International Journal of Computer Architecture and Mobility (ISSN 2319-9229)
Volume 7 -Issue 6, June 2019

Biometric In Cyber Security

HarshWardhan Singh Khichi
Computer Science , SVIIT ,
SVVV, Indore , India
(Email : harshkhichi1098@gmail.com)

Abstract

Due to the Internet revolution in the last decade, each and every work area of society are directly or indirectly depending on computers, highly integrated computer networks an communication systems, electronic data storage and hig transfer based devices,commerce, security,governance, and e-business. The Internet revolution is also emerged as significant challenge due to the threats of hacking systems and individual accounts, malware, fraud and vulnerabilities of system and networks,etc. In this context, this paper explores E-Security in terms of challenges and measurements. Biometric recognition is also investigated as a key e-security solution.Security is precisely described to understand the concept and requirements. The major challenges of e-security;namely, threats, attacks, vulnerabilities are presented in detail. Some measurement are identified and discussed for the challenges. Biometric recognition is discussed in detail wit pros and cons of the approach as a key e-security solution. This investigation helps in clear understating of e-security challenges and possible implementation of the measurements for the challenges in wide area of network communications.

1 Introduction

Information Technology has become one of the prominent support structure for any organization in this modern era.The primary goal of the technology is to provide efficient and secure flow of information flow in the organization.The present age is running on the wheels of information technology, computational devices and other value added services. Security of data has become increasingly important in any organization, and thus; organizations are working hard in their information security systems for implementing the effective and recent security approach and risk management techniques. Information security system always considers information a critical component of the organization. Protection and security of information has evolved due to unauthorized and non-authenticated changes in information of any organization.

2 Cyber-Security

In this section, E--security is precisely explored. E-security stands for \cyber-security", \Internet-security" as well as \IT-security".

1) E-security or electronic information security means protection of important data and information from undefined and unauthorized disclosure, transfer, modification and deletion of the information.

2) It is concerned with the security of any data that passes over the e-network in electronic form.

3) It mainly deals in securing both information as well as the network(s) through which information flows.

4) E-security is protecting an organization from internal as well as external threats and attacks.

5) It protects information networks and communication networks from the unauthorized use of the information
.
6) E-security also secures the intranet, extranet from the outside world. Due to the wide spread range, vast and continuously changing nature of communication network and environment, solutions derived e-security should be exible, adaptable and able to detect and provide solutions to different security threats. The solutions should fulfil the requirements of the organization that are based on thee-network and information based systems.

3 Challenges for E-Security

In this section, various challenges in the design of e-security solutions are discussed. There are various challenges for e-security and various measures do exist to overcome these challenges. In spite of these measures the challenges prevail in the form of newer vulnerabilities, threats and attacks. The security challenges are of many types and manifolds and each with dire consequences if it is no addressed properly. E-security provides open and easy communications as well as secure communication through the internet and electronic media. E-Security is a continuous process by which confidential and proprietary data and information are secured from the unauthorized and non-authenticated access from outside world in the network. Some Challenges for E-Security are listed be-follow.

1) Protect the inadequate knowledge, data, information and tools of companies and also provides the security to internal resources and network.

2) To enable the secured exchange of confidential information, by keeping unscrupulous elements out and by providing the necessary hidden policies and methods.

3) To enable controlled access to IT network and their process, consistent with defined roles and responsibilities.

4) Make-up secure, effective, effecient, robust and trusted network for important and sensitive areas.

5) Avoid attack, fraud within business processes and transaction, and also detect the affected area also release the respond to attempted attack and fraud within the network.

6) Non-availability of e-security information knowledge is great challenges for e-security.

7) Confirm that each component of the e-world or network infrastructure is accessible when needed and also develop the verification of the transaction at the time of resource sharing.

8) To maintain trust and secure platform for transaction and processing in e-network and controlled access to computer systems and their processes, consistent with defined job and responsibilities. Iterating all possible security factors and challenges are virtually impossible, we therefore categorized these e-security challenges in three main factors: threats, attacks and vulnerabilities. All three main factors threats, attacks and vulnerabilities are discussed in detail in the next sections.

E-Security Measurement And Biometric Recognition

In this section, common e-security measures have been identified and bio-metric recognition is discussed as keys security solution.

E-Security Measurement

Effective e-security policy must consist of the objectives; namely, confidentiality, integrity, availability, legitimate use (identification, authentication, and authorization), auditing or traceability and non-repudiation. Common e-security measures are listed below.

1) Authentication: A digital certificate that approve authentication during the use of any

individual's unique signing key. Basically, authentication mechanisms [that existed today use one or more of the authenticators (factors) viz. Knowledge-based, Possession-based and Physiology-based. Knowledge-
based is an authenticator only the individual knows, which typically denotes to PIN, pass phrase or a response to a secret security question. In the possession-based is an authenticator only the individual possesses, which usually refers to keys, smart cards and tokens. Physiology-based is an authenticator only the individual is or can do, referring to biometrics. Knowledge and possession-based authentication mechanisms imply that users in order to be granted access to a system, building, service – need to carry or remember the authenticator.

