International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195335

Improving Net Banking Security with Face Recognition Based Bio-Metric Verification

V. Manju[1], S. Madhumathi[2]

[1]Assistant Professor, M.E. Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, karaikudi, Tamil Nadu, India

[2]M.E., Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Karaikudi, Tamil Nadu, India

ABSTRACT

Internet banking services must be more responsive towards security requirements. Now a days with the network world, the way for cybercrime is become easier for hacking purpose. Because of this reason, network security has become one of the biggest concerns of today security environment. While there is no doubt that Internet banking transaction must have layered safety towards protection threats, the vendors should technique protection issues as part of their provider services. And heard a lot about hackers and crackers ways to steal any logical password or pincode number character, crimes of ID cards or credit cards fraud or security breaches. In existing work, Identification can be processed to a username and is used to authorize access to a system. As usernames can be lost or stolen, it is necessary to validate that the intended user is really the person he or she claims to be – the authentication process. Biometric based totally authentication and identification structures are the new answers to deal with the issues of safety and privacy. The Face Recognition is the examine of physical or behavioral traits of individual used for the identification of individual. These biometric characteristics of a person include the various features like fingerprints, face, hand geometry, voice, and iris biometric device. Here implement real time secure authentication system using face biometrics for authorized the person for online banking system. The general objective of our project is to develop fully functional face recognition, verification system provide and understand the key aspects of these major technologies, social environmental system and performance aspects. And also provide multiparty access system to allow the multiple persons to access the same accounts by providing access privileges to original account holders. Experimental results show that the proposed system provide high level security in online transaction system than the existing traditional cryptography approach

Keywords : Secure Net Banking, Multi party access, ICP Feature detection, KNN Classification

I. INTRODUCTION

Online transaction has end up a commonplace fashion now-a-days and security related to the identical is turning into an difficulty. Authentication using passwords is liable to assaults like hacking; therefore by making use of biometric traits we are able to authenticate the person‘s identification. Face is a included internal organ whose random texture is complex, particular, and very stable at some stage in lifestyles, it can serve as a kind of living passport or password that one want no longer to be remembered however can usually be gift. So face popularity is one efficient manner of securing online transactions. Iris

popularity machine affords correct, strong, speedy, secure and user-pleasant authentication solution. It protects personal identity of users by using the acquisition, processing, evaluation and contrast of face patterns from their iris image. The intention of this undertaking is to enhance the safety of Internet Banking using face biometrics, as comfy authentication can't be judged most effective on the basis of username and password as they may be guessed easily. Face is an inner organ of an eye fixed this is rather blanketed. It has random texture with excessive complexity. They are recognised for their forte and balance throughout lifestyles. This undertaking aims to put in force an application so as to ask for the username, password as well as an iris photograph of the consumer, which the person must provide through his respective tool digicam. The software will pre-technique the iris photo and experiment through the database for authentication. If the username, password and iris image suits with database that in database then the consumer is authenticated.

1.2 BIOMETRICS

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is applied in laptop era as a form of identity and get admission to manipulate. It is also used to grow to be privy to people in companies that are under surveillance. Biometric identifiers are then unique, measurable traits used to label and describe individuals. Biometric identifiers are often labeled as physiological in place of behavioral trends. Physiological trends are related to the form of the body. Examples consist of, however are not confined to fingerprint, palm veins, face reputation, DNA, palm print, hand geometry, iris popularity, retina and odour/fragrance. Behavioral developments are associated with the pattern of behavior of a person, which include however no longer restrained to typing rhythm, gait, and voice. Some researchers have coined the term behavior-metrics to give an explanation for the latter beauty of biometrics.More conventional method of get entry to control include token-based identity structures, which include a driver's license or passport, and knowledge-based identity systems, such as a password or private identity quantity. Since biometric identifiers are specific to individuals, they're more reliable in verifying identity than token and expertise-based totally methods; but, the gathering of biometric identifiers raises privacy concerns approximately the final use of this statistics

1.2.1 Functionality:

Many specific components of human body structure, chemistry or behavior may be used for biometric authentication. The choice of a specific biometric for use in a specific software involves a weighting of several elements. And recognized seven such elements for use when assessing the suitability of any trait to be used in biometric authentication.

