INTERNATIONAL JOURNAL · ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

xx

IJIEMR Transactions, online available on 31th May 2024. Link
https://www.ijiemr.org/downloads/Volume-13/ISSUE-5

10.48047/IJIEMR/V13/ISSUE 05/61

TITLE: ROLE OF BIOMETRICS SYSTEM FOR CYBERSECURITY SURVEILLANCE

Volume 13, ISSUE 05, Pages: 558-562

Paper Authors Sakshi Dubey, Dr. Rishi Kumar Sharma, Bhanu Partap, Deepak Saini

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

ROLE OF BIOMETRICS SYSTEM FOR CYBERSECURITY SURVEILLANCE

Sakshi Dubey, Dr. Rishi Kumar Sharma, Bhanu Partap, Deepak Saini
Research Scholar (M.Tech CSE)Quantum University Roorkee(UK), India sakshidubey2511@gmail.com
Associate Professor (CSE) Quantum University Roorkee(UK), India rishi.rishi1526@gmail.com
Assistant professor(CSE)Quantum University Roorkee(UK), India bhanu8909@gmail.com
Research Scholar (M.Tech CSE)Quantum University Roorkee(UK), India sainideepak1323@gmail.com

***Abstract*—As digital data become more prevalent, person tryto secure their data with using highly encrypted passwords and authentication identities. But the security measures like this are still misused and stolen. Hackers take advantages of security flaws in authentication identities which ends up in cards being duplicated and counterfeited due to which they get misused. We will analyse cyber security surveillance by using biometrics security system. The security criteria and notations are well explained in this paper. Threats, assaults and vulnerabilities are three main e-security obstacles which are discussed in depth. This increasing challenge in front of cyber security give rise to biometrics. The Internet revolution becomes a serious issue because of the risks of hacking systems and individual accounts, malware, fraud and vulnerabilities in systems and networks. This study examine the problems and evaluations of e-security in this environment. In this work we are present the new problem area of Biometrics Cyber Security Surveillance system.**

***Index Terms*— intrusions, approaches, authentication, cyber attacks, behavioral traits, threats, artificial mold, security risks, tiers, assaults**

I. INTRODUCTION

In the dynamic landscape of cybersecurity, the arrival of biometric systems has emerged as a transformative force, revolutionizing traditional approaches to surveillance and authentication. As cyber threats become increasingly sophisticated, the need for strong and reliable security measures is more pronounced than ever. This paper explores the integration of biometric systems in cybersecurity surveillance, provides a defence mechanism against unauthorized access and cyber intrusions[1].

A. *Cyber Security*

Cyber security is design to protect Network, mobile devices, electronic system, and data from malicious attacks. It is basically used to provide authentication mechanisms. for eg:- If a user wants to access his account then his name identifies on account, while a password is mechanism that proves that this account is associated with him. It is concerned with the security of any data that passes over the e-network in electronic form. It mainly deals in securing both information as well as the network(s) through which information flows. E-security is protecting an organization from internal as well as external threats and attacks. 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 the-network and information based systems.

B. *Types of Cyber crime*

Cyber criminals uses various techniques to hack the system to gain profit. Some of the frequently used cyber crimes are discussed below:

1. Denialof service, or DOS attack: In order to prevent the targeted users from using a computer system or network, a Denial-of- Service (DoS) attack attempts to bring it down. DoS attacks accomplish this by flooding the victim with an overwhelming volume of information or traffic, which results in a crash. Both times, the DoS attack prevents genuine users (such as employees, members, or account holders) from accessing the service or resource they were expecting.

2. Malware: The term “malware” refers to a broad class of malicious software that is frequently distributed to and installed on servers and end-user computers. Cyber criminals use these attacks to steal data for financial benefit. They are intended to harm a computer, server, or computer network.

3. Man in the middle attack: In MITM attack, a user gets introduced to two parties at some sort of meeting, manipulates both parties, and obtains access to the data that the two parties were attempting to pass to one another. An adversarial attacker can also use a man-in-the-middle assault to send data that was never intended to be delivered, but was instead intended for someone else, without any of the participants realizing it until it was too late. **4. Phishing attack:** Phishing is the act of an attacker trying to get a user to do “the wrong thing,” such as opening a malicious link or visiting a dubious website. Phishing can take place through text messages, social media, or phone calls, but it most commonly refers to attacks that come in the form of emails. Phishing emails can directly reach millions of users and can blend in with the countless good emails that busy users receive. Attacks can install malware (like ransomware), steal money and intellectual property, or destroy systems.

