Security Enhancement in Biometrics At Higher End to Avoid Security Breach [A Survey]

Anusha M.S.
Dept. of CSE [Ph.D],
VTU, Belagavi India

Dr. Kavitha K.S.
Prof., Dept. of CSE
Global Academy of Technology,
Bangalore, India

***Abstract*:-In this modern world of technology and research work, there is scope for development linking technology with biology or human anatomy, where we can use our own eyes, fingers, body temperature and other factors to prove who we are, this is a technology known as *BIOMETRICS*. Biometrics is the rapidly advancing field of research today with Billons $ invested around the globe. The main driving factors for this can be identified as,**

1. Demand for more authenticate yet simple Security systems.

2. Introduction of Biometrics enabled authentication on "Smart Phones", "E-payments" and many more

3. Identity „to know your X‟.(uniquely identify who we are)

The security breaching has become a biggest problem even with the advancements in the implementation of new security procedures and even the much hyped biometrics is also proved not to be false proof.

There are so many cases where the biometric security is breached mainly because it is easily accessible and the points under consideration are not of secured grounds. As identity continues to become a bigger part of our lives, biometrics is playing an increasingly critical role in establishing identity „to know your X‟.

In this paper, we would like to present the different Biometrics used to provide unique identification and its breaches and future of Biometrics in Research.

I. INTRODUCTION

Today‟s world is driven by the word "IDENTITY" .

In every step of our life we need to prove „who we are‟ (authenticate & uniquely), with the advancements of the technology, it has become easy along with Biometrics. Biometrics research has varied applications ranging from Automated recognition of people, Sharing data over network, Mobile computing, Criminal investigations, Forensic applications, Digital Forensic, Machine Learning, Image understanding, Neuroscience and so on.

Applications converged in a truly multidisciplinary effort to devise and build advanced systems to facilitate the interpretation of signals recorded from individuals acting in a given environment. This is what we simply call today "Biometrics".

Biometrics with its ease of use has driven the world towards it. The growing needs to deliver strong identity verification and access control in areas of high sensitive activity, (banking, security records …) along with an increasing emphasis on Security, has driven the adaption of Biometrics in day to day life.

II. DIFFERENT USAGES OF BIOMETRICS

Mass market is the target field with one to one context, for which processing of Biometrics driven Technology (especially Fingerprint Technology) for Identification and Authentication in as small time as possible (typically less than 1sec) is the requirement of the day.

There are many projects proposed around the world, based on Biometrics in different fields of usage in day to day life where Authentication of „who is using‟ the system is important. There are already a number of products that we are using in our life and here is what more we can expect from this area of research,

□ **Banking Sector:** With the Indian IT giant INFOSYS proposing the Biometrics for ATM‟s and Banking transactions across the world, the focus is on Biometric Systems and its Security.

□ **Citizen Sectors:** US Govt. under General Services Administration has announced a Personal ID for all its Citizens, with the principle of Biometrics.

□ **Customs Sector:** US Immigration and Customs Sector has announced that they derive the help from Biometrics (Fingerprint) to identify the parent of illegal youth immigrants in the country.

□ **Computers Sector:** Today‟s trend start with Smartness and Biometrics is one such smartness principle that has attracted the world today. Lenovo, Dell and other giants in the computer manufacturing industry have shown their interests in adapting Fingerprint and iris or facial recognition systems in their product as the key to switch on their systems.

□ **Mobile Sectors:** The world today is around "Technology used in Small", there is situation such that no mobile no life and smarter the mobile smarter is the life. With this situation and Apple‟s rocking introduction of fingerprint access in their 4s shook a big wave in the Mobile industry.

Huawei has announced 5C fingerprint access with precise biometrics in its new unrevealed cell phone.

The world is waiting eagerly to know what‟s new every day morning. The technology and research today is focused on smartness and the fields around

Biometrics, Image Processing, AI, Neural Networks mainly over others.

But as the Technology increases the fear of breaching and corrupting the system have become the biggest challenge to be tackled. Let us look at the few famous applications of Biometrics and the breaches.

III. BREACHES IN SECURITY SYSTEMS

USING BIOMETRICS

We have the incidents of records where we have the breaches in the biometrics. To name a few,

1) A man at Manchester Airport swapped his passport with that of his wife and the facial recognition system had given the clearance to the passport.

2) A man in China had prepared the artificial fingers with gelatin and provided the required temperature during the finger scanning time to dupe the machine which he succeeded up to 90% with different manufacturers.

3) Even the apple i Phone5s was also a victim of the break of biometric system where hackers from Germany have broke the much touted Touch ID Security for the APPLE i PHONE.

