Olha Kucheruk, graduate student,
Tetiana Vakaliuk, doctor of pedagogical science, professor,
professor in the department of software engineering
Zhytomyr Polytechnic State University

DATA PROTECTION IN CLOUD TECHNOLOGY

Problem formulation in general form. Nowadays, there is a rapid growth in usage of cloud technology. This article id devoted to the data protection in modern cloud technology.

«Cloud technologies – is a fundamentally new service that allows you to remotely use the means of processing and data storage».

User's data in cloud computing, are primarily saved in virtual stores of cloud infrastructure. In public models such as SaaS (Software as a service) and DaaS (Desktop as a service) users possess only stored data. All the hardware and software involved in storage and processing of information are owned by service providers. In all other models, such as IaaS (Infrastructure as a service) and PaaS user has an access to data processing and software, but has no access to hardware. Thus, according to the user's opinion of the cloud service user's data are the most valuable asset in the cloud environment, especially those containing sensitive information and demand a different approach, specifically the following: governmental, health care, finance data.

Advantages for using cloud computing provide users, that used to public sensitive information on their PC with more attractive prospects to the outsourcing their data in the cloud. Cloud services can also detect security attacks as well as other internet services. Compromising of cloud services availability, for the most part leads to the short-term effects and all the deteriorations can be restored. Compromising of confidentiality and privacy of user's data can lead to long-term effect and any losses can be challenging to restore.

Internal risks may be from hackers that use the same service, and in this case, risks mitigation totally depend on the cloud provider and gets out of data owner's control. From data owner's perspective, cloud technology is invisible and data owner can not be sure that their data are protected from security risks. Therefore, data owners are concerned about security and privacy of their data and wish to keep their data safe even from the service provider of cloud services. Besides, they prefer managing their data security policy on their own as if these data were saved on their PC.

Based on the described above, let's consider the list that underlines criteria that shall meet the provided security solution: 1. Every set of data is an autonomous container able to describe and protect itself on its own. Thereby, security requirements for every set of data and features are ensured inside it and do not depend on the objects within the set of data, except for some main data processes. 2.Data protection does not depend on the service provider or trustworthy third party. 3.Only data owner is responsible for creation and management of security requirements and characteristics for every set of data from the inception till the end of lifecycle of data set. 4.All operations connected to the access to the secured data are set by authorized users, supplied by the data security policy and run without privacy compromising or violation of user confidentiality.

Data oriented solution is made in order to meet the following requirements in the cloud technology: data is encrypted and available only for authenticated users; data is available for searching without the risk for their confidentiality; data meet the requirements of self-protection and necessary security settings; access control settings are hidden from cloud services providers and other users; server provider does not know the amount or identity of authenticated users and have access to the data; unauthorized subjects, including service suppliers cannot get access to the data; data contains all the necessary information to check its integrity and the accuracy of the authorized users; interaction between data owners and authorized users shall be minimal.

All the requirements mentioned above are defined by the set of modules, each of them realizes at least one of the demands above.

«Cloud services can be distinguished in three types: «software as a service», «platform as a service» and «infrastructure as a service»: *Software as a service (SaaS) is easy to understand: users access applications on the Web, for example, a word processor, a spreadsheet or email software. The services offered by Google (e.g., Google Docs, Gmail) are well known examples of SaaS. Data are also stored on the Cloud providers' IT systems. In such context, the CCS provider (e.g. Google) is technically responsible for the application services and for the data of the users (secure storage and secure access). *Platform as a service (PaaS) offers an operating system where users can install their own applications. The platform provides services such as application services and database services. The data are stored depending on the application, either on the provider's system or locally on the client's system. *Infrastructure as a service (IaaS) offers one «logical hardware» infrastructure.

Users have to install their own operating system, the applications they need and they have to decide which storage provider to use and they have to decide how to connect the different PaaS components they use. In general, the user cannot determine where the data is physically located because the Storage provider will store several copies of the data at possibly changing locations».