2) Access Controls: This limits unlike classes of users to subsets of information and make sure that they only access authorized data and services. Network constraints to safe access of other computer systems and network.

3) Encryption Policy: By this policy original data
should be changed in the cipher data form for security point of view.

4) Intrusion Detection: These product monitor system and network activity to spot any attempt being made to gain access.

Biometric Recognition: As a Key Cyber security Security Solution

Biometric Recognition is the statistical analysis and measurement of folks' physical and interactive characteristics The technique is primarily used for identification, access control and identifying individuals that are under surveillance. The basic evidence of biometric authentication is that each person is unique. She can be identfied by her intrinsic physical or behavioral traits. The term"biometric" is consequent from the Greek words "bio"means life and "metric" means to measure. Information security is an unlimited concern to electronic users, which is not only a technical challenge, but also related to human factors. For example one of the key issues in Malaysia related to Internet banking is the pathetic security used for Internet banking application. Hence it is an important study to investigate further the solution and enhance the security issues in Internet banking applications. Modern world is fast world, billions of transactions occur each minute. On behalf of these transactions, data prerequisite to be readily available for the unpretentious.

Biometric Recognition is normally considered as physiological or behavioral characteristic based recognition .

Physiological characteristic represents to stable characteristics of human beings including fingerprints, structure of face, eyes, ears, hands, legs, and fingers, the pattern of hairs, teeth, and samples of DNA structure. Physiological characteristics of each individual are normally
permanent and distinctive. It changes only due to fatal accidents, serious illnesses, genetically induced defects, or in some cases changes due to aging. Behavioral characteristics are represented by the day-to-day way of living life by the particular human being. Interactions with other human beings are also include to measure the behavioral characteristics. Biometric recognition can be utilized as a key e-security solution. Biometric recognition generally works in five steps. The steps and the actions needs to be executed in the corresponding steps are listed below.

1) Sample acquisition: Collection of biometric data using appropriate sensors.

2) Feature extraction: Conversion of biometric data into templates.

3) Storage: Storage of templates in appropriate memory which depends on the application.

4) Matching: authentication of user by comparing bio metric template of the user with the existing templates stored in the database.

5) Decision: Based on the result of the matching, the user will be authorized or denied to access the resources.

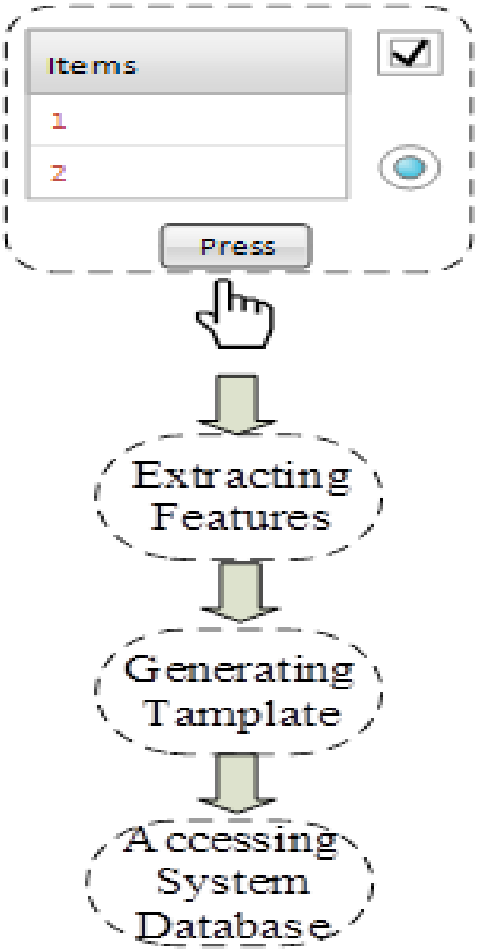

Figure 1: Enrollment in biometric recognition

Problems to Biometric Security

There are various threats to the biometric methods used and are also threats to the biometric data

1. Theft of Biometric Data: The most important threat to Biometric method is to secure the Biometric data stored or how to securely the biometric data from different Hackers and attackers.
2. Physical Factors:
The second challenge to the biometreic method is to implement the Biometric method on various different platform i.e to implement the Biometric method via using different tools to implement the biometruic method for example in to implement the eye we need various eye equipments to implement the Biomentric method or to gain the data for the authentication process.
3. Environmental Factors:
The third important challenge to implements the Biometric method is Environmental Factors: The working of Biometric devices may be adversely affected by the environmental conditions. For voice recognition, the surroundings must be noise-free. Humidity and temperature might also play a part. Sufficient amount of light is to be present while scanning the face, iris, and retina If the threshold of the device is decreased to make it work in these kind of conditions, security might be breached.
4. Ease of Use: This problem is closely related to the public acceptance of Biometric devices as security systems. One advantage of Biometrics is that a person need not remember or carry anything with him/her. But, user acceptance can only be obtained if the Biometric devices are convenient to use and operate. This convenience should not be provided at the cost of security . An administrator 10 must know the functionality of a Biometric Device.

