“PRATYUG”
(THE TOTAL SECURITY SYSTEM)

SIVARAMAN .S[1] **NADADUR CHANDAN**[1] **VIJAY.N**[1]
siva4593@yahoo.com *chandanone2002@yahoo.co.in* vijaycage56@yahoo.co.in
[1]Department of Information Technology#Department of EEE Sri Sairam Engg College Chennai-600044
INDIA.

ABSTRACT :- “*The innocent are always the first to suffer*”. This is an often used proverb. In our quest to make them strong we have devised a total hack proof system for the communication process. In our mission the hackers are not the hunters but the prey. So we introduce a new security system called the bio scanning and sensing security system**.** Centralized computers are employed as the database storage systems in the network security process. The systems input signals are sent by the biometric sensors that are being programmed for sensing the retina and fingerprints of the human body .The process is carried out in three phases of authentication and identification.1)PFP SENSING 2)FAREN-EYE TESTING and 3)KEY-SPEED TECHNIQUE. The encryption and decryption process of the message or the information uses the sequential authentication-identification methods of the above phases, the bio-signal inputs acts as a shield cover for the message and can be accessed only if the input signals matches with those in the database with respect to the public key given i.e. the logical AND output is 1 and it is transmitted to the service requester. **.** The user’s systems are always online with the centralized database system server for transmitting and receiving the input and outputs which is nothing but accepting or denying the access of the private sector of a person’s information. Thus we reveal a new leak proof network security system which proves to be a real un-hackable network security. Thus it provides a permanent protection from the hacking community.

1. INTRODUCTION TO NETWORK SECURITY.

The requirements of information security within an organization or world wide networking system have undergone major changes in last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. An example is the use rugged filing cabinets with a combination lock for storing sensitive documents. The other example is personal screening procedures used during the hiring process.

With the introduction of computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as time-sharing system, and need is even more acute for systems that can be accessed over a public telephone or data network. The generic name for the collection of tools designed to protect data and to thwart hackers is computer security. The other major change that affected security is the introduction of distributed systems, and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer. Network security measures are needed to protect data during transmission. In fact, the term network security is some what misleading, because all organizations interconnect their data processing equipment with the collection of interconnected networks. Such a collection is often referred as internet.

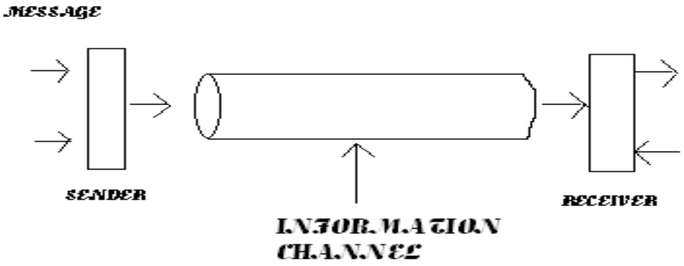

Figure 1: security system

There are no clear boundaries between these two forms of security, for e.g. one of the most publicized types of attack on information systems is a computer virus.

2.INTRODUCTION TO PROJECT

This security system consists of three sequential phases of identification and authentification where a centralized computer system or a server (dynamic) acts as the database for the recognition process. All the users systems are in online with the database while the process goes on .The three main phases of the security system are

1)PFP(PRINT-FLOW-PULSE) SENSING

2)FAHREN-EYE TESTING.

3)KEY-SPEED TECHNIQUE

The first two phases of the project makes use of the biometric sensors to authenticate the user. Thus Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. The key characteristics that are emphasized in our project are as follows:-

- *Universality*: Every person should have the characteristic. People who are mute or without a fingerprint will need to be accommodated in some way.
- *Uniqueness*: Generally, no two people have identical characteristics. However, identical twins are hard to distinguish.
- *Permanence*: The characteristics should not vary with time. A person's face, for example, may change with age.
- *Collectibility*: The characteristics must be easily collectible and measurable.
- *Performance*: The method must deliver accurate results under varied environmental circumstances.
- *Acceptability*: The general public must accept the sample collection routines. Nonintrusive methods are more acceptable.
- *Circumvention*: The technology should be difficult to deceive.

3.THE SECURITY SYSTEM

3.1 EXISTING SYSTEM

The current scenario where we see certain conventional encrypting algorithms such as Triple DES, Blowfish, RC5-114, CAST 128 uses cipher selecting criteria such as exhibiting considerable cryptographic strength, internet based applications, modern symmetric block cipher techniques which have been developed since the introduction DES. These techniques lack the power of efficiency, which means unstoppable eavesdropping, privacy of secured messages. Thus these methods do not ensure confidentiality for the users and does not reveal a leak proof security system.

