UDC 004.056.5 + 004.75

O.V. Spirintseva, A.S. Lozovsky

THE MODELS OF THE INFORMATION SECURITY IN THE CLOUD STORAGE

Annotation. The features of the data storage in the cloud are analyzed. One of the most important features is the lack of the need to think about the operation of the technological infrastructure of the "cloud". But the user's private information becomes available to third parties, the provider, the data is under threat during their transmission through the communication channels. There is the comparative characteristic of the basic information security models regarding to cloud storage in the paper. There are the advantages and disadvantages and corresponding schemes.

Keywords: information protection, cloud storage, authentication, encryption, personal data.

Introduction. The proliferation of networks with high capacities, relatively low cost of computers and storage devices, led to a wide introduction of virtualization and the creation of service-oriented architectures. One example of such architectures can be considered cloud storage services.

They provide their clients with access to memory cells that are on their servers and also guarantee the safety of data that is placed in these cells. Thus, the user can not worry about the security of the data, and also has the ability to retrieve this data from any Internet access point [1].

The aim of the work is the comparative analysis of the various models of the information security in cloud storage.

Main part. The way to protect the data in cloud storage is through user authentication. An authentication is an act of confirming the truth of the attribute of one piece of data claimed by the present entity. Unlike the identification that relates to the act of the application or in the same direction that it allegedly confirms the identity or the thing, authentication is the actual confirmation of this person [2].

Advantages of this method are:

- Only the authenticated user can receive the data.

 ISSN 1562-9945

- The data integrity is at a high level.

For any authentication, it is important that the parties have a common secret, through which the user can verify their identity. An example of a secret is the key-pair - login/password.

The main problems encountered during authentication are the ability to intercept authentication data and leak the database with user keys.

Prevent interception or theft of sensitive data by using additional tools such as:

1. Authentication using public key encryption.
2. Authentication based on the shared secret key using HMAC.

The first authentication method is used when both the client and the server have certificates [3].

The sequence of steps for this type of authentication is described below (Fig. 1).

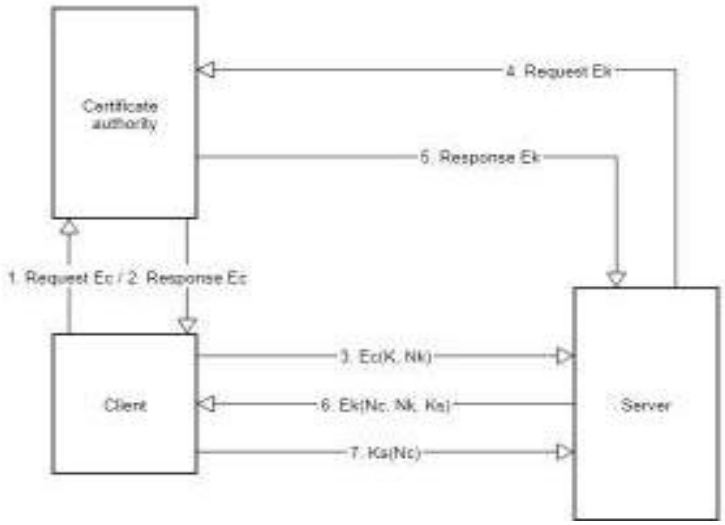

Figure 1 - Authentication using public key encryption

Nk, Nc - 128 bit number, chosen randomly by the client and the server separately; K, C - client and server identifiers (for example, IP address); Ks is the shared secret key; Ec, Ek - open keys of the server and the client respectively, which are transmitted in the form of certificates.

When designing an authentication system, unlike a standard protocol, it is assumed that clients will not have their own certificate, but will send their public key to the server, encrypting it with a previously public key of the server received with the certificate. This will avoid the need to obtain multiple certificates for each client, which would entail

the user's need to be distracted by its configuration, which contradicts the system's limitations (Fig. 2).

