

IaaS (Infrastructure as a Service) – computer infrastructure presented, as a rule, in the form of virtualization. It is a service within the concept of cloud data processing.

PaaS (Platform as a Service) – an integrated platform for development, deployment, testing and support of web-applications. It is presented in the form of service on basis of the "cloud computing" concept.

SaaS (Software as a service) – is a business model of licensed software use which implies software development and maintenance by a vendor. Customers have an opportunity of pay use, as a rule, by means of the Internet.

DaaS (Desktop as a Service) – one more business model of licensed software use which is a slightly advanced SaaS model, and generally assumes the use of several services necessary for adequate operation simultaneously. It was first introduced at the beginning of the 2000th.

Safety of cloud computing

At present cloud computing is more and more considered as one of the most perspective methods of IT infrastructure optimization. Cloud Computing technology has a lot of advantages, but the issue of data protection reliability, when using the concept of cloud computing, is becoming the main constraint. To ensure information security it is necessary to master new protection methods and technology, methods of incidents registration, to develop new standards of information security. There are also difficulties of legal nature. In particular, it becomes difficult to differentiate, who is responsible and what they are responsible for, as cloud computing essentially differs from customary model in infrastructure way and can dynamically change. There is a psychological aspect of this problem. IT outsourcing has not got such development in Russia as it has in the West, and many company executives skeptically welcome the idea of handing over the IT infrastructure to the third-party expert for maintenance. As practice shows, application of cloud computing is capable to improve data security level. One of the reasons is constant concern of the companies providing access to cloud computing services for a high security level. Knowing about their clients' apprehension they have to invest heavily in creation and support of reliable protection system. Some IT service providers that work in the sphere of Cloud Computing emphasize the guarantee of a high security level in their marketing campaign.

Information ranks high in the life of our society therefore information security is an integral part of its use. Information security is often considered for the purposes of information media security. Information media security requires difficult and diverse software and hardware. With existence of a great number of architectural solutions for media, there is the same number of the ways of their protection.

Existing security methods

There are two classes of security implementation:

– Absolute prohibition of operation or information modification beyond an OS at the hardware level;
– Timely detection and neutralization of threats during OS operating time (RedPill, timing attack, performance attack).

Security at the hardware layer is expensive and difficult to implement, and there are no reliable methods of detection and neutralization of such threats at present. The method of virtualization form detection by a thin hypervisor «RedPill» was offered by Joanna Rutkowska. It is based on a count of a number of interrupt vector tables in a computer RAM. This method can work appropriately only in one core processor systems. Timing attacks and performance attacks are based on distortion of time and speed computer characteristics in case of a hypervisor implementation.

Cloud computing and future of anti-virus systems

With the development of telecommunication systems many anti-virus companies started to pay attention to cloud computing. The concept of cloud computing consists in providing remote dynamic access to services, applications (including OS and different infrastructure) and computational resources of different capacity to end users.

Cloud computing are divided into two types: platform clouds and clouds of services;

Platform clouds provide access to some platform. It can be an operating system, a system for scientific computations, etc. Clouds of services provide only services. Platform clouds are rather special-purpose and usually serve as a big calculator and a pool of operation statistics of desk anti-virus systems, or as a database of the latest signatures. Clouds of services are used to enable users to load some suspicious files in a cloud and check them with the anti-virus without consuming computer resources of the user.

Antivirus cloud operation organization

Several ways of anti-virus clouds operation can be distinguished: operation with metadata and hash functions of executable files, their analysis in the cloud performed by an expert system; transmission of actual virus signatures in frequent and small portions to a user computer; SONAR technology (giving marks of application danger by the operations executed, and analysis in the cloud). Anti-virus cloud computing adopts all the problems inherent in clouds as well as the problems of antivirus software.

The advantages of cloud anti-viruses are:

– Security of decision-making environment;
– Increased performance;
– Decrease of response time to new threats; keeping a threat database up-to-date;
– Fast implementation of new means of fight against malicious software;
– Hidden logic of decision-making;
– Impossibility to check efficiency of new malicious software disguise without entry the information about it into a cloud threat database;
– Minimizing of misoperations.

There are disadvantages as well; many of them are caused by the use of cloud computing, therefore all the shortcomings of cloud computing inherent in cloud anti-virus systems.

– Problems of network connections loading at slow communication channels;
– Impossibility of effective anti-virus check on demand of a user without serious increase in number of the client requests to the cloud;
– Inoperativeness of anti-virus system when there is no connection with the cloud (a local computer, without connection to a network).

Apparently there are more advantages of cloud anti-virus systems than disadvantages. Modern accelerated development of telecommunication networks is certain to make the most

part of the problems in cloud computing use irrelevant. Created secure runtime environment is also a great advantage. It allows bringing the modern anti-virus means up to a new level in the fight against the modern threats.