Digital Signal Processing useful for Cyber Security

Shruti Shivhare

Student, Institute of Engineering & Science, IPS Academy, Indore, India

Abstract: In this world of ever growing technology, everyone is competing in the race of innovation and research. So let me put a step ahead for some innovation in the field of EC engineering for the application of cyber security. This research paper is being presented with an aim to find a solution for the cyber security by applying digital signal processing for the identification of user. Here firstly there is a brief description of what is digital signal processing and also a brief introduction of cyber security is provided. An overview of the techniques that are already in practice for security has been given in the paper. They follow the basic security principles such as confidentiality, authentication, integrity, open access control, etc. Some of the techniques are Cryptography, Public key infrastructure, Internet security protocols, User authentication mechanisms, Network security and firewalls. Also the innovation in these technologies is illustrated below. The use of the heart beat sensor to create the digital pulse waveform and analyzing these signals to identify the original user of the system Also the digital image processing of the eye retina images is also useful for the identification and security purposes. The experimentation & results are also provided regarding the new technique. Also the proper way of implementation is also discussed elaborately in order to gain qualitative results.

Keywords: Cryptography, cyber security, digital signal processing, transmission protocols, firewall.

I. INTRODUCTION

Today in this modern human civilisation everyone is in the race of success. In this era of enormous requirements, one needs to be fully secure and safe. Nowadays cybercrimes have been the major reason due to which people hesitate in using the internet. But this hinders them from the major benefits of web which they deserve to get. The solution lies in the electronics and communication engineering. Due to the digital processing of the signals, one can built a new and full proof digital system for the cyber security [1].

So let me first introduce with the digital signal processing. Digital signal processing has been constantly observed in the fields like biomedical, engineering, speech communication, acoustics etc. Actually it is performed using a digital computer. In order to perform digital signal processing an interface between the digital and analog signals is created. An analog to digital converter is mostly preferred. It could also be a large programmable digital computer or a small programmer designed to perform various operations. The benefit is that it can be reprogrammed without modifying the hardware. The performance of this is not affected by temperature or age. The uniform results can be obtained as there is no variation due to component tolerance. Thus digital signal processing is an overall best solution in order to serve the security purposes [1-2].

Now moving on to the cyber security, I will give a brief introduction to it. As technology improved, the communication infrastructure became extremely mature and new applications began to be developed for various user requirements. Then some people realized that the basic security measures were not enough in order to fulfil the need for security. Then the encoding and password security was not sufficient. Thus the new and advanced methods of security were employed such as the cryptography, firewalls, virtual private networks etc. So these new ways employed in order to provide safety and security to the data of the users which are strict defence measures against the cybercrimes is termed as cyber security [1-4].

II. METHODS OF SECURITY: AN OVERVIEW

The security methods are based on some of the basic principles of security. Some of the principles are confidentiality, authentication, integrity, non repudiation, access control, availability. The various techniques are:

A. *Cryptography Techniques*

Cryptography is a process in which the plain text messages are embedded in order to transform the plain text into cipher text. Cryptanalysis is the technique through which the messages can be decoded from an unreadable format to readable format. This is basically done by the cryptanalysts. Cipher text is produced by codified messages In order to convert the plain text to the cipher text various substitution and transposition techniques are used. The process of encoding plain text to cipher text is called as encryption. On the other hand the process of converting cipher text to plain text is termed as decryption [2].

Figure 1: Cyber security

B. *Public Key Infrastructure (PKI)*

It consists of various features such as digital certificate which is a disk file and binds the user with its public key. The certification authority issues digital certificates OCSP and SCVP are the protocols for the online checks. Private key management is very important and losing private keys is very risky. Issues related with the PKI are dealt with the PKIX models. PKIX play a very important role to solve these issues.

C. *Internet Security Protocols*

HTTP protocol for request response, TCP/IP for actual communication is used by the internet. For securing communication in the internet the secure socket layer (SSL) is the most widely used protocol in the world. The SSL handshake establishes necessary trust between the client and server. The other protocols used are TSP, SET, TLS etc.

D. *User Authentication Mechanism*

Establishing the identity of user/system is concerned with the authentication. Most common mechanism of authentication is clear text passwords. Encryption of passwords and message digests of passwords are used to stop transmission of protocols. Authentication token is a more secure two factor authentication mechanism.

Figure 2 Output Waveforms

E. *Network Security, Firewalls, And VPN*

Corporate networks can be internally or externally attacked and information can be leaked out. A special type of router which applies rules for allowing and stopping traffic is called firewall. The strongest firewall architecture is screened subset firewall. Network Address translation (NAT) allows few IP addresses to be shared across network thus IP address is saved. Authentication and confidentiality services are served by IPSec. A virtual private network is both virtual and private. A VPN is used for linking up and connecting offices with other companies in inexpensive fashion.

III. INNOVATION BY DIGITAL SIGNAL PROCESSING

Digital signal processing channels can be used by the industries in order to serve the purpose of cyber security. By using the various digital signal waveforms that can be traced from the human body can be used for the security purposes.