- Universality manner that everyone the usage of a machine ought to own the trait.
- Uniqueness approach the trait ought to be sufficiently exclusive for individuals within the relevant population such that they may be prominent from each other.
- Permanence pertains to the manner in which a trait varies over time. More particularly, a trait with 'top' permanence may be fairly invariant through the years with respect to the unique matching set of rules.
- Measurability (collectability) relates to the benefit of acquisition or measurement of the trait. In addition, obtained facts ought to be in a form that allows subsequent processing and extraction of the relevant characteristic sets.
- Performance relates to the accuracy, velocity, and robustness of era used (see overall performance section for greater info).

- Acceptability relates to how well individuals in the relevant population accept the technology such that they're willing to have their biometric trait captured and assessed.

Proper biometric use could be very application based. Certain biometrics could be higher than others primarily based on the specified ranges of comfort and security. No unmarried biometric will meet all the necessities of each viable utility.

MULTIMODAL BIOMETRIC:

Multimodal biometric structures use multiple sensors or biometrics to conquer the restrictions of unimodal biometric systems. For instance iris reputation structures may be compromised with the aid of getting older irises and finger scanning structures by means of tired or reduce fingerprints. While unimodal biometric systems are limited via the integrity of their identifier, it's miles unlikely that several unimodal systems will be afflicted by same barriers. Multimodal biometric structures can obtain sets of information from the same marker (i.E., more than one pics of an iris, or scans of the identical finger) or information from exclusive biometrics (requiring fingerprint scans and, using voice popularity, a spoken bypass-code).

Multimodal biometric systems can fuse these unimodal systems sequentially, simultaneously, a combination thereof, or in collection, which discuss with sequential, parallel, hierarchical and serial integration modes, respectively. Fusion of the biometrics information can occur at distinctive levels of a reputation machine. In case of characteristic degree fusion, the data itself or the capabilities extracted from multiple biometrics are fused. Matching-rating degree fusion consolidates the rankings generated by way of multiple classifiers referring to one of a kind modalities. Finally, in case of decision degree fusion the final effects of multiple classifiers are mixed thru strategies together with majority voting. Feature stage fusion is believed to be greater powerful than the other levels of fusion due to the fact the characteristic set incorporates richer statistics approximately the enter biometric statistics than the matching rating or the output selection of a classifier. Therefore, fusion on the characteristic level is anticipated to provide better recognition results. Spoof attacks consist in submitting fake biometric tendencies to biometric structures, and are a prime threat that can curtail their safety. Multi-modal biometric structures are commonly believed to be intrinsically extra robust to spoof assaults, but recent studieshave proven that they may be evaded with the aid of spoofing even a single biometric trait.

II. Related Work

Roger A. Leite, et al., [1] In proposed system the first task is the classification of known frauds. This process produces visual signatures for each group of similar fraud cases. Those signatures are later used, during monitoring, to identify potential hybrid attacks trough signature comparisons. This can be done automatically to some extend. However, fraud attacks are changing constantly. The visual comparison allows for appraising suspicious cases where automatic methods fail. This information is then used to modify the detection metrics accordingly. Costumers monitoring focuses on real-time monitoring of the data for an early identification or even prediction of suspicious behavior. To this end, use the fraud detection mechanisms described above. Our proposed technique include the following steps: (a) Generate different interactive visualizations from the uncooked multivariate information that are used to clear out the maximum interesting attributes in addition to their price tiers. Besides a focus on features desired by means of the experts, this step additionally lets in for producing first hypotheses approximately attribute relationships. Here have prototypically implemented this first phase. In the

next step, metrics or AI techniques are applied. Fraud detection analysts need to be able to set and edit available financial metric formulas, and also create their own metrics.

Roger Almeida Leite, et al., [2] Proposed system builds a profile for each user based on past transactions in which he/she was involved. For instance, considering financial transactions, we could construct a profile based on (1) how often the costumer executes operations, (2) how much money does he/she usually transfer, and (3) the geographic locations involved. New transactions are then evaluated against these profiles to figure out whether they are suspicious or not. This evaluation has different metrics depending on the dimension that is being analyzed. The output of this analysis is a set of score values that indicate how uncommon each dimension of the transaction is compared to the profiles – for instance, a high score for 'amount' indicates that the transaction transfers an uncommon amount of money. Based on this set of single score values, an overall score is computed. If this overall score exceeds a given boundary value, the transaction is classified as fraudulent. An alert prompts the analyst to check the transaction and to decide, based on his/her experience, if this is indeed a case of fraud or if this is a false alarm. This is mainly aims reduce the number of false alarms and increase the quality of the query by adding human interaction and cognition in the fraud discovery loop. Yet, there are no VA approaches to aid the task of profile analysis in fraud detection. This task is usually supported by machine learning techniques used to generate the profiles. To fill the current lack of VA support in profile analysis, we propose a VA approach to support the exploration of customer profiles to aid reasoning as well as the adaption and fine tuning of the fraud detection system (i.e., the transaction evaluation system).