II. BIOMETRIC SYSTEM

Biometrics refers to the measurement and statistical analysis of an individual’s unique physical and behavioral characteristics for the purpose of identification and authentication. Biometric systems are used to recognize and verify the identityof a person based on their unique biological or behavior traits. Biometric systems, such as voice, iris and facial recognition were developed in the second half of the 20th century. In the 2010s, these technologies achieved economic viability, and they have subsequently been widely used. Border control, law enforcement, access control, and identity verification are just a few of the current biometric applications. Through the application of advanced algorithms, machine learning, and artificial intelligence, biometric systems have gotten more sophisticated. All the biometric systems have four basic modules which are sensor module, feature extractor module, matcher module and decision module [2]. These four modules are necessary in any biometric system to acquire and process raw biometric data and convert it into some useful information.

1. **Sensor Module**: In this type of module raw biometric data is captured by the sensor and it scans the biometric trait to convert it into digital form. After converting it to digital form, this module transmits the data to feature extraction module.
2. **Feature Extraction Module:** It is used to process the raw data which is captured by sensor and then it generate a biometric template. It take out the necessary features from the raw data which requires much observation because those key features must be extracted in an exclusive way. It basically removes noise from the input sample and transmits the sample to input sample to the succeeding module known as matcher module.
3. **Matcher Module:** This module uses a matching algorithm to compare the input sample with the templates that are stored in the database and generates a match score. The decision module then received the output match score and made the decision regarding whether or not to accept the applicant.

III. **Decision Module:** It compares the matching score to the predefined security threshold after accepting the match score from the matcher module. This module decides whether to admit or reject the person based on a predefined security threshold. Individual will be accepted if match score is higher than predefined security level; otherwise, this module will reject him.

IV. ATTACKS ON BIOMETRIC SYSTEM

Biometric based authentication systems use physiological (like face, iris etc.) and behavioral traits (like voice, signature etc.) are become very popular day by day and utilized in many applications to increase the security of the system. Outmoded systems are unable to differentiate an authorized person and unauthorized person properly who can fraudulently access the system. We can use Biometric systems more conveniently because we do not need to remember any password and with a single biometric trait as we can be secure different accounts without the burden of remembering passwords. Biometric systems offer huge advantages over outmoded systems but they are vulnerable to attacks [3]. These attack points are divided into two categories: Direct attacks and indirect attacks.

1. **Direct attacks:** It typically refers as such attacks that do not need any specific knowledge regarding system operation such as matching algorithm used, feature vector format, etc. It consists only type 1 attack which is referred as “Sensor Attack”.

1) Type 1 attack: The sensor module is vulnerable to type 1 attack which is known as “Attack at the sensor”. In this assault, an impostor presents a phony biometric feature, such as a fake finger or facial image, to the sensor in order to get around identification systems [4]. An impostor can also physically compromising the recognition system and flood overloading the system with false access requests is a straight forward tactic. Attacking the sensor is made simpler by the fact that it doesn’t require specific knowledge of the system’s operation. Additionally, there are no digital security measures, such as watermarking or cryptography, in place at the sensor level. Sensors often struggle to differentiate between genuine and counterfeit individual traits, and they can be readily deceived by artificial fingerprints and face picture of a person.

2. **Indirect attacks:** Unlike direct assaults , these are the type of attacks that necessitate knowledge about the internal operations of the authentication system to achieve success. It encompasses the seven remaining points of attacks (2, 3, 4,

5, 6, 7, 8) that an impostor can exploit in a biometric-based authentication system.

1) Secondary Attack: When the sensor collects raw biometricdata, it transmits this data to a feature extractor module for initial processing using a communication channel. This channel is situated between the sensor and the trait analysis unit. The interception is performed to capture the biometric trait, which is then saved in a different location. The previously stored biometric trait can be replayed to the feature extractor to circumvent the sensor. This is denoted as "replay attack" [4].