3.2 PROPOSED SYSTEM

This security system consists of three sequential phases of identification and authentification where a centralized computer system acts as the database for the recognition process. All the users systems are in online with the database while the process goes on. The three main phases of the security system are

1)PFP(PRINT-FLOW-PULSE) SENSING

2)FAHREN-EYE TESTING

3)KEY-SPEED TECHNIQUE

4. PFP SENSING SYSTEM

In this technique the biometric device is designed for checking the finger print of an authenticated person and then checks for the pulse and blood flow in the sensing area.The fingerprint collected is cross referenced with databases from around the country. Minutiae is the term used to describe recognizable details on a fingerprint. Details are marked, by the software, on the digitized image of the fingerprint.

Figure 2: PFP sensing system

The system is also designed to check the blood flow using the infra-red sensor added and also checks for the pulse in the finger area. The IR technique checks for the motion of hemoglobin in given elapse of time such that to authenticate whether the person is kept an alive original input and the pulse is checked for the normality of a person i.e. to verify whether he is in normal state not being forced to enter network. Fingerprints have been in use for a long, long time for forensics identification. Sensor technologies for acquiring the data include Thermal, Capacitance, Ultrasound, and Optical. Typical features are "minutiae," which are the little bumps, breaks, rapid shifts, etc. in the otherwise smooth curves of the fingerprint pattern.

5. FAHREN-EYE SENSING

Iris recognition today combines technologies from several fields including, computer vision (CV), pattern recognition, statistical interference, and optics. The goal of the technology is near-instant, highly accurate recognition of a person's identity based on a digitally represented image of the scanned eye. The technology is based upon the fact that no two iris patterns are alike.

This technology looks at the unique characteristics of the iris, the colored area surrounding the pupil. While most biometrics have 13 to 60 distinct characteristics, the iris is said to have 266 unique spots. While most biometrics have 13 to 60 distinct characteristics, the iris is said to have 266 unique spots. Each eye is believed to be unique and remain stable over time and across environments (e.g., weather, climate, occupational differences). The testing undergone also checks for the human temperature in the eye part using a Wein-bridge chip where it is been integrated along with the regular scanner using the concept embedded systems.

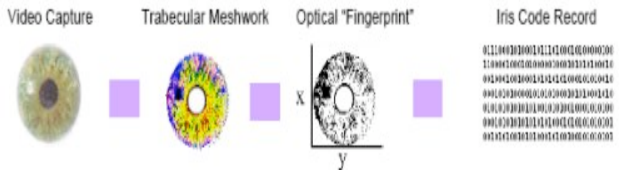

Figure 3: scanning the eye

The testing undergone also checks for the human temperature in the eye part where it is given a common maximum minimum limit in the database which is done using a small temperature finding device in the system which is nothing but a wheat stone chip. The temperature is converted to current using the chip as it works on the formula

$$H=I^2R$$

H→ Heat produced

I→ Current

R→ Resistance

Thus the heat produced from the sensing area is converted to current and detected within the system. Although each pattern normally remains stable over a person's lifetime, it can be affected by disease such as glaucoma, diabetes, high blood pressure, and autoimmune deficiency syndrome

6. KEY-SPEED TECHNIQUE

THE THEOREM

"Each person's typing pattern is unique and distinct"

PROOF:

We have devised a new security process based on this theorem. It is literally based on "Summation Codes".

BASIC PARAMETER:-

Speed :

Time :

Frequency :

Intensity :

In this technique the software is developed in such a way that the user is asked to re-type the given two to three lines of text in the given text space and press ENTER key only after the completion phrase. The time taken to press the keys of text is noted until the enter key is pressed. The user is asked to give the aFx value which is used to encrypt the message.

a- Alphabet (a-z, case insensitive)
F- Functional format (S/R/J) S-straight forward, R-reverse, J- Jumble
x- Multiplier (1-100) with two decimal places

The alphabet chosen will have the value 1x, according to the functional format (F). The other alphabets will take their respective values multiplied by the multiplier 'x'.

For example, if the alphabet is 'B' and the multiplier is 1.50 and the functional format is straight forward, then

B	-	1x1.50
C	-	2x1.50
.	-	.
.	-	.
A	-	26x1.50.

