SECURITY AND PRIVACY METHODS IN DISTRIBUTED SYSTEMS.

Irida Gjermeni[1*] Dudina Hoxha[2]

1. Department of Mathematic and Informatics, Agricultural University of Tirana, "Pajsi Vodica" St., 1029 Tirana, Albania

* E-mail of the corresponding author: igjermeni@ubt.edu.al

Abstract

Rapid technological developments and distributed systems have found their most significant expression in the field of communication and dissemination of information. This mass spread of communications through distributed systems such as: internet, intranet, web services, etc., has been influenced by a number of advantages that they present, which have to do with the ease, speed of communication, the ability to communicate in real time between two or more subjects that are located at great distances from each other, etc.

Increasing use of computers, computer systems, and distributed systems has increased the potential risk of damage or misuse of data and computer systems. The dangers that exist are many where some are with minor consequences and some with major consequences, such as: viruses that delete or modify data in systems, gain access to personal computers and use them to attack others, theft of credentials or credit card data, etc. Unfortunately 100% security in a distributed system does not exist despite the measures that can be taken, but taking some security measures minimizes the risk. While in institutions and private companies the protection measures are greater due to the organization, technical structures or investments made for security systems, etc. and thus ensuring a certain level of security, ordinary citizens or users are the ones who are most exposed and must show personal care in their protection. Therefore, they should have basic knowledge about the methods of its preservation.

In this paper, we first study the features and types of distributed systems, security methods through CAPTCHA systems, cryptography, firewalls, etc; DS access channels. As a conclusion, it is intended to build a program in Java, with NetBeans IDE environment that enables the encryption (encoding) of a file with the help of the symmetric encryption algorithm TEA, in this case the encryption of an image, its decryption and display after decryption.

Keyword: encryption algorithm, security, IOT

DOI: 10.7176/CTI/10-07
Publication date: December 31st 2020

1. Introduction

We are all witnesses to the fact that increasingly, human activity is shifting from physical or interpersonal communication to virtual communication in cyberspace. Digital technology has already become part of our daily lives, and has occupied the spaces of developing social, family and friendly relationships, professional activities, consumption and cultural activities.

Rapid technological developments and distributed systems have found their most significant expression in the field of communication and dissemination of information. This mass spread of communications through distributed systems such as: internet, intranet, web services, etc., has been influenced by a number of advantages that they present, which have to do with the ease, speed of communication, the ability to communicate in real time between two or more subjects that are located at great distances from each other, etc.

In addition, most of the information nowadays is stored digitally on computers as this provides great convenience for storing, copying and modifying it. Given that computer systems are interconnected, this further facilitates the dissemination of information from one entity to another or to an unspecified number of entities. The information stored in this form can be easily transferred beyond the borders of a country, in large geographical areas in a very short time. All of these advantages make digital information the most widely used form of information storage and exchange. This transformation has long raised a debate: What effect will it have on the secrecy and security of communications?

If at the beginning of the use of the Internet, the answer to this question could have been dubious, we can now rightly say that breaches of confidentiality and security of electronic communications no longer remain at the level of special cases, but have taken on the dimensions of a phenomenon.

Statistics that have emerged from recent studies show an extremely large increase in the use of distributed systems, particularly the Internet. According to The Internet World Stats (2021), the portal of statistics regarding Internet users reports 4.88 billion people around the world use the internet in October 2021 – that's almost 62 percent of the world's total population. This number is still growing too, with our latest data showing that 222 million new users came online over the past twelve months.

Just as the Internet has significantly facilitated the work and lives of people, at the same time have evolved the acute security and privacy problems that this system or other distributed systems have encountered and today even more are facing. .

In addition to the security of communication of ordinary users of public electronic communications services, "malicious computer attacks" have greatly questioned the security of the information or telematics systems through which these communications are realized, thus making the dimensions of the intervention of affect an indefinite number of persons.

In this way, the right to privacy of individuals can be significantly violated, who, in their daily interaction with the computer infrastructure, throw and transmit in digital form data of a personal nature. Since a large number of computers are usually connected to the Internet, this allows malicious people to gain unauthorized access to these devices by installing viruses while their user is browsing the Internet. .

