IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue-9, April 2019 E-ISSN: 2347-2693

Security Enhancement through Cryptography and Hardware Devices

Aruna Devi.T[1*], Tejaswini S Majjigi[2], Shyam Vaibhav. M S[3]

[1,2,3] Dept. of Computer Applications, Dayananda Sagar College, Bangalore, India

Corresponding Author: arunadevi@dayanandasagar.edu

DOI: https://doi.org/10.26438/ijcse/v7si9.7679 | Available online at: www.ijcseonline.org

***Abstract*—** Security is being a hot topic in present digital era. The growing usage of technology for communication generates data which is available everywhere but data security is the important issue which draws the attention of all. Cryptography and security is a notion to secure the network and information transmission through wireless network. With ever progression in digital system security has been appeared as a major concern. In this era of virus and hackers of electronic bugs and electronic fraud security is primary. The concept of hardware security has been normally related with the cybersecurity and cryptography. Cyber-attacks are usually more due to lots of users connected to the internet. The basic issues in guarding the safe transmission of data through the web are concern of the security. This paper emphasizes on the key concepts of cryptography and security on critical infrastructure devices to overcome the threats of computer network security.

***Keywords*—**Cryptography, Cybersecurity, Network Security, Hardware security

I. INTRODUCTION

Cryptography is related with the procedure of converting basic script into undetectable script and vice-versa. Cryptography helps in generating codes where they allow data to be reserved private. Cryptography translates information into some form that is not readable by an unofficial user, making it to transmit without unofficial entities interpreting it back to readable form, by compromising the information. Data security has been used by cryptography on many stages. The data cannot be read without key to decode information. The data preserves its unification during transmission and while being stored back [1]. Security invoke to all the measures that are taken to protect or to ensure that only people with permission are allowed to go through the process. Computer data usually travels from one system to other, without having the protection to the data. Once the data is not under control, data hackers might modify or misuse our data for entertainment or for their advantage. Cryptography can format information in unreadable and transform our information making it secure while sending data between networks. The technology is built on the secret codes, improved by modern mathematics that secures our information in many different ways. Network security is mix of numerous layers of barriers in the Network and at the Network. Strategies and controls are actualized by each network security layer. Access to network is picked up by approved clients though vindictive performing artists are without a doubt obstructed from executing dangers and adventures. Securities are classified as network security and hardware security. Network security can be Firewall, Virtual Private Network (VPN), Web Security, and Wireless Security, etc., Hardware security is vulnerability insurance that comes as a physical gadget as opposed to programming that is introduced on hardware of the PC framework. Hardware security is concern to a device which is used to scan system network traffic. A few precedents like hardware firewalls, proxy servers, hardware security modules, where they provide cryptographic keys for remarkable functions like encryption and validity for different systems. Hardware devices can provide added security than software and can also complement an supplementary layer of security for the system. In this paper we have discussed about the cryptography and hardware device security and compared both software and hardware device security.

This paper is organized as follows: Section II Related work, Section III Introduces Cryptography, Section IV explains about Security, Section V Comparison of different security, a brief conclusion is discussed in section VI.

II. RELATED WORK

The concept of a cryptographic hardware device depict its capacities, uses and executions and the features offered by hardware security, the basics of cryptography, Public Key Infrastructure and the use of smart cards [1]. The extent of hardware security and the difficulties undertaken inside the hardware security space and to support various industries [2]. An overview of security and various techniques through

which security can be enhanced by cryptography hardware [3].

III. CRYPTOGRAPHY

Cryptography is the process of converting original information or the data into a secret code using the encryption formula or the code to secure the data from the unauthorized user or the hacker. To protect our data the security method used like firewall in the cryptography method [3]. In this different kind of technique are used to protect or to secure the data in the storage place or during transmission of data from one host to another host. In this method the information is converted into a new format and secure our information from the unauthorized persons or the hackers. It works like a drama artist because the drama artist wears the mask plays the different roles likewise in this cryptography also it hides the originality and then shows its reality only in front of the authorized user or the owner. All these tasks are performed only to protect our secrete data and our hardware system. To do this task the hardware should also support otherwise it cannot able to perform the task [5]. Cryptography does not only secure the information from malpractices, modification and it also used to find out the authorized users. Authentication is a must to access the data or the information. Cryptography is an art of protecting or securing the data of the computer or information of the user. The cryptography is also known as cryptology. The cryptography contains the pre written or the self-generated codes or the program that makes the data and the information secure. It converts the data or the information into a special format and this special format can be understood only by the cryptography and the authorized user or the owner Figure 1. Therefore, any unauthorized people cannot access, read or do any type of malpractices or to alter. If an unauthorized people want to access the data the special code should be recoded. The information security uses the cryptography on different steps or in different levels. The data or information cannot be decoded without the help of the secret code or the formula. Because of this code or the formula, it can be more secure during the time of transferring the data and during the time of storage. The cryptography protects the data like an electric fence protecting the fields. The verification method means that the data is verified before sending and after delivering the data, that means the sender and the receiver of a data can be confirmed. This verification is done by using the secret code, program or by using the secret key or the formula [6]. There are different types of processes for encryption of the data some of those commonly used algorithms are

- Secret Key Cryptography
- Public Key Cryptography
- Hash functions

A. Secret Key Cryptography

The Secret Key Cryptography is also known as SKC in short. In this type of cryptography, it uses only one formula or the secret key to encryption and decryption of the data or the information. It includes only one level of security. This type of the encryption and decryption is known as symmetric encryption.

