Reducing Cyber Threats: via a Multimodal Biometric System

Aparna Narayanan, Gunjan Chhabra

***Abstract*—This era of Information Technology and Computing has provided us with various emerging trends in every field of our life. One of its blessings is in the field of cyber world which allows easy communication and transfer of information and data.**

As cyber demands increases, related issues also come under play like hacking, cyber wars, etc. As the communicated data is very crucial, everyone tries to keep it secure or transfer it securely. Some security techniques use human body characteristics known as biometrics. In this paper we have tried to highlight the various methods of reducing cyber threats by using the emerging technology of biometric systems. We have further described its classification and usage as a multimodal biometric system for a secure cyber world.

***Keywords*—Cyber Security, Biometric, Multimodal System, Heart beat pattern.**

I. Introduction

A. *Cyber Security*

Everything in today's world relies on the computer and internet, be it communication, entertainment, transportation, or even shopping and the list goes on. The advent of computers has made an individual store all their personal and professional information in its digital form, which is accessible from anywhere through the internet.

With the increased use of internet, people have found various ways to commit crimes. The internet has become a whole new world on its own- **the cyber world**. The crimes committed in this cyber world are being termed as cyber-crimes, which range from identity theft to fraud, phishing to hacking.

With a marked increase in cyber-crimes there arose a need to secure the internet, so that only the correct party can access the information. From this emerged the area of Cyber Security, which involves protecting information by preventing, detecting and responding to attacks.

Cyber security is the body of processes, technology and practices which are designed to protect networks, computing devices (computers and hand held devices), programs and data from damage, attack or unauthorized access.

The most important aim of any kind of security system is preventing the attack. If the attack is prevented there would be no need for detection or responding to these attacks.

There are various modes of prevention:

- Keep your software up to date.
- Use of strong passwords.
- Encryption.
- Use of antivirus.
- Use of firewall.

With regards to cyber security one of the key areas is identification or authorization. If there is an error in this area, then the information can fall into wrong hands, leading to catastrophic results.

B. *Cyber Security: Enterprise architecture and risk assessment*

Enterprise architecture is a discipline which has gained interest in industry and academia both. It pays attention to the fact that effective management of business and IT needs to take a holistic view of the enterprise. With regards to cyber security, the security analysis framework can be adapted to architectural languages so as to get a holistic view.

Enterprise architecture can be used to develop abstract models built from attack and defense tree, relevant for control systems, which will help the decision maker to make an informed decision, even on limited knowledge about the cyber security management. This is described in detail in [7].

There is also a need to assess the risks related to the cyber network. This can be done by using Bayesian defense graphs as described in detail in [5].

The cyber security needs to be strengthened so as to reduce the possibility of any kind of attack. In the subsequent sections a method for identification or authentication has been described as an alternative to the current method of using a strong password and a security question.

Aparna Narayanan
University of Petroleum and Energy Studies, India
appunara@gmail.com

Gunjan Chhabra
University of Petroleum and Energy Studies, India
g_chhabra@yahoo.com

II. Biometrics

Biometrics or biometric authentication refers to the identification of humans by their specific characteristics or traits. Biometrics can be used for access control and identification purposes.

The biometric identifiers need to be distinctive and measurable characteristics of human beings. The more unique these identifiers are to an individual the more reliable the system can be as compared to the traditional methods of using passwords or smart cards.

Biometrics is widely used for verification, identification and authentication of humans. But still various errors have been encountered during the performance of the biometric systems currently in use. The false match rate and the false non-match rate are quite high in the matching of various biometric characteristics. Any human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- ***Universality***: each person should have this characteristic.
- ***Distinctiveness***: any two people should be sufficiently different in terms of this characteristic.
- ***Permanence***: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
- ***Collectability***: the characteristic can be measured quantitatively. [6]

However, in a practical biometric system, there are a number of other issues that should be considered, including:

- ***Performance****:* refers to the achievable recognition accuracy and speed.
- ***Acceptability***: refers to the extent to which people are willing to accept the use of a particular biometric identifier in their daily lives.
- ***Circumvention***: refers to how easily the system can be fooled using fraudulent methods.[6]

The various biometric traits which can be used as identifiers are listed out in Table I. The biometric traits listed out in Table I can be divided into two basic categories:

- **Soft Biometric**: These are the ones which are bound to change as time passes. The soft biometric characteristics are gait, voice, handwriting, etc.
- **Hard Biometric**: These are the ones which are permanent and time has no or very less effect on them. The hard biometric characteristics are Iris, fingerprint, palm print, heartbeat patterns, etc.

There are many such human characteristics which can be used as a biometric. Only a few of these traits have been explored yet. There may be many other unidentified traits which could turn out to be better identifiers than the ones currently being explored.