2) Tertiary attack: The feature extraction module is susceptible to a tertiary attack referred to as the "Attack on the feature extraction module". When the sensor collects raw biometric data, it transmits this data to the feature extractor module. An impostor exerts pressure on the feature extractor module, compelling it to generate feature values selected by the intruder, rather than producing the feature values derived from the original data captured by the sensor.

3) Four-tier Attack: This attack shares similarities with secondary attacks. The distinction lies in the fact that an impostor intercepts the communication channel between the feature extractor and matcher modules, acquiring the feature values of genuine users[4]. These values can be subsequently replayed to the matcher. It is denoted as "Attack on the channel between the feature extractor and matcher".

4) Tier 5 attack: The matcher module is unprotected to tier 5th attack which is known as "Attack on matcher module" [5]. The attack is launched to produce a high matching score, as chosen by the impostor, in order to circumvent the biometric authentication system, irrespective of the values derived from the input feature set.

5) Tier-6 attack: This situation arises when an deceiver compromises the security of the database by introducing new prototype, altering existing prototype, and deleting pre- existing prototype [5]. Circumventing the system database is a challenging task therefore prototype are secured by cyber system such as steganography, watermarking, etc. To make successful attack on system database some understanding the inner workings of the system is a prerequisite.

6) Tier 7 attack: An attack can occur only when a protype is being sent through the conduction path between the system database and the verification unit. This happens when an impostor alters or tampers with the contents of the sent prototype. An impostor catch the channel with the intent to steal, replace, or alter a biometric prototype Attack on the communication channel between the system database and the matcher" is how it is described.

7) Tier 8 attack:- An impostor can potentially override the outcome provided by the verification unit. In this scenario, an impostor may manipulate the match score transmitted via the communication channel between the verification unit and the application device. It alters the match score to influence the original decision (accept or reject) made by the verification unit. After examining these eight attack points, the author noted that in most cases, adversaries target the templates intended for storage in the database . These stored prototype in the database are susceptible to tampering through the addition of new prototype, by altering the existing templates in the database and deleting templates from the database.

V. Common Security Risks

All classical systems and biometric systems are vulnerable to a variety of threats . These threats include:

i. **Service blockage:** It describes the action in which an impostor inundates the authentication system with fake requests, rendering it unusable for genuine users. An verification server that handles access requests can be packed with many fake access queries, to a point that all hardware capacity are useless in fake requests and cannot handle valid requests any more.

ii. **Bypass:** It happen when an imposter gains access to the system that was protected by the verification process and control the system by altering records in an wrongly manner.

iii. **Rejection:** A real user may access the system tool and

iv. claims that the system had been bypassed by the impostor. For instance, a dishonest bank officer illicitly manipulated certain financial records and asserted that their biometric data had been stolen.

v. **Corruption:** It involves the act of an impostor clandestinely acquiring the biometric data of legitimate users and utilizing it to gain unauthorized entry to the system. For e.g., a biometric data connected with a particular application can be used in another application (using a fingerprint for obtaining medical records in place of the intended use of officedoor security control).

vi. **Compulsion**: An impostor intimidates the genuine user in order to gain control of the system themselves. For example, an ATM user could be threatened at gunpoint.

vii. **Collusion:** It occurs when administrator user with high privileges makes wrong use of his benefits and altering the factors of system wrongly. A administrator user with wide access perks has right to access all the system's resources. All the threats discussed earlier are utilized to launch potentially harmful attacks on biometric-based authentication systems. These attacks are often motivated by financial gains, such as attempting to hack a bank account secured with biometric authentication to make unauthorized withdrawals. Therefore, it is crucial to defend against these attacks. In the following section, we explore various template protection techniques to counteract these threats.