4) Recently there was a car theft in Germany whose unlocking system was of finger locking system, which was breached and stolen.

and so on. With these incidents it‟s an alarming sign to provide the security for the security systems.

IV. REQUIREMENTS / FACTORS TO BE CONSIDERED TO PROVIDE A STRONG AUTHENTICATION

A. BANKING SECTOR AND BIOMETRICS

Authenticating with Confidence is what we require today in the Banking Sector. We can call it as "your security connected". Utilizing Lumidigms‟s multispectral imaging with advanced technology to scan and authenticate fingerprints from the inside out is the technology. By capturing additional data from below the surface of the skin, we can read and match fingerprints even when the external characteristics are damaged or obscured. When it is important to know "who" is transacting, the only option is secure, convenient and trusted Biometric solutions.

B. ENSURING BIOMETRICS DATA IS USELESS TO IDENTITY THIVES

Biometrics is the only authentication method that binds a myriad of digital and physical credentials to a person. As such Biometrics plays an important role in eliminating digital identity theft in today‟s increasingly complex and vulnerable digital environment.

Fingerprint images were among the sensitive information that was stolen in the 2015 U.S. office of Personnel Management (OPM) breach.

Conceivably this biometric data could be used by the perpetrators to hijack a user‟s identity and gain fraudulent access to security systems.

It is important to understand that biometric characteristics are not secrets. Facial characteristics are quite public, not only observable but also generally associated with our names and other personal information. Critical importance is the ability to detect fraudulent attempts to use biometric data. Liveness detection — the real-time determination that the biometric characteristics presented are genuine and not fake — is a highly effective design feature in solutions where users physically interact with authentication systems.

Augmenting biometric liveness detection with other security layers for multi-factor authentication greatly enhances digital security and renders the theft of any one personal data element inconsequential. There are also a number of concepts that combine biometric data and other data elements to create an even more robust digital credential that will ensure stolen biometric data is insufficient and therefore useless in enabling the fraudulent use of legitimate identities.

C. IMPROVING LIVENESS DETECTION

One of the most effective liveness detection approaches for fingerprint biometrics needs a technology that virtually eliminates the possibility of counterfeit fingerprints being used for authentication. The unique capability, of collection fingerprint characteristics from both the surface and subsurface of the finger, results in superior and reliable matching performance paired with the exceptional ability to detect whether the finger is alive or not.

D. MULTI-FACTOR AND MULTI-MODAL AUTHENTICATION

For strong and reliable user authentication, organizations should consider where practical, multi-factor and even multi-modal authentication is required. Today‟s authentication technologies enable solutions that can enhance security while replacing passwords and improving convenience in a seamless way that is non-intrusive to the legitimate user.

For example, personal devices like Smartphone‟s, wearable‟s, RFID cards and other intelligent personal devices can all generally be used as factors of authentication. Regardless of which additional authentication factor is presented by the user, when it is intelligently combined with biometric data associated with an identity claim, it is possible to quickly determine a definitive "yes" or "no". Strong authentication by means of two or more factors (with one being a biometric) is fundamentally more secure than outdated username/password alternatives.

When identity is firmly established, the use of mobile devices in authentication solutions offers the opportunity for greater personalization and a seamless experience for legitimate users. Information systems can be tailored to each user‟s need, resulting in enhanced, individualized security, allowing individuals to fully control their real identity. Instead of the system blocking the legitimate user an unintended consequence of blocking an attacker the system is made more secure and efficient and thus returns a higher ROI for both the consumer and system administrator.

E. IDENTITY PROFFING

It‟s important to remember that the chain of trust is only as strong as the weakest link. The biometric solution used in identity-proofing must interoperate with trusted devices at each verification point. Additionally, the physical devices themselves must be tamper-resistant to ensure that all transaction integrity is preserved.

Trusted devices must be encryption-enabled with various tamper resistance and detection capabilities that protect the integrity of the communication between the client and the sensor.

The end-point device must connect to the institution‟s systems through a cryptographically secure channel protected by hardware tamper detection and response, which establishes trust between the device and the institution‟s systems independent of intermediate systems and networks.

A trusted biometric device must be able to perform a live scan of a finger with strong liveness detection to ensure that the person making the transaction is who they claim to be (that is, the person is not a fraud and he is a genuine entity of who the system claims to be).

F. REGULATIONS OF FINANCIAL MARKET

Operational risks that financial institutions face are increasing due to the elimination of face-to face service and the advent of electronic banking. Banks must verify the legitimacy of customer identifications, transactions, access and communications, which demands an incredible amount of vigilance.

Implementing a biometric-enabled authentication system can be a very efficient method of protecting the technological assets of an enterprise against the attacks of internal and external intruders.