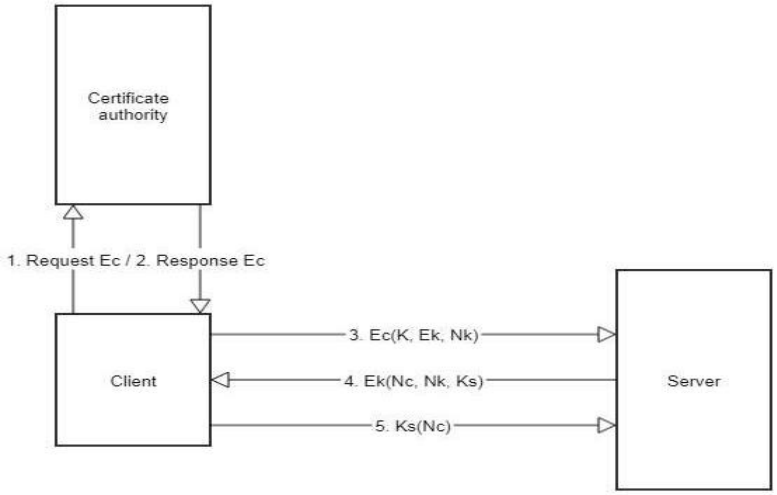

Figure 2 - Authentication using public key encryption without using separate certificates for each user

The second type of authentication implies that the client and the server have a secret key, which is known only to the two of them.

HMAC (short for hash-based message authentication code). That is, it is a mechanism that uses cryptographic hash functions in combination with a secret key.

The sequence of protocol authentication is as follows (Fig. 3):

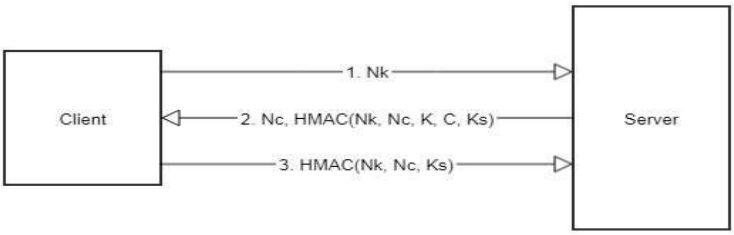

Figure 3 - Authentication based on the shared secret key using HMAC

Another way to securely store data is encryption. Encryption alone does not interfere with interference but does not allow a comprehensible interpretation of the contents of the potential interceptor [4].

The advantages of this method of protection include:

1. Confidentiality. Encryption is used to hide information from unauthorized users during transmission or while storing.

2. Integrity. Encryption is used to prevent changes in information during transmission or storage.

The disadvantages are:

1. The process of encryption and decryption is time consuming and resource intensive.

2. At the slightest damage to the data, the decoding becomes ambiguous.

When using this method of data protection, the encryption process must be performed either on the client before the data is transferred to the server, or when data is directly transferred to the storage.

For the first case, the data protection model is presented as follows (Fig. 4):

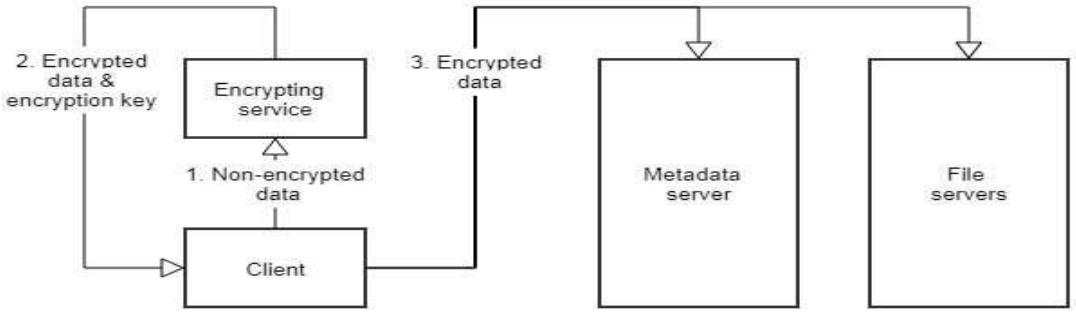

Figure 4 - Data encryption on the client before data transfer to the server

Thus, the server does not know anything about the information contained in the files, because in an encrypted form they do not have an easily understandable meaning and the provider cannot open them without a key.

