Identity Recognition in Network Security Using Laser Pumer Technology and Fingerprint

S. Meena[1], M. Madhura[2], S. Girja[3*]
[1]Assistant Professor, Master of Computer Applications, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India. Email: meenas.mca@mkce.ac.in
[2]Assistant Professor, Master of Computer Applications, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India. Email: madhuram.mca@mkce.ac.in
[3]Assistant Professor, Master of Computer Applications, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India. Email: girjas.mca@mkce.ac.in
*Corresponding Author

Abstract: This research work focuses on the cyber crime for the illegal activities which is potentially large. To save the information the Laser Pumer technology is used. By using this involves the scanning process more than one for various eye patterns and fingerprint, permission can be given for access after recognition and restrict the access from intruders. The sensor device reads the fingerprints at any angle and it does not require power supply. The USB Port capability makes it truly plug-and-play and makes an easy access.

Keywords: Cyber crime, Finger print, Laser pumer.

I. Introduction

Introduction of computer and usage of the systems dominating in all the areas like research, medical, analysis and information. Cyber crime is an offense and it is committed against individuals or group of individuals. This crime is classified as:

- Fraud and financial crimes
- Cyber terrorism
- Cyberextortion Cyberwarfare
- Computer viruses Denial of attacks Malware
- Phishing Scams Spam

Past technologies have used the passwords, Firewall to ensure the authentic entry and for security with total isolation / zero isolation. Sometimes unfortunately the right user requests may be rejected for some security reasons.

II. Need for Network Security

- Security is necessary as hackers are prone to attack any where…
- Netware present today is not hacker repellent.
- Secure data is a healthy data…
- Trojan and virus attack!

III. Categories of Cyber Crime

The computer crime is classified as two ways:

(1) Direct target of Computer networks.

(2) Indirect target which is simulated by computer networks independently.

IV. Problem Definition

A self supported security system based on entities can be introduced. This system performs the XOR operation in the affected data. The foreign entity is biotic consumes data with itself by copying that data into the buffer. The Lazer pumer technology has been introduced to safe the data from hackers in cyber security and it is an alternative solution to the cryptic passwords. The finger print of human being is also used as an additional security mechanism for safe guarding the system.

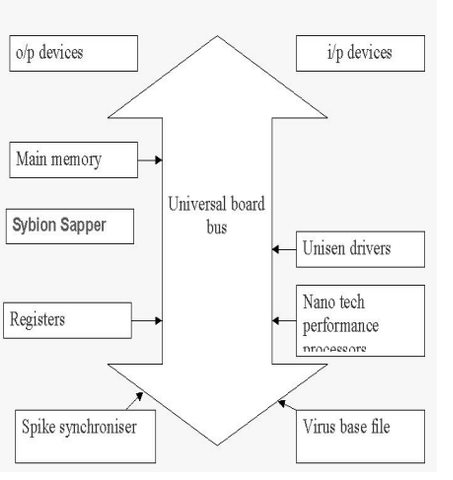

Fig. 1: Process Flow

V. Laser Pumer Technology

The Laser Pumer Technology is based on authenticating DNA testing. It is fast laser decoder. The basic genetic coding has two stands of which the ride side strand is not easy to decode. So pumer uses the left strand for analysis. The decoding is done is the user places is palm over the reader, which extracts sweat from which the strands are extracted by a super fast laser decomposer which disintegrates the given strands to its basic building blocks for analysis. This system is user friendly with touch boards and indeed there is no more a need to remember the cryptic passwords.

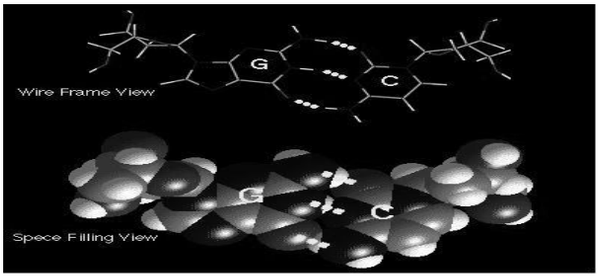

Fig. 2: Laser Pumer Technology - Break Pattern

VI. Finger Print Validation

The fingerprint reads any four fingerprints of the authenticated person in any angle. The Sensor reads the fingerprint patterns which is easy for the use. It doesn't require power supply. This system contains the USB port and makes it easier with capability. If the fingerprint is recognized the authorized person will get an access to all applications without password though it is strictly secured.

There are three basic groups of patterns in fingerprint, it contains the 'n' number of subgroups. The Loop is a pattern and it will be of 65% all Copies. The arch patterns are a more open curve than the loop. In this, Open Arch is the plain arch and another one is tented arch. Whorl is the pattern which occurs 30% of all fingerprints.

Loop: The loop is the largest part general kind of fingerprint pattern and accounts for about 65% of all copies.

Arch: The Arch model is an added open arch than the Loop. There are two kinds of arch models the Plain Arch and the Tented Arch.

Whorl: Whorl patterns occur in about 30% of all fingerprints and are defined by at least one ridge that makes a complete circle.