A. *Security by Heartbeat Sensing*

Here heartbeat is sensed and a digital pulse is created which varies from each and every individual. Due to the variation in the tissue cells & the RBCs, WBCs & platelets present in the blood contains different structure, behaviour & counts, every individual have a distinct pulse varying from one to other. This waveform is used to detect the identity of the user. It is generally sensed by a heartbeat sensor. It uses a pair of LED and LDR and a microcontroller for its operation. Her first the pulse rate of heart per minute is counted then LED light is passed from one side of finger and received by LDR on other. The voltage variation is measured by OP-AMP. Then this amplified signal is detected by microcontroller and the digital output pulse is generated. This waveform can be used in he production of a security protocol. This way the heartbeat is useful in sensing pulse of the ethical user.

©2016, IJAERA - All Rights Reserved

B. Security By Eye Imaging

In this method eye imaging is used for the security purpose Here the digital image of the retina of eye is captured. Digital signal processors are used in obtaining the information from the captured image of the eye retina. If the biological information of the user matches with that of the user then the user is legal otherwise not. That is the stem cells behaviour & structure differs from person to person present in the tissues of retina. This way the different retina imaging of the individuals is helpful in knowing the identity of the user.

This way the use of digital signal processing is helpful in order to get the identity information of the users. A whole protocol system can be built on the basis of human body controlled digital signal analysis. This signal assures the safety and security of the data of the users [1-4].

IV. EXPERIMENTAL PROCEDURE & RESULTS

> *"A theory is something nobody believes, except the person who made it*
> *An experiment is something everybody believes, except who made it"*

A. Heartbeat Sensing

a. First of all heartbeat sensor is used in order to sense the heartbeat.
b. A pulse is created by digital signal processing of heartbeat.
c. The cells in the tissues of heart consist of different structure & behaviour which is recorded.
d. Also the amount of blood cells and platelets in the blood differs. Thus readings are taken.
e. Then these are compared with the original records. If they match then the identity is verified.

B. Eye Imaging

a. In this technique firstly the image of the retina of the eye will be taken
b. The image will be taken using digital signal processors.
c. The output will be provided in the waveforms generated.
d. These waveforms vary from person to person due to disparity in the structure, behaviour & count of the stem cells present.
e. Then these will be compared with the original information available.
f. If on comparison it purely matches the original then the identity is confirmed.

V. IMPLEMENTATION

Today in this era of technologically advanced human civilisation the problems are becoming more complex but their solution lies in the problem itself. Here I would be telling you about the implementation of this new technique which is innovated. This is one of the most feasible techniques as it requires only the already available resources for its task completion. Moreover it is easily accessible & not very complex. In order to implement it I require only 2 things, first is the software containing original information and having the ability to perform comparisons. The second one is the testing software where the tests could be performed easily that is containing a heartbeat sensor & digital signal image processing to take the image.

The most important task for the implementation is the designing of the software which will be done by the sensors and microcontrollers present in order to perform proper digital signal processing & producing an actual output. After the designing of the software, it requires its proper operation which will be done by using it for trails. After successful trails it will be working based on the principle of testing & comparing it with the original results thus checking the original identity of the user [4].

VI. CONCLUSION

Through this research paper we get an idea of the digital signal processing channels which are operated by either analog to digital converter or digital computers. As diamond cuts diamond I, in a similar way digital signal processing is used here in order to curb out the problem of cybercrimes. Also a brief description of the cyber security problem, how major problem is it and the solution by EC engineering. Digital processing of signals is useful in te search of finding solution to the problem of cyber security. Thus it can be concluded that the sensing of the heartbeat for the identification purpose is one of the most accurate way and secure. Also the digital imaging of the eye retina by digital signal processor is one of the simplest and fully safe method to know the exact identity of the user. So finally it can be concluded that digital signal processing is also able to find the solution for the cyber security.

VII. ACKNOWLEDGEMENT

I, Shruti Shivhare, student of Electronics and Communication Engineering Department of IES, IPS Academy solemnly declare that the research paper entitled “DIGITAL SIGNAL PROCESSING USEFUL for CYBER SECURITY” has been completed. I avail this opportunity to express my gratitude towards respected HOD Mr. Rupesh Dubey and the College Management for giving me the facilities and the privilege to carry out this work successfully. I am indebted and thankful to my faculty for their purposeful and able guidance by which I could carry out this research work.

VIII. REFERENCES

[1] Raman, Bhaskaran. "Cryptography & Network Security." IIT Kanpur, May (2005).

[2] Nagpal, Sujata, Shashi Bhushan, and Manish Mahajan (2015), "Image Watermark Embedded Using Dwt, Neural Network and RSA." International Journal of Advanced Engineering Research and Applications, Vol. – 1, Issue – 7, pp. 276-284.

[3] Singh, Gurjeet. "Performance Analysis of Quality of Service Stability Methods in WiMax Networks." (2015), International Journal of Advanced Engineering Research and Applications, Vol. – 1, Issue – 8, pp. 337-344.

[4] The Wikipedia website (online) Available: http//:www,Wikipedia.org.