In case of data encryption directly when transferring to cloud storage, the protection model is as follows (Fig. 5):

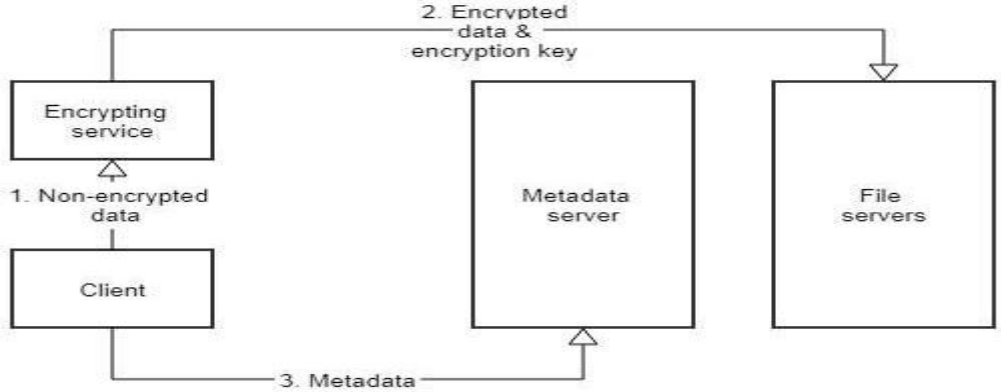

Figure 5 - Data encryption directly when transferred to cloud storage

Thus, the client does not need to spend the time-cost operation of data encryption and decryption and there is no need to search for special means for securely storing the key from the cyphers [5].

There are the risk of information security violation R dependences on information value of the cloud storage objects on the Fig. 6. It means that the inner treats of the information security are the most unsafe.

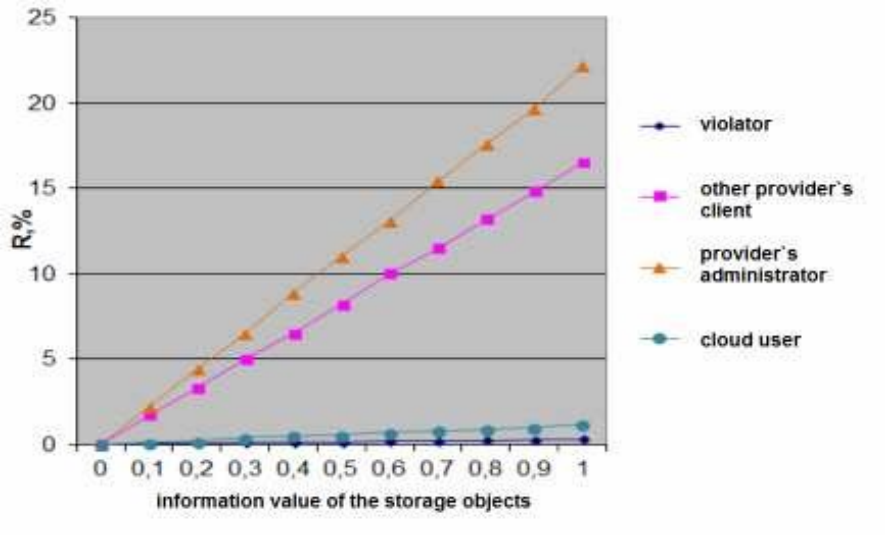

Figure 6 - The Risk level- The Information value diagram

Conclusion. Additional authentication tools are a more reliable means of protecting personal data since the more stringent identity check is performed. However, in the event of theft of a database with client certificates or the interception of a public key, the data can be easily obtained by the third party. On the other hand, additional encryption is a more costly method for resources, but even if a third-party person accesses data stored on a cloud storage server, understanding the information contained in the files will not be possible.

SOURCES

1. Захист даних в хмарних технологіях обчислень [Ел.ресурс] – Режим доступу: http://conf.vntu.edu.ua/allvntu/2013/inaeksu/txt/tytarchuk.pdf.

2. Authentication [Ел. ресурс] –
Режим доступу https://en.wikipedia.org/wiki/Authentication

3. https://habrahabr.ru/post/144282/

4. Encryption [Ел. ресурс] –
Режим доступу https://en.wikipedia.org/wiki/Encryption

5. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб.: Питер, 2014. – 944 с.