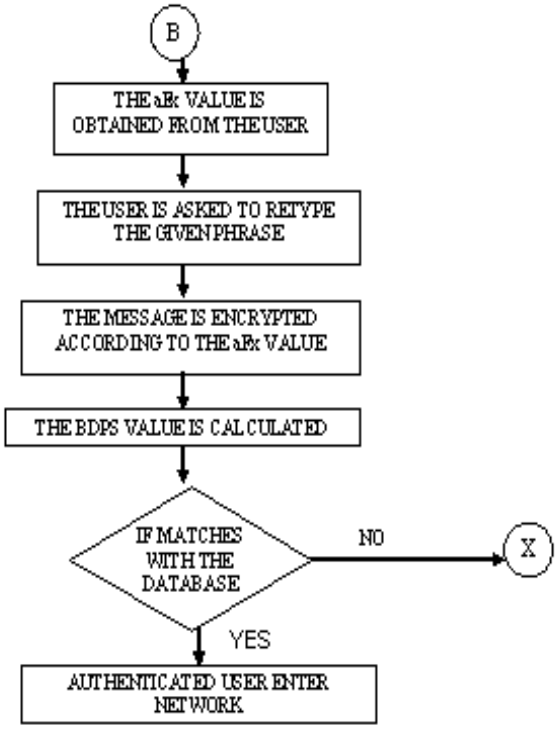
B
THE aFx VALUE IS OBTAINED FROM THE USER
THE USER IS ASKED TO RETYPE THE GIVEN PHRASE
THE MESSAGE IS ENCRYPTED ACCORDING TO THE aFx VALUE
THE BDPS VALUE IS CALCULATED
IF MATCHES WITH THE DATABASE
NO
X
YES
AUTHENTICATED USER ENTER NETWORK

Figure 4: Key-speed flow

For a given phrase that has to be typed each character will be converted to the corresponding values above and hence they are converted to their respective binary code. To differentiate two characters we use an OR "|" operator and to refer to an blank space we use an Dollar " $"symbol. The numeric and the special character will be converted to its jumbled values selected by the users while initialization. Each and every character converted to its binary form contains same number of bits where the maximum is "26x".

After converting all the characters, the total number of bits encrypted is found and the number of bits per second is calculated (bdps-binary digits per second). This value is normalized to max-min value and stored in the database. Thus the user is identified and authenticated. If his key-speed is within the normalized value stored in the database.

7.PRATYUG FLOW ALGORITHM

- START
- GET THE PUBLIC ENCRYPTION
- GET PFP-SENSING INPUT
- IF IT MATCHES THEN GET THE FAREN-EYE INPUT
- IF THAT ALSO MATCHES THEN GO FOR THE KEY-SPEED TECHNIQUE.
- IF THE USER PASSES ALL PHASES HE IS AN AUTHENTICATED USER.
- IF ANY OF THE PHASE FAILS PARALLELY IT STOPS AND DOESNOT GOES TO NEXT PHASE.
- IF ALL MATCHES THEN THE USER ENTERS HIS PRIVARE NETWORK.
- END.

8.APPLICATIONS

The natural application of biometric technologies is replacement of PIN, physical token or both needed in automatic authorization or identification schemes. Additional uses are automation of human identification or role authentication in such cases where assistance of another human needed in verifying the id card and its beholder. Different application cases include:

- Logical access control in computer, net recourse, role, file and network access.
- National identity cards and passports, traditionally verified by another human.
- More generally preventing fraud of fake identities like in US welfare where no proven, official and secure official ID card is in use.
- Banking, using ATM:s, net access or telephone.
- Physical access control of buildings, areas, doors and cars.

Natural targets for piloting these things are institutes concerning national security. The recent news have told that like military has taken in use an face scanning system in some sites. Possible, more widespread use of biometrics could be incorporating it to the national ID card project. It will start without, but biometric methods could easily replace the PIN needed. Thus our project in securing the network community will make sure that the hacker community gets their bait by trying the illegal methods.

9.CONCLUSION

Authorizing the user with secret PIN and physical token is not enough for applications where the importance of user being really the one certified is emphasized. If biometric technologies are when not used, we accept the possibility that the token and secrecy of PIN can be hacked off. On applications like bank account cards the companies count the money lost because of fraud and value the risk with the bottom line. Biometrics offers many advantages to the law enforcement community. These advantages fall into two distinct areas, but are not mutually exclusive.

Firstly, the business, process, cost and security advantages that biometrics bring to any organization can be applied throughout the world, which is a collection of agencies, all of which have premises and data to protect. Secondly, there are the direct advantages to law enforcement itself as applied to the two major objectives of the prevention and detection of crime. Clearly, there is a wealth of experience and expertise already applied in these fields and technology is enhancing them at a rapid pace.

The possibilities cannot all be mentioned in this paper, because of space and the fact that many more ideas exist than we have even begun to think about. We hope that this short paper will stimulate debate and bring even more of these possibilities to the fore. Biometrics itself is solution to this problem. It just provides means to treat the possible user candidates uniquely.

10.REFERENCES

[1] Agaron L, "Show me some ID - Biometrics is leaving its fingerprints on the market with low-cost devices", PC Week Online article, 12.1.1998 [referred 9.11.1998]<http://www.zdnet.com/pcweek/news/0112/12bio.html >

[2] Cuijpers E.P.E, A design for a safe internet communication channel with the help of smartcards, Master's thesis, Eindhoven University of Technology <http://www.iscit.surfnet.nl/team/Erik/masterth/masterth.htm>

[3] Daugman J, Recognizing persons by theirs iris patterns, University of Cambridge The Computer Laboratory.
< http://www.iriscan.com/basis.htm >