This has brought to attention the enhancement and more advanced development of DS security and privacy protection methods and techniques. The fight to protect security and its inviolability continues. According to The Statistical Portal (2021), the global statistics portal on security spending worldwide reports that the cost of security of distributed systems worldwide is about $ 72.5 million.

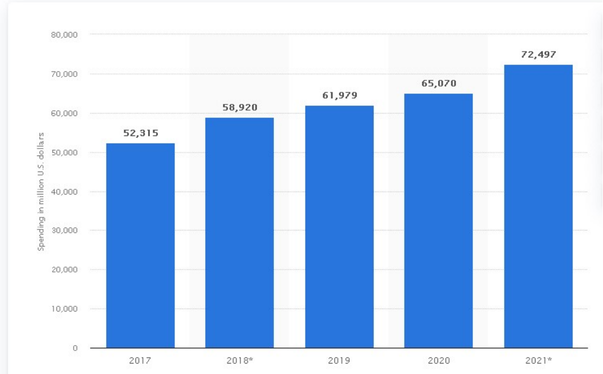


Figure 1: Worldwide security costs in $ million (vertical axis) over 2010-2021 (horizontal axis). Source: The Statistical Portal.

These expenditures are made for the development of technologies such as: firewalls; utilization of encryption technologies; intelligent security systems etc.

An expression of Larry Page (Google CEO), which is very relevant to the issue of security and privacy says: "For me, privacy and security are really important. We think of it in terms of both: There can be no privacy without security. "

The above statement is very current for the situation in which the security and privacy of DS is today, as well as for the focus of this topic. Distributed systems incorporate many of the most important technological developments of recent years and thus in a fundamental sense of technology, it is absolutely at the heart of modern computing knowledge. But, along with the rapid developments come various problems where the most important are and continue to be the security and privacy of these systems.

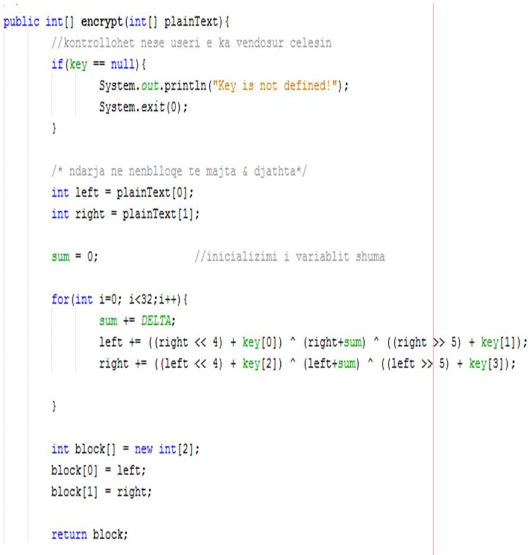
Therefore, this study attaches importance to the knowledge of methods and techniques of security of distributed systems. Although the possibilities for detailed information are numerous, in our country these methods are very little known. For this reason, I bring to the attention of ordinary people, who do not have much to do with the field of computing in particular, some of the cryptographic methods, certificates, firewalls, etc.

2. Methods

The TEA coding algorithm is programmed in C. It stands out for the simplicity of its design and implementation, as well as its use to give concrete illustrations of the nature of such algorithms. But, in this case, its implementation in Java with NetBeans IDE 8.1 framework is presented.

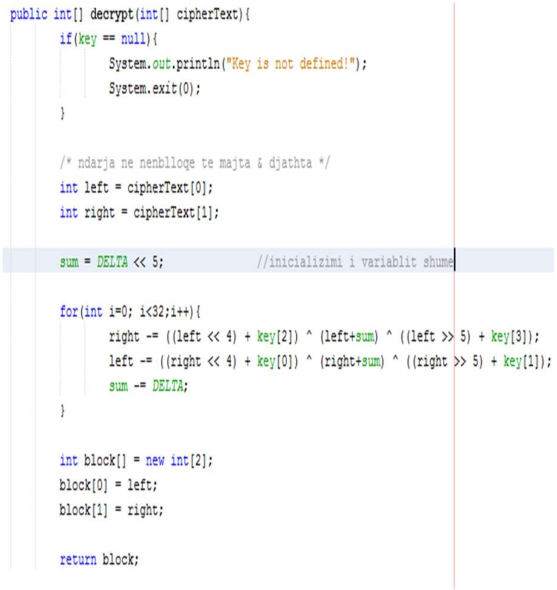
This program itself represents an interface that uploads an image, encrypts it and saves it in a specific folder, and then displays the decrypted image in a new interface.