Johnatan S. Oliveira, et al., [3] In this work, besides of collecting the large FaceBank dataset with real banking face images of selfies and ID documents, here also put in force a robust method for pass-domain face matching based totally on two properly-referenced Convolutional Neural Networks (CNN), VGG-Face [5] and OpenFace [6], to extract deep and sturdy capabilities from the faces, with properly level of invariance to the domain variations. We also applied normalization techniques to the facial images and to their feature vectors to attenuate such issues even more and improve the model performance. After normalizing the selfies and IDs, extracting and normalizing their deep feature vectors using the VGG-Face [5] or OpenFace [6] CNN models, we trained and assessed four classifiers (Linear Support Vector Machine - Linear SVM [18], Power Mean SVM - PmSVM [19], Random Forest - RF [20], and RF with Ensemble Vote Classifier - Voting RF [21]) in order to verify which one performed better in the task of classifying a pair of face images (ID and selfie) as genuine or imposter and compare their results in the banking context.

T. Suganya, et al., [4] This device proposes the amalgamation of Face Recognition System inside the identity verification procedure engaged in ATMs to beautify the safety gadget. The face detector spot the face, getting rid of any other detail, now not associated with the face (just like the backdrop). It identifies the facial area and leaves the non-facial region within the image of the individual to be recognized. Various facial reputation algorithms be familiar with faces by means of extracting capabilities, from a snap of the problem's face. For example, an algorithm may look at the dimensions, relative position, similarly to/or define of the nose, eyes, cheekbone and jaw. These facial appearances are then used to look for other imagery across matching capabilities. Other algorithm manage a balcony of face pictures and then compress the picture‟s face statistics and it saves simplest the records inside the image this is used for face detection. A searched photo is then compared with the face file. Facial

verification software is at gift as much as the project of supplied that essential healthy quotes for use in ATM transactions. Adding up facial popularity structures to the identification affirmation process utilized in ATMs can reduce forged transactions to a exquisite quantity.

Olutola Fagbolu, et al., [5] Proposed a more secured ATM can be designed and implemented with more secured feature of biometrics- facial recognition as PIN. Security is an indispensable problem in banking operations; with the advent of technology such as e-banking, mobile banking etc security has become an issue that needs utmost paramountcy. Principal Component Analysis (PCA) are employed in face recognition system, it seeks to capture the variations in a collection of face images and use them to encode and compare images of all individual faces by using statistical dimensionality reduction method to produce the optimal linear squares decomposition of a training set and eigen faces. The research has shown that ATM users have encountered many problems in the past which the research work has offered solutions to. But for the scope of this research, further works could be considered in the area of integrating virtually all the biometric measures into a single system. This will invariably ensure maximum security in all ATM-related transactions and drastically reduce frauds and to overcome all the aforementioned problem it is advisable that government partner with banking sector to use biometric techniques "face-based access control" in ATMs as it will eradicate the problems associated with smartcard access control.

III. Existing Methodologies

Online Protection stays a task to make certain safe transacting on the net. User authentication, a human-centric process, is seemed as the idea of computer protection and consequently comfortable get right of entry to to on-line banking services. The elevated use of era to implement extra movements has the ability to improve the satisfactory of authentication and hence on-line security, however often at the rate of usability. Today, there are some of technology in use to combat fraud in the banking industry. One of those is the usage of One Time Passwords (OTPs), which is a fraud prevention era specific for e-banking transactions. The most basic technique shows a time-dependent code that a consumer is required to input into the banking interface. Smart cards and USB tokens are different security features employed with the aid of banks that paintings with the aid of verifying the user via their possession of a clever card or USB tool. The problem is that each one present safety features gift one mission or the alternative. Transaction tracking is a specific kind of technique that comes from an variation of credit/debit card fraud prevention systems. This approach analysis the sender and receiver of the transaction and compares with recognized fraud styles. This approach requires no extra hardware for the user as all analysis is achieved in the historical past. However, this too comes with its risks, as there can be a loophole in the machine while new fraud patterns occur earlier than they're detected. Also, on occasion true transactions could be forwarded to call centers which then inconvenience customers.