SOLUTIONS

Educating Public about Biometrics

Solves Public Acceptance and Ease of Use problem: With the introduction of any new technology, user participation and acceptance is

essential. Educating the public about Biometrics will help greatly to solve many problems and help in the growth of this industry. The society's misconceptions about the security, privacy and working of the technology can be eradicated through providing adequate education regarding the technology. Education definitely improves public confidence and acceptance of Biometrics. People shouldn't feel that there are too many unanswered questions in using Biometrics . People are understanding the wide use of technology and can introduce certain risks to individual privacy. So, the business organizations should understand this and introduce policies and develop some assurance models of privacy protection for their customers. This raises the need for understanding Biometrics from both the individual's and organization's perspective An informed public-policy debate about Biometrics is necessary. Clear discussions about the capabilities and limitations of every Biometric system should be made.

Ensuring Cleanliness before using a Biometric Device – Mitigates Environmental Factors:

People should be educated about the conditions in which a Biometric device can be used. An instructor should be present at the location where the scanning is being done and should ensure trouble free scanning. In the jobs involving usage of chemicals, construction work, or mechanical works, a person's hand will be smeared with dirt or grease. He should clean his hands before fingerprint or hand scanning. Notices and instructions can be put in an obviously visible position so that the user can go through them before moving forward for scanning.

Encryption, Centralization, Multimodal Biometrics and Revising Algorithms – Solves the Problem of Theft:

The fact that a Biometric cannot be changed makes the theft of Biometric data a problem of top priority. Certain algorithms are used by organizations to convert the Biometric into a Binary file which is stored in a database. There should be people supervising and safeguarding the Biometric Devices and databases. These databases should be placed in inaccessible locations. Even if an attacker has the data, the corresponding Biometric cannot be regenerated with this data unless the algorithm is known. Once the attacker gets the algorithm used for conversion, he can make use of the stolen information. So, one way of protecting the stolen data is to use complex algorithms which are difficult to crack. It's also a good practice to change these algorithms at random intervals. Another way is to encrypt the saved data so that it'll be impossible for the hacker to decrypt and use it. Instead of saving the Biometric information as binary data, it can be hashed using any hashing algorithm and then saved as a reference string.. These systems demand the user to submit more than one random Biometrics for authentication. This is similar to two factor authentication. So, the attacker should have all the Biometrics of a user in order to gain access. One more solution is to centralize all the Biometric data which is mentioned in the previous section. Each organization has to invest a lot of capital to store the data and to secure it. Instead of maintaining separating databases, all the organizations can store the Biometric data in a single safe location. This location can be provided with the highest level of security. These organizations can be divided into groups and access to data can be provided based on these groups.

CONCLUSION

Biometric technologies are widely used in the public sector and the private organizations are yet to adopt it in large scale. With the problems faced in password based and token based security systems, Biometrics is definitely the future of security. But the Biometric system of the present day is still immature. Even though Biometrics is the principal method for physical

security, research is still being done. It is being combined with other branches of security (e.g. Biocryptics) and a huge amount of money is being put in this field by the government. A lot of questions are to be answered for the technology to be universally existent. In this paper, I have tried to address some of the issues faced in this field. The factors responsible for these issues are analyzed to come up with the solutions. Though the solutions provided are not completely feasible and may depend greatly upon the application and organization, it can be a start for finding more concrete methods to overcome the problems. Advanced research is needed to improve the existing technologies and also invent new methods.

Acknowledgments

The research is supported by Mr . Romil Rawat Assistant Professor SVIIT, SVVV and conducted by Harsh Wardhan Singh Khichi (1601DMBCS00944). The support by Mr . Romil Rawat is gratefully helpful and precious and without that support the research would might not complete in time .I would also like to thank for their anonymous and valuable time to support the research.

REFERENCES

[1]https://www.academia.edu/Documents/in/Biometric Security

[2]https://dl.packagestromsecurity.net/papers/general/Handling problems in biometrics

[3]Other Internet websites eg Wikipedia, GreeksforGreeks etc.

Harsh Wardhan Singh Khichi has done his 10 and 12 from Shri Gujarati Samaj A.M.N English Medium School, Indore 2014 and 2016 respectively He is Currently pursing his B.Tech from Shri Vaishnav Vidhiyapeeth Vishwavidiyalya, Indore in Computer Science (2016-2020) and is currently in 4th year. His is doing his research work for the last ½ month and currently doing his research further to evalualte some advantages nd disadvantages of Biometric used in Cyber Security and how to Secure the Cyber world from attackers and hackers.