In the NetBeans IDE 8.1 version, a new project has been created for the environment where it will work under the name encryption_decryption. Java Developement Kit 8.1 was used as the editor / compiler. The language for creating objects and components is Java.



```
public int[] encrypt(int[] plainText){
        //kontrollohet nese useri e ka vendosur celesin
        if(key == null){
                System.out.println("Key is not defined!");
                System.exit(0);
        }

        /* ndarja ne nenblloqe te majta & djathta*/
        int left = plainText[0];
        int right = plainText[1];

        sum = 0;                //inicializimi i variablit shuma

        for(int i=0; i<32;i++){
                sum += DELTA;
                left += ((right << 4) + key[0]) ^ (right+sum) ^ ((right >> 5) + key[1]);
                right += ((left << 4) + key[2]) ^ (left+sum) ^ ((left >> 5) + key[3]);

        }

        int block[] = new int[2];
        block[0] = left;
        block[1] = right;

        return block;
```

Figure 2-1 Encryption function



```
public int[] decrypt(int[] cipherText){
        if(key == null){
                System.out.println("Key is not defined!");
                System.exit(0);
        }

        /* ndarja ne nenblloqe te majta & djathta */
        int left = cipherText[0];
        int right = cipherText[1];

        sum = DELTA << 5;               //inicializimi i variablit shume

        for(int i=0; i<32;i++){
                right -= ((left << 4) + key[2]) ^ (left+sum) ^ ((left >> 5) + key[3]);
                left -= ((right << 4) + key[0]) ^ (right+sum) ^ ((right >> 5) + key[1]);
                sum -= DELTA;
        }

        int block[] = new int[2];
        block[0] = left;
        block[1] = right;

        return block;
```

Figure 2-2 Decryption function

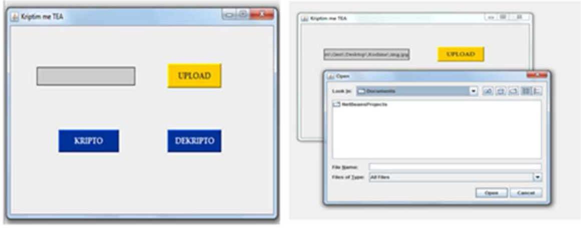
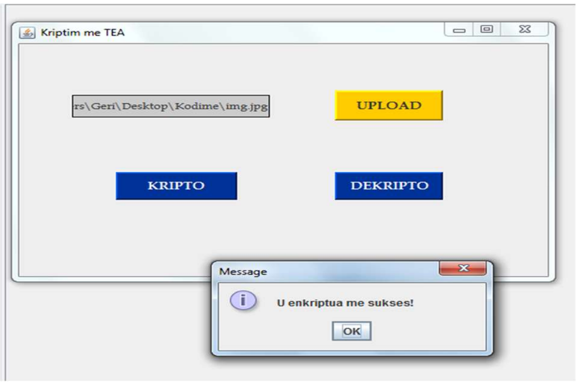


Figure 2-3 View after pressing the Upload button



U enkriptua me sukses!