One Touch Log-In:

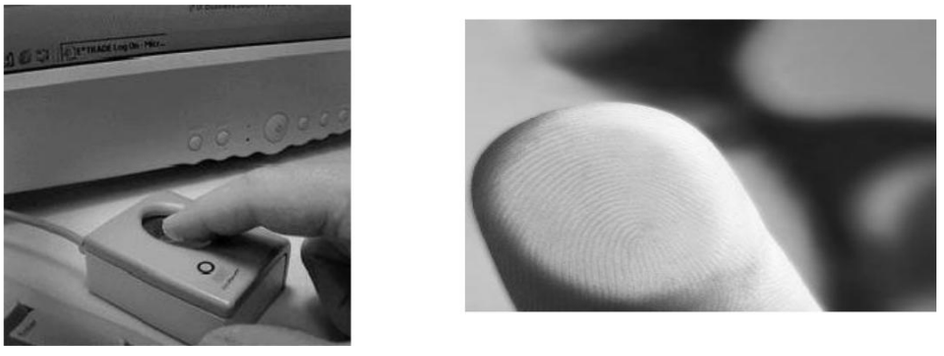

Fig. 3: One Touch Log-In

VII. Results and Discussion

This system used genetic coding an exclusive that the replication point of possibility is <0.03% which matches to a unfeasible occurrence. The eye and pulse extol validation repeatability of the same pattern of probability is below 0.42%. By combining the eye and finger which gives the accuracy 99.56% for best security.

VIII. The Future of Network Security

- The Network security crackers bounce back each time a fool proof system is employed!
- In the past over 1,300 systems have been tested of which only 13 remained crack resistant!
- We are sure that the future of the Network security is resting in the hands of LASER, the word that spells power as it is mumbled! There is a wide possibility that this might be leading to a new age that was so far seen in the fiction movies of Star wars only!
- The futuristic ideas under development in India are:
  - ✓ Laser protocol testing
  - ✓ Atomic authenticator
  - ✓ Password Brain

Laser technology is now under consideration to be replaced by the EM wave authenticator, which has much wider bandwidth so that more passwords can be accommodated for the storage unlike the hard disks, which occupy physical space and can be stolen!

IX. Conclusion

Dual scanning of the eye and fingerprint is safe and it is very complex to hackers and act as virtual firewall to secure the data. This might lead to a new research and avoiding the password remembrance and PIN Codes and smart cards. Fingerprints are safe and it reduces the chance of forgetting, losing.

References

[1] G. Aaron, K. A. Bostik, E. Chung, and R. Rusmussen, "Protecting the web: Phishing, malware, and other security threats," *Proceeding of the 17th International Conference on World Wide Web 2008, WWW'08*, Beijing, China, pp. 1253-1254, 2008.

[2] I. I. Amit, "The attack almanac," *Engineering and Technology*, vol. 4 , no. 1, pp. 68-69, 2009.

[3] Z. Anwar, M. Montanari, A. Gutierrez, and R. H. Campbell, "Budget constrained optimal security hardening of control networks for critical cyber-infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 1-2, pp. 13-25, 2009.

[4] Y. Ben-Itzhak, "Organised cybercrime and payment cards," *Card Technology Today*, vol. 21, no. 2, pp. 10-11, 2009.

[5] J. S. Bhatia, R. Sehgal, B. Bhushan, and H. Kaur, "Multilayer cyber attack detection through honeynet," *Proceedings of New Technologies, Mobility and Security Conference and Workshops, NTMS'08*, 5-7 November 2008.

[6] C. J. Blakeley, "Cybercrime law: International best practices," *Doha Information Security Conference*, Doha, Qatar, 10-11 June 2008.

[7] D. M. Downs, I. Ademaj, and A. M. Schuck, "Internet security: Who is leaving the 'virtual door' open and why?," *First Monday*, vol. 14, no. 1-5, 2009.

[8] D. Dwyer, "Chinese cyber-attack tools continue to evolve," *Network Security*, vol. 2009, no. 4, pp. 9-11, 2009.

[9] N. Gilman, "Hacking goes pro," *Engineering and Technology*, vol. 4, no. 3, pp. 26-29, 2009.

[10] A. Jenik, "Cyberwar in Estonia and the Middle East," *Network Security*, vol. 2009, no. 4, pp. 4-6, 2009.

[11] J.-S. Kim, D.-G. Kim, and B.-N. Noh, "A fuzzy logic based expert system as a network forensics," *Proceedings of the 2004 IEEE International Conference on Fuzzy Systems*, vol. 2, pp. 879-884, 25-29 July 2004.

[12] T. F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. Neumann, and C. Jalali, "IDES: A progress report," *Proceedings of the 6th Annual Computer Security Applications Conference*, 1990.

[13] S. F. Owens, and R. R. Levary, "An adaptive expert system approach for intrusion detection," *International Journal of Security and Networks*, vol. 1, no. 3-4, pp. 206-217, 2006.

[14] A. Peiravi, and M. J. Rahimzadeh, "A novel scalable and storage-efficient architecture for high speed exact string matching," *ETRI Journal*, vol. 31, no. 5, pp. 545-553, 2009.

[15] M. Qi, Y. Wang, and R. Xu, "Fighting cybercrime: Legislation in China," *International Journal of Electronic Security and Digital Forensics*, vol. 2, no. 2, pp. 219-227, 2009.

[16] G. Rasche, E. Allwein, M. Moore, and B. Abbott, "Model-based cyber security," *Proceedings of the 14th Annual IEEE International Conference and Workshops on the Engineering of Computer Based Systems*, *ECBS'07*, pp. 405-412, 26-29 March 2007.

[17] B. Rodrigues, "The cyber-crime threat to online transactions," *Network Security*, vol. 2009, no. 5, pp. 7-8, 2009.

[18] A. Yassir, and S. Nayak, "Cybercrime: A threat to network security," *International Journal of Computer Science and Network Security*, vol. 12, no. 2, February 2012.

[19] A. Peiravi, and M. Peiravi, "Internet security - cyber crime paradox," *Journal of American Science*, vol. 6, no. 1, pp. 15-24, 2010.

[20] S. Yadav, T. Shree, and Y. Arora, "Cyber crime and security," *International Journal of Scientific and Engineering Research*, vol. 4, no. 8, pp. 856-861, August 2013.

[21] R. Moore, *Cybercrime: Investigating High-Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing, 2005.

[22] S. W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, ABC-CLIO, 2010.