Face classification using icp and knn classification

Online banking is now very popular amongst customers because it gives a convenient manner to perform transactions from everywhere the use of smart gadgets. Now a days thieves are the usage of excessive tech techniques to benefit get entry to to person records together with passwords, PINs and safety questions. This mission objectives at improving the security of Internet banking machine with additional face biometric Authentication combination. Internet banking now makes use of Static User ids and passwords at the side of OTP-One time Passwords to cellular range. Although this is the satisfactory security function to be had up to now,

this security technique continues to be prone and it is very essential to decorate the present protection. The time period biometrics refers back to the rising field of era devoted to the identity of individuals the usage of organic behaviors. Biometrics is a powerful combination of science and technology that may be used to shield and comfy our maximum precious information. Biometrics isn't into Internet banking packages yet. It is due to the realistic difficulties and it's miles very luxurious to put in force and execute this technology. But, now with era development and cost of Biometric gadgets coming down, we've probabilities to combine Biometric Technology to Online Banking. Face biometric can be used to provide value powerful rather than other biometric capabilities such as fingerprint, iris and other features. And also amplify the process to implement the machine with multiparty get admission to. The user of the account is considered as number one person. The number one user gives the permission to get entry to account to different individuals considered as secondary customers. The primary consumer set the restriction for secondary get right of entry to. At the time of login verification, face may be recognized as whether or not it's miles primary or secondary. The OTP based totally password may be send at the time transactions. Finally SMS alert send to primary consumer with detail description of consumer name, time of access, amount details. Session time evaluation can be used prevent from infrequent get right of entry to.

IV. ALGORITHM

ITERATIVE CLOSEST POINT ALGORITHM:

In The Iterative Closest Point or, in some resources, the Iterative Corresponding Point, one point cloud (vertex cloud), the reference, or target, is saved constant, at the same time as the other one, the source, is converted to exceptional suit the reference. The set of rules iteratively revises the transformation (aggregate of translation and rotation) had to minimize an errors metric, usually the gap from the supply to the reference factor cloud. ICP is one of the widely used algorithms in aligning three dimensional fashions given an initial guess of the inflexible body transformation required. Given 2 points r1 and r2 , the Euclidean distance is:

Taken a point r_1 and set of points A , the Euclidean distance is:

$$d(r_1, r_2) = \|r_1 - r_2\| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}$$

$$d(r_1, A) = \min_{i \in 1..n} d(r_1, a_i)$$

The shape extracted from scene S is aligned to be in the best alignment with the model shape M.
The distance of each point s of the scene from the model is calculated using:

$$d(s, M) = \min_{m \in M} d\|m - s\|$$

Algorithm steps as follows:

Input: Face Image
Output: Detected closest feature points

Processing Steps:

Step 1: function ICP (Scene, Model)

Step 2: begin
E` ← + ∞;
(Rot, Trans) ← In Initialize-Alignment (Scene, Model);

Step 3: repeat
E ←E`;
Aligned-Scene ← Apply-Alignment (Scene, Rot, Trans);
Pairs ← Return-Closest-Pairs (Aligned-Scene, Model);
(Rot, Trans, E`) ← Update
Alignment (Scene, Model, Pairs, Rot, Trans);

Step 4: Until |E` - E| < Threshold
return (Rot, Trans);

end

KNN CLASSIFICATION ALGORITHM:

The k-nearest neighbor set of rules (k-NN) is a technique for classifying gadgets based on closest training examples inside the feature space. K-NN is a kind of example-based totally learning, or lazy getting to know in which the characteristic is simplest approximated locally and all computation is deferred until classification. The k-nearest neighbor set of rules is amongst the handiest of all device getting to know algorithms: an item is assessed through a majority vote of its neighbors, with the object being assigned to the elegance most common amongst its okay nearest associates (okay is a positive integer, usually small). If k = 1, then the object is actually assigned to the class of its nearest neighbor.

