International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

A Review of Cyber Security Using Biometric Devices

Ashwini Satkar[1] *Asst. Prof. Dept. of Comp Sci. Dr. D. Y. Patil ACS College, Pimpri, Pune. Maharashtra, India*

Ashwini Patil[2] *Asst. Prof. Dept. of Comp Sci. Dr. D. Y. Patil ACS College, Pimpri, Pune. Maharashtra, India*

Rohini Bhoware[3] *Asst. Prof. Dept. of Comp Sci. Dr. D. Y. Patil SCS College, Akurdi, Pune. Maharashtra, India*

Kalyani Shinde[4] *Asst. Prof. Dept. of Comp Sci. Dr. D. Y. Patil ACS College, Pimpri, Pune. Maharashtra, India*

Abstract - *Biometric security identifies human's body elements or biological data to verify person's identity. Using this technique we can identify a person. It is a method used to identify person using his biometric features and provide access to different applications, accounts, systems, facility etc. This paper focuses what is need of biometric authentication, different biometric devices, their advantages and disadvantages in detail.*

***Key Words*: Biometrics, Security, Benefits, Problems with biometrics.**

1. INTRODUCTION

Person can be can authenticate and identified by different ways. Government issued documents such as Aadhar card, driving license, PAN card, voting card are few examples of such documents. The main concept behind this authentication method is having something unique which nobody has. Unique identification number is assigned to all these documents which is known to us and cannot be re-produced.

As we started moving towards digital world, we started using passwords, smart cards, access cards but the main concept behind implementing it remains same. Possess something unique which nobody has.
As we made progress in technology creating duplicate documents became piece of cake. One can easily scan these documents, make digital copy of it and edit it as per requirement. Due to advancement in printing technology, one can easily re-create these documents and forge your identity. So basically, idea of having something unique has been compromised which put great risk for authentication mechanism.

Biometric security has further broadened the concept of possessing something unique which cannot be easily reproduced. This identification method use human body characteristics to authenticate and identify a person. Human body characteristics such as Fingerprint, Eye retina, hand patterns, facial recognition never change for a person during his lifetime. Also, it's difficult to reproduce them. This enhances the security in authentication mechanism.

In case of Biometric security, person's body characteristics are stored in system. When that person tries to access the facility, he/she must provide that body characteristic in order to gain access. For example: fingerprint reading machine has been implemented to provide access to secured facility. If someone must access it, he must be authorized to use that facility by registering at security desk. In order to enter the facility, he should use fingerprints and validate himself

2. Benefits of Biometric Devices:

- Its fast and user friendly – don't require efforts to remember different passwords
- Secure than traditional methods, since biometrics are difficult to reproduce
- Once added, no need to change anything at fixed intervals as in case of passwords
- Simple to store and takes less memory space to store
- Chances of having 2 persons same fingerprint or eye retina is almost impossible
- Biometrics are non-transferrable which makes them secure and misuse can be completely avoided.

Nothing can be perfect in this world and so does the biometrics. They are certainly better than traditional mechanism but it also has its own issues.

3. Problems with Biometric Devices:

Problem 1: Privacy issue

A password which we use is not stored anywhere, its memorized which makes it very difficult to guess someone what password is. We feel safe when our password is strong. Hacker can access it by phishing and other mechanism but still it's safe.

Consider an example of fingerprint or facial recognition. Whatever we touch has our fingerprints on it. Which can be easily copied and forged? Similar case with face. It's visible to everyone. Anyone can misuse it. Meaning the entire biometric trait we possess are accessible to everyone around us.

Problem 2: Biometrics can also be hacked

If someone has our picture, they can easily recreate our face. Facial recognition system can be fooled by using face mask or duplicate face. With CCTV & high definition cameras everywhere its also easy to get our retina scan and reproduce it.

Problem 3: Extra security needed

Due to the limitations of biometric one cannot completely rely on biometrics. We still need second layer of security. Hence passwords along with biometrics are implemented to enhance the security of systems.

Problem 4: Initial implementation cost.

Older authentication such as password doesn't require any additional equipment's to be setup. Biometric require additional equipment's such as retina scanner, fingerprint reader which has high cost.

4. CONCLUSION

Advantages and disadvantages are there with every system therefore before implementing any technology**;** we need to review the use case. There is no one size fits all approach in security systems. If someone wants to mark attendance and record IN-OUT time of employee, **it's** always beneficial to go for fingerprint scanner. It's fast, reliable and hard to forge someone's attendance. For more secure banking related applications – it's better to have passwords, along with fingerprint scanners for additional security. This second layer security makes it harder for hackers to hack into bank accounts and avoid fraud transactions. Due to advancement of technology, biometric devices are becoming cheaper. Its also difficult to fool them by using photo or fingerprint pattern.

REFERENCES

[1] https://www.techopedia.com/definition/6203/biometric-security

[2] https://www.bayometric.com/advantages-disadvantages-biometric-identification/

[3] https://blog.ipswitch.com/3-reasons-biometrics-are-not-secure

[4] https://www.securitycommunity.tcs.com/infosecsoapbox/articles/2017/01/05/15-important-pros-and-cons-biometric-authentication

[5] http://www.m2sys.com/blog/biometric-hardware/top-ten-mind-blowing-advantages-of-biometric-technology/

[6] https://dl.packetstormsecurity.net/papers/general/Handling_Problems_in_Biometrics.pdf

[7] https://www.ifsecglobal.com/cyber-security/4-drawbacks-of-biometric-authentication/

[8] https://biometrictoday.com/10-advantages-disadvantages-biometrics-technology/