UDC 004.223.2

POSSIBLE OPTIONS FOR INFORMATION STORAGE, ANALYSIS AND SELECTION OF THE OPTIMAL STORAGE FOR FURTHER IMPLEMENTATION

JEKATERINA DENISOVA, YURY PASTUHOV
Polotsk State University, Belarus

The article discusses various options for storing information. The result of the analysis is choosing the best option for storing information. Design of a system for storage and transmission of information is discussed, as well as issues of these data protection. There is also provided research on the relevance of this system development.

In the modern world, users of personal computers, smartphones and other devices with access to the world wide Web have a large amount of information (photos, videos, music, various documents, etc.) that has to be stored somewhere. To store information, there are a large number of different resources. Consider the possible options for storing information:

– disk drives can either be housed internally within a computer or housed in a separate box that is external to the computer. They are found in PCs, servers, laptops and storage arrays, for example. They work by rotating very rapidly around a head or heads, which read and write data. They differ from solid state drives (SSDs), which have no moving parts and offer greater performance, but also cost more and generally offer less capacity. Today they are used in most desktop PCs, and have also found application as portable data storage. Usually, such a device works properly for 3-10 years and its service life depends on many external factors and the quality of production;

– an SSD drive is a type of nonvolatile storage media that stores persistent data on solid-state flash memory. Two key components make up an SSD: a flash controller and NAND flash memory chips. The architectural configuration of the SSD controller is optimized to deliver high reading and writing performance for both sequential and random data requests. SSDs are sometimes referred to as flash drives or solid-state disks. Such devices, on average, work properly for about five years. Many flash drives can break even much earlier, because they cannot tolerate a voltage surge or static discharge at the time of connection to the PC;

– an optical disc is an electronic data storage medium that can be written to and read from using a low-powered laser beam. This is, perhaps, one of the longest-time ways to save information, in some cases, such a disk will reliably store all recorded data for more than 100 years, but optical disks can occupy a large number of physical space, which is not very convenient for the user;

– cloud storage is a service model in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). The use of cloud media is very popular nowadays. It is a very convenient option to provide information to any person, being anywhere in the world, with any multimedia device and access to the Internet.

Based on the mentioned above options, one can conclude that in the age of modern technology and the availability of the Internet, users increasingly "trust" their data to cloud services, which is sufficient and convenient, because the service does not take any physical space, unlike other possible options for storing information.

The relevance of the development of a cloud storage: the basis of the developed system is the ability to store, store and process data, as well as the ability to share files with third-party people. When developing our own cloud storage, we have the opportunity to make encryption "for ourselves", that is, to choose the algorithms that we need and, if necessary, modify them. At this stage, a two-key mathematical model of the cryptosystem based on two types of encryption (AES+RSA) is implemented in such a way that we can change/add the encryption algorithm at any time. This makes our system flexible to develop and more secure against intentional information theft.

The principle of information security. Based on the fact that this system is designed to store sensitive data of users, it is necessary to develop a system of authentication and cryptographic protection of data.

For secure data transmission over the Internet there are the following technologies:

– Hypertext Transfer Protocol Secure (HTTPS) is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection. HTTPS enables encrypted communication and secure connection between a remote user and the primary web server. When using HTTPS, the traffic between the browser and the web server is encrypted. This prevents anyone who happens to have access to any of the many wires that your data will traverse as it crosses the Internet from looking at what you are sending to the server, or what the server is sending to you. This is why HTTPS is used for sending passwords and other login credentials. This is one reason, why websites dealing with banking and other matters that require privacy, use HTTPS. This is why you probably want to use HTTPS if you are reading your webmail from a public wi-fi connection.

– SRTP (Secure Real-Time Transport Protocol or Secure RTP) is an extension to RTP (Real-Time Transport Protocol) that incorporates enhanced security features. Like RTP, it is intended particularly for VoIP (Voice over IP) communications.

SRTP was conceived and developed by communication experts from Cisco and Ericsson and was formally published in March 2004 by the Internet Engineering Task Force (IETF) as Request for Comments (RFC) 3711. SRTP uses encryption and authentication to minimize the risk of denial of service (DoS) attacks. SRTP can achieve high throughput in diverse communications environments that include both wired and wireless devices. Provisions are included that allow future improvements and extensions.

– SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites for the protection of their online transactions with their customers.

– Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithms used worldwide. This algorithm has its own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult for hackers to get the real data when it is encrypted by AES algorithm. For the time being, there is no case of craking this algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit, and each of these ciphers has a 128 bit block size. This paper will provide an overview of AES algorithm and explain several of its crucial features in details, and as well as demonstrate some previous researches that have been done on it in comparison to other algorithms, such as DES, 3DES, Blowfish etc.

– The RSA algorithm is the basis of a cryptosystem - a suite of cryptographic algorithms that are used for specific security services or purposes -- which enables public key encryption and is widely used to secure sensitive data, particularly when it is sent over an insecure network such as the Internet. RSA derives its security from the difficulty of factoring large integers that are the product of two large prime numbers. Multiplying these two numbers is easy, but determining the original prime numbers from the total – or factoring – is considered infeasible due to the time it would take even using modern supercomputers.

After analyzing the above, we can conclude that cloud storage is one of the best options for storing information at the moment. Developing cloud storage, it is necessary to learn the methods of encryption and their relevance, and choose the most versatile protection methods.

REFERENCES

1. WebRTC API [Электронный ресурс] – Режим доступа: https://developer.mozilla.org/ru/docs/Web/API/WebRTC_API. – Дата доступа: 23.09.2018.
2. Протокол HTTPS – что такое? [Электронный ресурс]. – Режим доступа: http://fb.ru/article/221368/protokol-https---chto-takoe. – Дата доступа: 24.09.2018.
3. SRTP – что такое безопасный протокол передачи данных в реальном времени? [Электронный ресурс]. – Режим доступа: https://www.3cx.ru/webrtc/srtp/. – Дата доступа: 22.09.2018.