VI. APPROACHES TO RESIST ATTACKS

All the approaches applied for securing biometric template are known for withstanding attacks. Some of the recognized biometric template safeguarding approaches are as follows:

i. **Liveness detection**

Liveness detection is a structure that is used for identify that input prototype functionality is offered by live human being or not. It is utilized to hinder the sensor from attacks. It is a capacity to differentiate between genuine input sample feature provided by living individual and a fake input prototype provided by a creation [8]. Liveness detection can be executed through software or hardware methods. Utilizationof additional hardware to deploy liveness detection methods for measurement various life signs comparable to heartbeat identifications, systolic pressure, warmth for fingerprints and visage changes, facial analysis through eyes. The drawbackof employing additional hardware renders the system excessively costly. Employing software based measures utilize the pervious gathered data to identify the vital signs . The only utilized methods is to employ existing data about sweat pores. For this a scanner capable of a capturing high image quality image is necessary. It is practically impossible to reproducethe precise dimension and location pores on an artificial mold.

ii. **Biometric cryptosystems:** A biometric cryptosystem combines cryptography and biometrics to provide a higher level of security. Biometrics replaces the need to carry tokens or remember passwords, while cryptography offers a better level of security. In traditional systems, one or multiple keys are used to encode a plain text into a ciphertext, which is known as an encrypting key. A decrypting key is required to restore the plaintext to its original state. If an imposter tries to

extract information from the cipher text, they would be unableto do so without this key. To prevent dictionary attacks, we use cryptography to protect the security of password-based authentication. Biometric cryptosystems are further divided into key generation and key binding. Key generation This process involves obtaining helper data solely from biometric traits. The helper data is then used to directly generate a cryptographic key. Key release This process involves binding a cryptographic key with a biometric template. The biometric template contains information about the individual’s unique biometric traits. The key is associated or linked with the biometric template to create helper data. The helper data, which includes the bound key and biometric template, is obtained

iii. **Steganography and Watermarking**: Steganographyis the term for covered writing. It speaks of the method through which the original data is concealed using a cover image [10]. Steganography is realized in watermarking technology. Attack points 2 (attack on the channel between sensor and feature extractor) and 7 (attackon the channel between matcher and application device) are protected by steganography and watermarking. The hiding strategy of these two techniques is the same, but the parameters of the embedded data, the host image, and the data transfer medium vary. The authentication of ownership claims uses watermarking. Important biometric data can be transferredfrom a client to a server using steganography.

iv. **Cancellable biometrics**

A technique known as cancellable biometrics involves purposeful and systematic deformation of the biometric template based on a chosen non-invertible transform [11]. If a converted template is lost, its parameters can be changed to cancel and reissue it. In order to stop form attacks at attack point 6 (attack on the system database), cancellable biometrics are utilized. The topic of non-replaceability is also covered.

CONCLUSION

In this research work we have described biometric technology along with its modules after which we explored various attacks on biometric system. Biometric strictures such as fingerprint perusing, retinal scanning, iris scanning, signature verification, hand geometry, voice verification and others are all well recognized with their own specific characteristics. We have found that most of the attackers are targeted towards the biometric templates which are stored in system database. This paper also focused on various techniques to oppose attacks that can be used to program biometric templates and also tells about generic security threats to any system. Additionally, it provides information on how to use steganography, watermarking, cancellable biometrics, and biometric cryptosystems to strengthen the integrity of biometric templates. The current mechanisms would be improved and changed to create a secure, error-free system. For a security system to be effective, accuracy standards must be raised. The right technique must be chosen in accordance with the requirements. Scientific work is being done to advance biometrics and prepare it for future uses.

REFERENCES

[1] A Jain, L. Hong and S. Pankanti, "Biometric Identification", Communications of the ACM, vol. 43, no. 2, pp. 91-98, 2000. Show Context Access at ACM Google Scholar

[2] Anil K. Jain and Arun Ross, "Introduction to Biometrics" in Handbook of Biometrics, Springer, pp. 1-22, 2008, ISBN 978-0-387-71040-2. Show Context CrossRef Google Scholar

[3] Sahidullah and Md, Enhancement of Speaker Recognition Performance Using Block Level Relative and Temporal Information of Sub band Energies, 2015. Show Context Google Scholar

[4] "Biometrics for Secure Authentication", (PDF)Retrieved. Show Context Google Scholar

[5] http://www.bioelectronix.com/what_is_biometrics.html.

[6] http://www.biometricnewsportal.com/biometricsissues.asp.

[7] http://www.explainthatstuff.com/how-iris-scans-work.html.