B. Public Key Cryptography

The Public Key Cryptography is also known as PKC in short. In this type of cryptography, it uses two secret keys or the formula to encryption and decryption. These two types of secret keys are named as public key and the private key. Such types of encryptions are called as asymmetric encryption. It includes duel level of security in it. Here the private key can only access by the owner of the data or the information. The receiver will encrypt or decode the data using the public key. In this method the receiver knows who sent this data and other information.

C. Hash functions

In this method there are no keys used and it is called as one-way encryption. They are primarily used to approve or to verify that the files are not altered or accessed by unauthorized peoples.

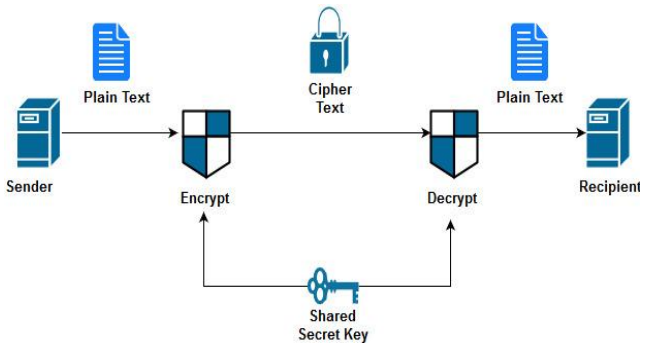

Figure 1: Cryptography

IV. SECURITY

In information technology (IT) the security means protecting or securing the data and the information from the hackers, and also from modification, alteration of data from the unauthorized persons or the hackers. Hardware security is a method derived out of cryptographic engineering hardware design. Hardware security includes the firewall and the proxy servers. It also includes the authentication of systems and it also provides another level of security to the system. Sometimes the hardware security secures the system and data from the viruses attacked from other external sources like internet, wireless networks etc. Hardware security is powerlessness assurance that comes as a external device instead of software this is introduced on the hardware of a PC framework. The hardware security module (HSM) is the

external devices connected to pc framework that protects and succeeds the digital keys for robust validation and provide crypto process [7]. These modules traditionally come either in module card or an external device that appends straightforwardly on a PC or server. A hardware firewall is a element that is connected between the system and the device for interfacing with the web. A software firewall is a program which is introduced on the PC with the Internet connections.

A. Hardware Device Security

Hardware security is susceptibility protection that will come in the form of a external device instead of software that is installed to the hardware of a computer framework. There is a dominant trend of securing critical infrastructures from cyber security attacks using software tools from the network security domain. However, when it comes to cryptography and security services there exist many attacks that a malicious entity can mount on a critical infrastructure device [8]. Using Hardware Means to secure Critical Infrastructure Devices.

a. Full Disk Encryption (FDE)

It is an encryption made at the hardware level of the computer. FDE acts automatically by translating data in the hard disk to unreadable format where unauthorized persons who don't have the key cannot undo the conversion of data to readable form. Without the correct verification key, even if hard disk is removed and added to some other pc, the data will be safe. FDE can be installed at the time of production or by installing some special software driver later stages.

b. Trusted Platform Module (TPM)

Trusted Platform Module (TPM) technology is intended to give hardware-based security. A TPM chip is a protected crypto processor that is maintained to complete cryptographic tasks. The chip incorporates various physical security systems to make it alter safe, and pernicious software is unfit to mess with the security elements of the TPM. TPM is special chip at the final stage, device that maintains RSA encryption key (EK) especially to the host pc for hardware verification. Every TPM chips contains two RSA keys called endorsement key. The key is kept inside the chip of devices and it cannot be retrieved by the software. While user acquires the ownership the new root key is formed. Then the second key is called a confirmation identity key that protects the device from unofficial access.

c. Hardware Security Module (HSM)

A hardware security module (HSM) is an external component that protects and accomplishes keys for solid verification and yield method. These modules will normally originate in the form of a plug-in card or a physical or external device that right linked to a computer. The function of HSM are locally available to protect cryptographic key generation and its storage at any rate for the top level and most sensitive keys which are regularly called master keys, key administration, use of cryptographic and sensitive data material for instance performing encryption or advanced mark capacities, It is totally combination or the mixture of the symmetric and the asymmetric cryptography verifying full software stack from consistent or physical assaults [9].

