Effective Authentication Mechanism in Real World

[1]Hridya Venugopal, [2]Mary Subaja Christo, [3]Uma Priyadarsini

[1,3]Assistant Professor, [2]Associate Professor
[1,2,3]Department of CSE, Saveetha School of Engineering,
[1]hridyavenugopal.sse@saveetha.com, [2]marysubajachristo.sse@saveetha.com,
[3]umapriyadarsini@saveetha.com

Article Info
Volume 83
Page Number: 5105-5107
Publication Issue:
May - June 2020

Article History
Article Received:*19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *16 May 2020*

Abstract

Authentication is used to verify the identity of an individual in various applications and scenarios. It is one of the methods to ensure security aspect in various domains. Authentication is employed by a server once the server must recognize specifically who is accessing their info or website. It can also be the one employed by a shopper once the shopper must recognize that the server is system it claims to be. In authentication, the user or pc must prove its identity to the server or shopper. Usually, authentication by a server entails the utilization of a user name and word, different ways in which to certify are often through cards, tissue layer scans, and fingerprints. But all these include the use of the touch in any aspect. So to enable an efficient touchless authentication system, a multimodal biometric including face and iris can be used.

Keywords: *Unimodal biometrics, multimodal biometrics, OTP.*

1. Introduction

A number of aspects, as well as lesser value of network devices, larger web and mobile web penetration, availability of devices and multiplied use of the smartphones have gone into commercialising on-line banking round the world. The circumstance remains that in spite of the advancements in security technology, vulnerablity still exist. Studies shows that a lot of phishing and social engineering attacks come about round the world each month. although there square measure several threats and vulnerabilities, awfully sturdy authentication mechanism for customers and transactions can address most fraud related problems except for incorporating sturdy authentication mechanism, sure banks limit the quantity of on-line banking operations that a client will perform every day. Biometric technology ensures the sturdy and safe technique to create secure authentications of persons. an outsized portion of system breaches square measure caused by authentication failure, either throughout the login method or within the dealings method that exist thanks to the constraints incidental to the prevailing authentication ways.

In the current world, authentication of on-line banking users is completed victimisation the subsequent methods: [1]

A. Information primarily based

This technique, that is that the most well-liked and customary, asks the users to manifest by getting into their User Id and arcanum. The bank safeguards the protection by making certain that the users have a robust arcanum which square measure modified at a frequent intervals that is appointed to be for few days.

B. TOKEN primarily based

Token primarily based technique is presently utilized in the majority onine bank transactions. This technique authenticates the users supported the information primarily based identity and one thing else that they need. This is sometimes done victimisation OTP (One Time Password), or token devices.

2. Related Works

A. Unimodal Life Science

The unimodal biometric systems have faith in the proof of one supply of knowledge for authentication of person. Though these unimodal biometric systems have several benefits, it's to face with selection issues like buzzing knowledge, Intra category variation, Interclass similarities, Non generality, Spoofing etc.

B. Multimodal Systems

Depending on the traits, sensors and have sets many various forms of multimodal systems square measure there. These include:[2]

1) Single biometric attribute, multiple sensors: Multiple sensors square measure accustomed record a similar biometric characteristic. The data taken from completely different sensors will then be combined at the feature level or intermediator score level to boost the performance of the system.

2) Multiple biometrics: Multiple biometric traits like fingerprints and face is combined. Different sensors square measure used for every biometric characteristic. The reciprocality of the traits ensures a major improvement within the performance of the system.

3) Multiple units, single biometric attributes: 2 or additional fingers of one user is used as a biometric trait. it's cheap manner of rising system performance, because it doesnt need multiple sensors or incorporating extra feature extraction or matching modules. Iris also can be enclosed during this class.

4) Multiple snapshots of single biometric: during this over one instance of a similar biometric is employed for the popularity. For e.g. multiple impressions of a similar finger or multiple samples of the voice.