TABLE I.

BIOMETRIC TRAIT	DESCRIPTION
Keystroke	Uses the typing rhythm of a person
Gait	Identifies the way a person walks
Voice	Distinguishes a person based on their voice patterns
Handwriting	Recognizes a person based on their handwriting pattern
Finger prints	Identifies based on individual fingerprints
Hand geometry	Utilizes the structure measurements of a human hand
Lips	Identifies using the movement of lips
Ear	Classifies based on the inner and outer structure of one's ear
Face	Recognises using the facial structure of a person
Retina	Uses retinal scans for identifying an individual
Iris	Iris scan is used for individual identification
DNA	The DNA structure is matched for individual verification
Brain patterns	Brain wave patterns are matched for identification
Heart patterns	Heart beat sound patterns are utilized for determining one's identity
Hand vein patterns	Hand vein patterns are used for recognition

The soft biometrics like gait, voice, handwriting and keystrokes keep changing making its usage for biometric authentication less reliable.

Table II describes to what level each biometric satisfies the aforementioned requirements. The symbols H, M and L indicate high, medium and low respectively.

TABLE II.

Biometrics Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial Thermogram	H	H	L	H	M	H	L
Fingerprint	**M**	**H**	**H**	**M**	**H**	**M**	M
Gait	M	L	L	H	L	H	M
Hand Geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	**H**	**H**	**H**	**M**	**H**	**L**	**L**
Keystroke	L	L	L	M	L	M	M
Odour	H	H	H	L	L	M	L
Palm print	**M**	**H**	**H**	**M**	**H**	**L**	**L**
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H
Heartbeat	**H**	**M**	**L**	**L**	**L**	**M**	**L**

HAND PRINT

A. *Examples of uses of Biometrics*

Biometrics has been used in combination with various cyber techniques to increase the security level. The use of biometrics is varied, ranging from entry control to ATM's; from law enforcement agencies to various government programs. A few examples are given below.

1) Generate a key for AES using biometric for VoIP network security

VoIP- Voice over Internet Protocol is much in use in today's world where private phone conversations are being conducted over the internet or public networks. Due to the increased use of VoIP over the cyber network, there is an increase in the security concerns regarding VoIP. One method to keep VoIP secure is encryption. But data encryption has become vulnerable to hijacking, man in the middle attack, spoofing or identity theft. So to overcome this problem, a Biometric-Crypto system has been suggested. The Biometric-Crypto system generates a cryptographic key from the fingerprints for encryption or decryption of VoIP and uses the Advanced Encryption Standard (AES) method. The use of a biometric trait along with the commonly used encryption system decreases the possibility of an attack over the cyber network. [3]

2) Biometrics for computer security and cryptography

Biometric traits have become a popular method for solving various security issues which are cropping up in the cyber world. Their uniqueness for a person makes the use of these traits for identification system or access control more secure. A brief explanation of biometric cryptography approaches and algorithm which use various biometric data is given in [4]. The use of biometric characteristics like fingerprint, voice and keystroke dynamics as biometric cryptographic keys as opposed to user based cryptographic keys are discussed in detail in [4].

3) Biometric authentication in smart grid

The Smart Grid aims at bringing modern IT network into the industrial control system (ICS) network to more effectively generate, transmit, and distribute electricity. These networks contain their own vulnerabilities and connecting them with IT network would not only increase its complexity but also create more vulnerabilities. Due to this there is a need to defend this network against cyber-crimes. Biometrics can be used for authentication to improve the security of the smart grid. Privacy enhanced methods that apply fingerprints for user authentication protects the biometric data, making it possible to include biometrics as a factor in the desired multifactor user authentication for the Smart Grid. [2]

4) Biometric technology stomps identity theft

However, with the rise of identity theft, it has become more difficult to prevent unauthorized access to information resources and installations. Methods of positively verifying and authenticating people may mitigate the current identity theft crisis. Biometric technologies may be the answer. Because of recent advances in computer science, biometric technology products (BTPs) have become more reliable and less expensive to own. With a BTP--such as an iris analyser--a living person's identity can be positively authenticated and verified, making it difficult for imposters to access resources by stealing someone else's identity. The benefits of implementing a biometric technology product—one more tool for safeguarding the information assets and key installations of an organization—are numerous. Various privacy issues are associated with the deployment of a biometric technology product, the details of which are available in [1].

B. *Problems faced by biometric systems*

While providing an excellent solution to the problem of authentication, these biometric systems also face quite a few problems of their own. Some of them have been stated below.