V. COMPARISON BETWEEN SOFTWARE SECURITY AND HARDWARE DEVICE SECURITY

A. Hardware Security

- Hardware security is one of the protections that come in the form of a physical device protection. It can be used in a device to scan a system or to manage monitor network traffic.
- In hardware security the program for smart cards executes basic code like the cryptographic algorithms which is attack free without physical access to chip.
- The running code in a physically protected chip like HSM or a digital card is used for protecting from software bugs. If there is a software bug in a HSM it can be broken just as any webserver, laptop and smart phone.
- Hardware based security utilizes a devoted integrated circuit (IC), or a processor with particular security hardware, explicitly intended to give cryptographic capacities and ensure against attacks. Security activities, for example, encryption/decryption and validation, happen at the IC hardware level. Sensitive data, for example, keys and basic end application parameters are ensured inside the electrical limit of crypto hardware.
- The security IC contains circuit squares, for example, a math accelerator, arbitrary number generator, non-volatile memory, tamper detection.
- Cybercriminals are deflected from attacks on hardware-based security. When attacked the security IC is fit for closing down activities and destroying sensitive information before being compromised.
- Hardware based security is compelling in all application situations particularly those where the end gear is uncovered and physically open to the trouble makers [10].

B. Software Security

- Software security is software or the computer program that is installed in a computer system.
- The software-based security can be compelling in physically secure situations, preventing unapproved access to the framework.
- When hackers know the software, they may send payloads to exploit vulnerabilities and run any arbitrary code they want remotely and destroy our data.

- A software security framework puts a heap onto a host processor. The software approach is the frail connection inside frameworks security engineering [11].

VI. CONCLUSION

The quick growth of internet technology, the network and data security have become an inevitable concern for any organization to secure the data. In this paper we have discussed the security types and compared with the different types of security. Data security can be maintained using different techniques like hardware device security and software security. Hardware devices can be built that it can identify the attacks at the application level. A hardware device includes its own OS and has embedded technology specifically designed for special-purpose processing such as cryptography. That means it's faster and more effective than software. As the hardware is built from the ground up to handle web services security, it won't be prone to hackers that can foil software such as buffer overruns. The best way is to secure the data by using hardware device-based security and the software-based security is not sufficient to protect the data whereas a more heavy-duty hardware-based solution is required.

ACKNOWLEDGMENT

The authors acknowledge Dayananda Sagar Institutions, Bangalore, Karnataka, India for providing the facilities for carrying out the research work.

REFERENCES

[1] Shyam Nandan kumar," Review on Network Security and Cryptography", International Transaction of Electrical and Computer Engineers System, 2015, Vol.3, No.1,1- 11.
[2] Jim Attridge, "An Overview of Hardware Security Modules" Version 1.2 of GSEC Practical Assignment for GIAC Certification, January 14, 2002.
[3] Yier Jin, "Introduction to Hardware Security", Department of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32765, USA.|13 October 2015
[4] Dr Sandeep Tayal, Dr Nipin Gupta, Dr Pankaj Gupta, Deepak Goyal, Monika Goyal, "A Review paper on Network Security and Cryptography", ISSN 0973-6107 Volume 10, Number 5, 2017.
[5] Sarita Kumari,"A research paper on cryptography Encryption and compression Techniques", International Journal Of Engineering And Computer Science, ISSN:2319-7242 Volume 6,4 April 2017.
[6] Shivangi Goyal,"A Survey on the Applications of Cryptography", International Journal of Engineering and Technology Volume 2 No. 3, March, 2012.
[7] Banga, M., Hsiao, M. VITAMIN," Voltage Inversion Technique to Ascertain Malicious Insertion in ICs", In proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust, Francisco, CA, USA, 27-27 July 2009, pp. 104-107.
[8] Love E. Jin, Makris Y," Proof-Carrying Hardware Intellectual property: A Pathway to Trusted Module Acquisition", IEEE Trans. Inf. Forensics Secure, 2012, 7, 25-40.
[9] Chakraborty R, Wolff F Paul, S Papachristou, C Bhunia, S. MERO, "A Statistical Approach for Hardware Trojan Detection", In Cryptographic Hardware and Embedded Systems" CHES 2009, Springer: Berlin, Germany; Heidelberg, Germany, 2009, Volume 5747, pp. 396–410.
[10] Bloom G, Simha R, Narahari B, "OS Support for Detecting Trojan Circuit Attacks", In Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust, San Francisco, CA, USA, 27 July 2009, pp. 100–103.
[11] Banerjee, S.K. Pandey, "Research on software security awareness: problems and prospects", ACM SIGSOFT Software Engineering 35(5):1-5 October 2010.

Authors Profile

Mrs. Aruna Devi. T received B.Sc., degree and Masters in Computer Applications from Madras University. M.Phil, Computer Science from Alagappa University. She has published good no of research papers in referred Journals. Also authored Computer Graphics Book. Currently working as Assistant Professor with 17 years of teaching experience in the Department of Computer Science and Applications, Dayananda Sagar College, Bangalore, India.

Ms. Tejaswini S Majjigi received Bachelor of Science, PMCs from Karnataka University, Dharwad in 2018. She is pursing master of computer application in Dayananda Sagar College, Bangalore. Her main interest is on cryptography and hardware security, Bitcoins, IoT, Cloud Computing.

Mr. Shyam Vaibhav.M.S. received Bachelor of Computer Applications from Mangalore University. He is currently pursuing his Masters of Computer Application in Dayananda Sagar College, Bangalore. His interest is on cryptography and hardware security, Cloud Computing, Big data, Artificial Intelligence.