5) Multiple matching algorithms for a similar biometric: In it completely different strategies is applied to feature extraction and matching of the biometric characteristic.

3. Proposed System Design

The essential attributes for any bioscience are: the amount of degree-of-freedom of variation within the chosen index across the human population, since this determines uniqueness; its unchangingness over time and its immunity to intervention; and therefore the procedure prospects for with efficiency encoding and faithfully recognizing the characteristic pattern. within the whole human population, no two irises square measure alike in their mathematical detail, even among identical twins. The probability that 2 irises may manufacture precisely the same Iris code is close to one in 1078.Iris recognition may be a technique of biometric identification , supported extraction options of the iris of an individual’s eyes. Biometric recognition refers to associate automatic recognition of people supported a attribute vector(s) derived from their physiological and/or activity feature. Biometric iris recognition systems ought to give a reliable personal recognition schemes to either ensure or verify the identity of associate person. Completely different algorithms area unit enforced to perform iris recognition system.

Iris recognition system is enforced as depicted in fig(a).

Here, the technique consists of the following elements:
Step 1: Preprocessing & Iris capturing: this method includes revises process within which the image which the image should be adequate ebe adaptive to successive step. Then the iris is truncated and resizing from rhe first image.
Step 2: changing image into grey scale: this method deals with the changing of color image into grey scale image.
Step 3: bar graph equalization: this method includes redistributing of pixels so as to reinforce the overall image.
Step 4: 2nd DWT: this method in applied to get the foremost important options of the image in order to attenuate the interval moreover on get minimum reduction size.
Step 5: Edge detection: this method in helpful to get the minimum feature needed to identify the particular iris.
Step 6: Storage method: this process tries to rearrange the generated options into vector to be prepared in testing process.

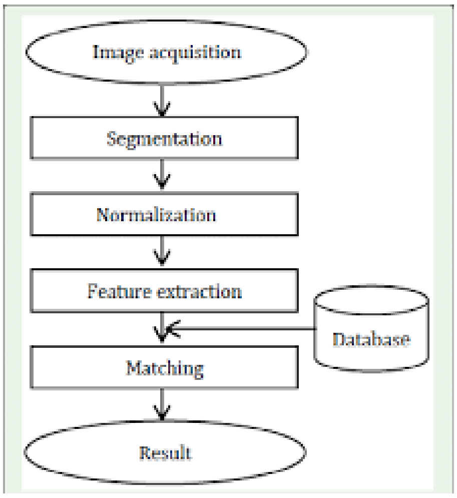

Figure (a): Iris Recognition system.

4. Result

Iris recognition is one in all the foremost secure biometric modalities for the needs of identification and therefore the ulterior authentication of a private. It's extraordinarily tough to forge associate iris scanner reading due to the distinctive characteristics of the iris. Compared to different modalities, it's a considerably lower false acceptance rate and false rejection rate. It is an extremely helpful technology in areas like border security, membership authentication, monetary institutes, and knowledge security to all simply some of its several uses.

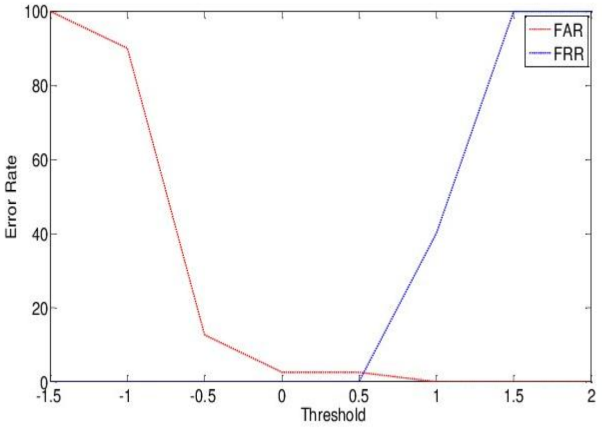

Figure (b): FAR and FRR comparison of iris.