Figure 2-4 Encrypted file view

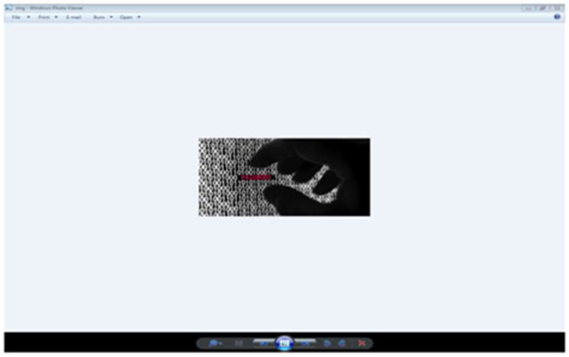


Figure 2-5 Decrypted file view

3. Conclusions

This paper addressed the role of DS security and privacy methods, while maintaining integrity and performance, regardless of the specifics or number of heterogeneous applications located in this distributed environment. The paper addressed the various ways that exist to integrate specific applications in organizations and not just to make these systems more secure, which makes their development and use as flexible as possible. People asked about knowing security methods answered that they knew very little about some of the methods.

These systems and applications enable more secure data transfer and storage. Intentionally or unintentionally, the current reality on the Internet and everywhere in computer networks is influencing the use of cryptography-based applications to become standard at the user level.

- In order to increase safety it is necessary to create some habits which are done instinctively during work. Shutting down the computer or open accounts when we leave the computer, disconnecting the Internet connection from the computer when we are not using it or occasionally checking security measures such as updating, occasionally scanning the computer with antivirus software, removing of unnecessary programs etc., are some of the basic actions.
- Using passwords is a very important element in ensuring that unauthorized persons do not gain access to your systems or personal information. Most people use short passwords that relate to personal information that can be easily remembered by them (birthdays, baby names, etc.) but it also makes it easy for other people to find it. It is suggested that passwords be as strong as possible containing letters (uppercase and lowercase), numbers, characters, and of considerable length. It is also advisable to use different passwords for different systems.
- Unfortunately many people use unlicensed software on their computers to save money doing so in addition to breaking the law and increasing their exposure to risk. Based on the analysis carried out by various laboratories, it results that more than 70% of them contain "malware" codes which are included in it and are not captured by protection systems.
- For any virus or attack that comes up, software developers in a short time create which fix the vulnerability of the affected system ensuring that that type of attack is blocked in the future. These settings are distributed to users via the update and are free. Keeping your computer and software up to date is very important as it creates opportunities for protection against known viruses. In many cases computers are affected by viruses which can be blocked by the updated system itself even in the absence of antivirus.
- One of the most important elements for our protection is the installation of antivirus, anti-spyware and firewall software. Using them can often reduce the performance of the computer but the installation and very significantly increases our defense. Using these licensed programs and keeping them up to date are two essential elements of personal safety. For example: AVAST software, AVG antivirus, 360Security, Avira antivirus, etc. for both PC and mobile devices.
- We can verify people who have physical access to our computers but it is very difficult to identify those who connect remotely when we are connected to a network or use a computer that is not personal. When we connect to networks that are not in our control or are open (such as when traveling to airports, internet cafes, etc.) care must be taken because in parallel with us in these networks can be connected and slaughtered persons who have malicious intent.
- Thanks to the use of the internet the speed with which we today communicate, buy or exchange information has become almost zero. But while performing these actions hackers can obtain information which brings financial consequences to the user. Using a trusted website for online shopping, taking precautions on the computer, checking the security options of "web browser" programs or updating them regularly are some minimal measures. AppScan is an application that enables website verification.

As a result, it was seen that the information and application of the program will be very valuable to anyone. It should be noted that despite all the measures taken, the systems will always have a percentage of risk of breach of security and privacy. Therefore, every other organization or unit is working to ensure that the security of DS applications is in line with all norms, based on cryptographic methods, which is already a well-established standard.

References

1. Coulouris.G, Dollimore.J, Blair.G & Kindberg.T (2012). Distributed Systems: Concepts and design.
2. Belapunkar.A...[et al.]. Distributed Systems Security: Issues, processes and solutions.
3. Reges.S & Stepp.M (v2, 2011). Building Java Programs: A back to basis approach.
4. The Statistical Portal, Statistics: http://www.statista.com/statistics/217362/worldwide-it-security-spending since-2010/

5. The Internet World Stats: http://www.internetworldstats.com/stats.htm

6. https://sites.google.com/a/ictedu.info/knowledge-centre/home

7. http://www.gazetatema.net/web/2015/08/05/siguria-dhe-privatesia-dy-iluzionet-e-koheve- moderne/