- Presence of noise in the sensed data.
- Matching failure due to incorrect interaction of human with sensor during data capturing.
- Spoof-attack i.e. sometimes an individual's voice and signature can be easily copied. Such an attack can't be detected by a biometric system easily.
- Fingerprinting and face recognition may produce an error due to cuts and age passage.

From Table II it can be inferred that there is no one such biometric which satisfies all the requirements to solve the problems being faced by cyber security.

III. Multimodal Biometrics

It is thus clear that the hybrid use of biometric characteristics and integrated biometric systems have better performance and provides better valid authentication of an individual. This manner of combining two or more biometrics for authentication is known as multimodal biometrics.

After the analysis of Table II, **hand print (finger and palm print together), Iris and heart patterns** have been selected to be used in a multimodal biometric system. All these three complement each other, in effect creating a better security system than available before. A block diagram to this effect is shown in Figure 1. Figure 1 depicts the control flow of this multimodal biometric system. The selected traits have been highlighted in Table II. Heartbeat patterns, Iris, and hand print (finger print and palm print together) have their own set of features which can be extracted and used for identification or authentication.

- Heart beat patterns are unique to each individual and cannot be copied, stored or reproduced thus making it impossible to clone and circumvent it. Also after experimentation by various researchers, it has been found that heart beat sound can be used as a new biometric with an accuracy of 85%.

This is an asset to multimodal biometrics and a lot of work still needs to be done in this area. [9] [10] [11] [12] [13]

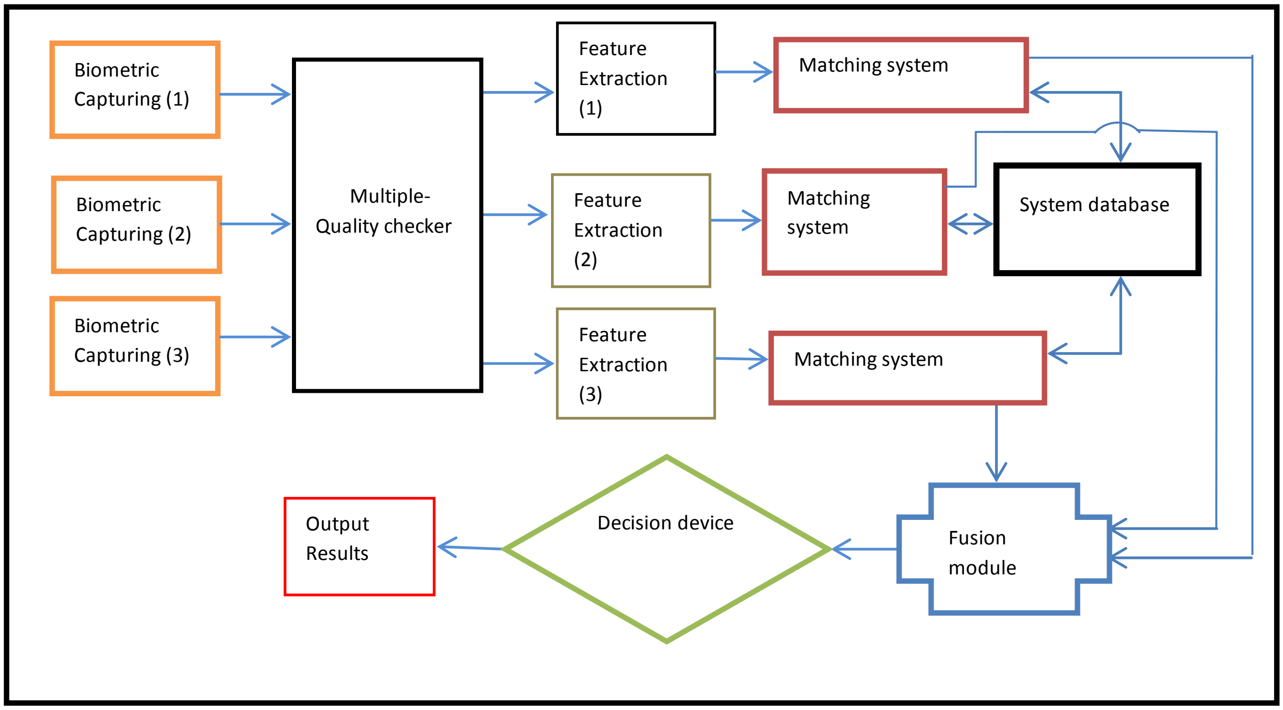

Figure 1. Multimodal Biometric Authentication (Block Diagram)

- The image patterns for iris are different for all individuals allowing for easy capture and cannot be reproduced. The human iris is rich in features that can be used to quantitatively distinguish one eye from another. The iris contains many collagen fibers, contraction furrows, coronas, crypts, color, serpentine vasculature, striation, freckles, rifts and pits. Measuring the patterns of these features and their spatial relationship to each other provides other quantifiable parameters for the identification process.
- The combination of fingerprints and palm prints increases the security by 20% as opposed to when each is used individually. The minutiae and the ridges (whorl, arch and loop) are used as features for fingerprint recognition. While ridge flow, ridge characteristics and ridge structure of the raised portion of the epidermis are used as features in palm print authentication.