5. Conclusion

Authentication mechanism using iris recognition is an efficient method where the false acceptance ratio is much reduced. Hence this can be used for any unique authentication system.

References

[1] Khattab M. Ali Alheeti ,"Biometric Iris recognition based on hybrid technique", International Journal on Soft Computing (IJSC) Vol.2, No.4, November 2011

[2] Available "http://www.edgeverve.com/finacle/resources/thought-papers/Documents/what-the-future-online-banking.pdf

[3] Sheena S, Sheena Mathew," A STUDY OF MULTIMODAL BIOMETRIC SYSTEM", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 — pISSN: 2321-7308

[4] S.R.Soruba Sree , Dr. N.Radha,"A Survey on Fusion Techniques for Multimodal Biomet- ric Identification, International Journal of Innovative Research in Computer and Com-munication Engineering, Vol. 2, Issue 12, December 2014.

[5] Mary Lourde R, and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010 1793-8163

[6] K.Saranya, K.Baskar, "Multibiometric Secure Index Value Code Genera-tion for Authentication and Retrieval", International Journal for Scientific Research & Development— Vol. 1, Issue 5, 2013 — ISSN (online): 2321-0613

[7] Uma Priyadarsini P S, Dr.P Sriramya, "Regenerate the Connectivity in Damaged Wireless Sensor Networks Using Modified Convex Hull Algorithm", Journal of Advanced Research in Dynamical and Control Systems Vol. 9. Sp– 17 / 2017.

[8] Uma Priyadarsini P S, Dr.P Sriramya, "Formalizing a Trust Management Control Mechanism in Wireless Sensor Networks Using a Polynomial Reduction Algorithm over the IoT", Journal of Advanced Research in Dynamical & Control Systems, ISSN 1943-023X, Vol No.06, 2017, Pages: 153-172.

[9] Uma Priyadarsini P.S, Sriramya.P, "Conditional Privacy-Preserving Authentication with Access Likability for Roaming Service over Internet of Things", International Journal of Engineering & Technology, 7 (1.9) (2018) 34-40.

[10] Midhun Chakravarthy**, Sybi Cynthia J.,** **"**Enhanced Heuristic Scheduling Design for Cloud Systems," TEST Engineering and Management, Vol. 82, February 2020, pp10845-10850.

[11] J. Venkata Krishnakanth**, Sybi Cynthia J.,** **"**A Framework for Detecting Spam Reviews in Online Social media," TEST Engineering and Management, Vol. 82, February 2020, pp 10766-10768.

[12] K. Sai Shashank**, Sybi Cynthia J.,** **"**Privacy Preserving Social Media Publishing for Personalized Ranking Based Recommendation," TEST Engineering and Management, Vol. 82, February 2020, pp 6540-6543.

[13] T. Vijay Kumar**, Sybi Cynthia J.,** **"**A Two Factor Key Authentication for End to End. Decryption," TEST Engineering and Management, Vol. 82, February 2020, pp 6601-6604 .

[14] Sheryl Radley**, Sybi Cynthia J.,** K. Premkumar , **"**Multi Information Amount Movement Aware-Routing in FANET : Flying Ad-hoc Networks," Mobile Networks and Applications, Special Issue on Mobility of Systems, Users, Data and Computing, November 2019, pp 1-13.(Annexure 1)

[15] **Sybi Cynthia J.,** Sheryl Radley, Mary Gladence., **"**Fuzzy Logic determining multi-paths in Gray hole attack for improving the energy efficiency of sensor networks," Journal of Mechanics of Continu and Mathematical Science, Special Issue no. 3, September 2019, pp 29-38.(Web of Science).

[16] **Sybi Cynthia J.,** Rathna R., **"**Fault Tolerance & Load Balanced Ad-hoc Networks using LRDV Routing Protocol, International Journal of Innovative Technology and Exploring Engineering, Vol. 8, Issue-9S4, July 2019, pp 222-226. (Scopus Indexed).