In terms of banking customers, a biometric identifier can measure an individual‟s unique physical characteristic or behavior and compare it to a stored digital template to authenticate that individual. Biometric identifiers can be created from sources such as a customer‟s voice, fingerprints, hand or face geometry, the iris or retina in an eye, or the way a customer signs a document or enters keyboard strokes. All of these identifiers are used in the banking sector, in a myriad of ways.

Financial institutions have also taken to combining multiple authentication factors. Multi-factor authentication is a method of multi-faceted access control which a user can pass by successfully presenting authentication factors from at least two of the three categories:

- Knowledge factors ("things only the user knows"), such as passwords or pass codes;
- Possession factors ("things only the user has"), such as ATM cards or hardware tokens; and
- Inherence factors (unique factors "things only the user is"), such as biometrics

Knowledge factors are the most commonly used form of authentication.

V. CONCLUSION

A unique proposition of biometrics is the diverse number of modalities that find application in Financial Sector. Modalities ranging from non-AFIS fingerprint recognition, face, iris, vein, voice, signature, and hand geometry recognition have all found varying levels of acceptance.

The main aim of Biometrics in Financial sector would be,

- To prevent Identity Fraud
- To make it more Reliable, Convenient & Secure.

Biometrics is the only technology that assures identity and knowing "who" to a high degree of certainty. Biometrics is also unique in its ability to raise the bar on security while adding convenience for the end user.

VI. FUTURE TRENDS

Most financial institutions have adopted biometrics for operational and employee-facing applications. Wider deployment in the financial industry is anticipated as the number of successful credible reference sites increases and financial institutions realize the cost-efficiencies and benefits of biometric technologies in comparison to alternate security technologies.

From an end-user perspective, it is imperative to publicize the benefits that biometrics can offer in terms of convenience, cost efficiencies and time efficiencies.

With biometrics, the ability of financial institutions to provide more value to their customers, while complying with regulations, can provide them with a competitive advantage.

REFERENCES

1. A paper by sans institute on "sans institute infosec reading room" 2013.
2. A thesis by seungil huh on "cellular event detection in time lapse in live cell microscopy images" 2014.
3. Bolgs at m2sys blogs on biometric pros and cons.
4. Newspaper at
    - Dily mail u.k.
    - The washigton times.
4. "Amid rampant data breaches and hacks, biometric takes off" by Deborah Gonealez, 2015.
5. Tech mazine fortune.
6. Information from biometric system manufacturers hoyos lab, u.s.
7. Soft biometrics for subject identification using clothing attributes, Jaha E.S. ; Nixon M.S. , IEEE oct 2014
8. Comparative Study on Biometrics: a Review , Aditi Verma , Meha Khera, IEEE may 2014
9. Improving the Security of MANETs Oriented Military Intelligence using Biometrics Authentication Technologies, Julius N. Obidinnu , Ayei E. Ibor, S. O. O. Duke Jan 2014
10. A Novel Framework for Multimodal Biometrics based on Dimensionality Reduction Technique for Reducing Overlapping Features , Manas Kumar Choudhury and Y.Srinivas , Feb. 2015.
11. On Generation and Analysis of Synthetic Finger-Vein Images for Biometrics Identification, Fieke Hillerström, Ajay Kumar, June 2014
12. Cloud Computing, Security Issues and Potential Solution by Using ICMetrics or Biometrics Based Encryption, Masudur Rahman, Wah Man Cheung , Oct 2014
13. An application framework for evaluating methods in biometrics systems, Kautsar, S.A
    - Akbar, S. ; Azizah, F.N, IEEE 2014.

14. Biometrics Based Key Generation using Diffie Hellman Key Exchange for Enhanced Security Mechanism ,M.S.Durairajan, Dr.R.Saravanan, chem tech, Dec 2014 .
16. Authentication Using Pulse-Response Biometrics, NDSS, Kasper B. Rasmussen,Marc Roeschlin, Ivan Martinovic, Gene Tsudik, 2015.
17. Preventing Lunchtime Attacks: Fighting Insider Threats with Eye Movement Biometrics, NDSS, Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic 2014.
18. Biometrics - a vision of future, white papers, HCL technologies, Kumaralingam R., Rahul G 2012.
19. Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System, Jucheng Yang, IEEE 2014.

WEBSITES REFFERED

1. WWW.BIOMETRICSUPDATE.COM
2. WWW. HIDGLOBAL.COM
3. WWW.AMC.ORG

ONLINE NEWSPAPERS AND TECHNOLOGY PAPERS

- LAYERS HEARLD
- NEWYORK TIMES
- TECHNOLOGY DAILY
- CNBC
- WESTERN MASS NEWS
- ABI RESEARCH