Multimodal biometrics can be used as shown in Figure 1. Here biometric 1, 2 and 3 refer to hand print, iris and heart beat patterns. The combination of these three could provide a better access control system to be used in cyber security than currently used systems.

IV. Biometrics and Cyber Security Standards

Biometrics plays an important role in the field of security in IT era, where protection of data is very crucial. In cyber world, the network must have knowledge of who is trying to access a system and data, and the protection of the same. Due to a strong binding between the biometric trait and the person to whom it belongs, biometrics has emerged as a strong option for access control in cyber security.

The ISO has developed several standards that support the use of biometrics in the cyber security environment. The two major areas of interest regarding biometrics and cyber security are:

- Use of biometrics as a security mechanism.
- Protection of biometric data within a system.

Confidence in the identity of user before providing him with access is of higher importance in open networks than in closed ones. As biometrics are not secrets its integrity and authenticity is of higher importance.

A few of the ISO standards regarding the use of Biometrics in cyber security are listed below, the details of which can be found in [8].

- ISO/IEC JTC 1 SC 37.
- ISO/IEC JTC 1 SC 27.
- ISO TC 68.

V. Conclusion

After a brief study of the cyber world and the issues concerning them, it is discerned that biometrics can play a vital role in cyber security. Each biometric characteristic has its own advantages and vulnerabilities. It makes one think how to combine one biometric with another to overcome these vulnerabilities. The hybrid biometric systems are less prone to circumvention than systems which utilize a single biometric for authentication/verification.

On comparison of various biometric traits it can be concluded that the combination of heart beat patterns, iris and hand print could provide a better security system for the cyber world than the systems currently in use. There is still a lot of work needed to be done to bring this proposal to fruition.

References

[1] Seyoum "Zeg" Zegiorgis;, "Biometric Technology Stomps Identity Theft," *SANS Institute 2002.*

[2] Quinghai Gao;, "Biometric authentication is Smart Grid," Energy *and Sustainability Conference (IESC), 2012 International*, vol., no., pp.1-5, 22-23 March 2012 doi: 10.1109/IESC.2012.6217197.

[3] Arul P, Shanmugam A;, "Generate a key for AES using biometric for VOIP network security," *J Theoretical Appl Inf Technol* 2009, 107–112.

[4] Alper Kanak;, "Biometrics For Computer Security And Cryptography," June 3rd, 2004.

[5] Teodor Sommestad, Mathias Ekstedt, Pontus Johnson;, "A probabilistic relational model for security risk analysis," Computers & Security, Volume 29, Issue 6, September 2010, Pages 659-679, ISSN 0167-4048, 10.1016/j.cose.2010.02.002.

[6] Jain, A.K.; Ross, A.; Prabhakar, S.; , "An introduction to biometric recognition," *Circuits and Systems for Video Technology, IEEE Transactions on* , vol.14, no.1, pp. 4- 20, Jan. 2004 doi: 10.1109/TCSVT.2003.818349.

[7] Ekstedt, M.; Sommestad;, T.; , "Enterprise architecture models for cyber security analysis," *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, vol., no., pp.1-6, 15-18 March 2009 doi: 0.1109/PSCE.2009.4840267.

[8] Tilton, Catherine;, "Biometric, Cybersecurity and Enabling Standards."

[9] K. Phua, T. H. Dat, J. Chen., and L. Shue;, "Human identification using heart sound," in Second International Workshop on Multimodal User Authentication, May 11-12 2006.

[10] F. Safara, S. Doraisamy, A. Azman, and A. Jantan;, "Heart sounds clustering using a combination of temporal, spectral and geometric 8 features," Computing in Cardiology, vol. 39, pp. 217–220, 2012.

[11] Beritelli F, Spadaccini A;, "Human Identity Verification Based on Heart Sounds: Recent Advances and Future Directions", University of Catania, Italy 2010, pp.1–18.

[12] S. Fatemian, F. Agrafioti, and D. Hatzinakos;, "Heartid: Cardiac biometric recognition," In Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, pages 1 –5, 2010.

[13] Spadaccini, A.; Beritelli, F.;, "Performance Evaluation of Heart Sounds Biometric Systems on An Open Dataset".