1. Each facts pixel fee within the facts set has a class label in the set, Class = c1,...,cn.

2. The facts points', k-closest pals (ok being the quantity of friends) are then discovered with the aid of reading the distance matrix.

3. The k-closest facts points are then analyzed to determine which class label is the most commonplace among the set.

4. The maximum not unusual elegance label is then assigned to the information factor being analyzed.

Processing Steps

Input: Face image with extracted features.

Output: Classification for authority checking.

Processing Steps:

Step 1: Calculate "d(x, x_i)" i =1, 2, ….., **n**; where **d** denotes the Euclidean distance between the points.

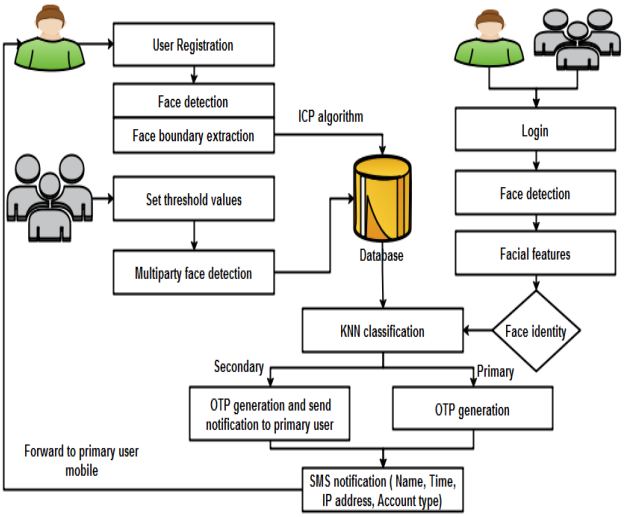
Step 2: Arrange the calculated **n** Euclidean distances in non-decreasing order.

Step 3: Let **k** be a +ve integer, take the first **k** distances from this sorted list.

Step 4: Find those **k**-points corresponding to these **k**-distances.

Step 5: Let k_i denotes the number of points belonging to the i^{th} class among **k** points i.e. $k \geq 0$

Step 6: If $k_i > k_j \; \forall \; i \neq j$ then put x in class i.



The proposed work is illustrated in fig 4.

V. EXPERIMENTAL RESULTS

Experimental results have the results of the proposed work. Proposed work was implemented using C#.NET is a front end and SQL is a back end process. Experimental result shows that the proposed work achieves higher security in banking with multi party access control system.

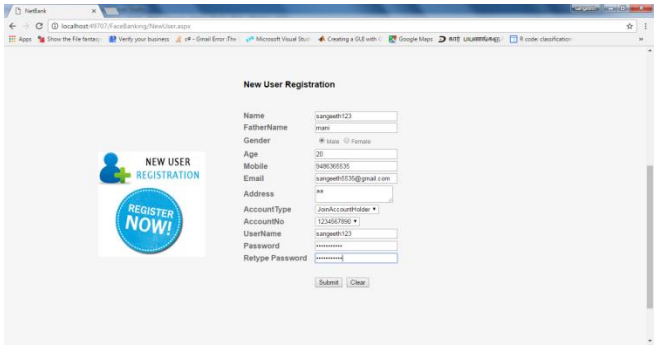


Fig 5.1 : Account Creation

Above figure shows the process of account creation. Here, user details are entered and stored on database for further verification.

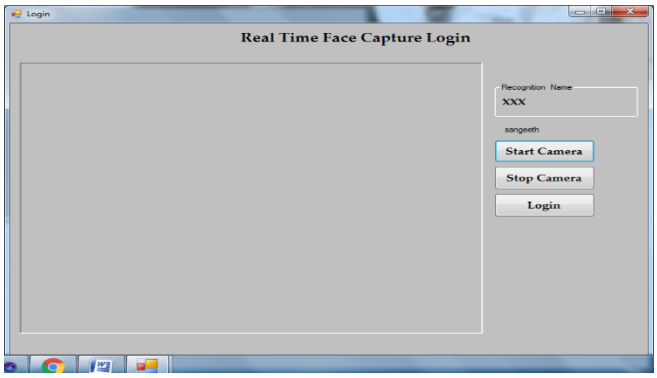


Fig 5.2 : Face Detection Module

This figure shows the face detection module. Here user face image is captured in real time. Then extract the facial features using ICP. Extracted features are labeled then stored on database.

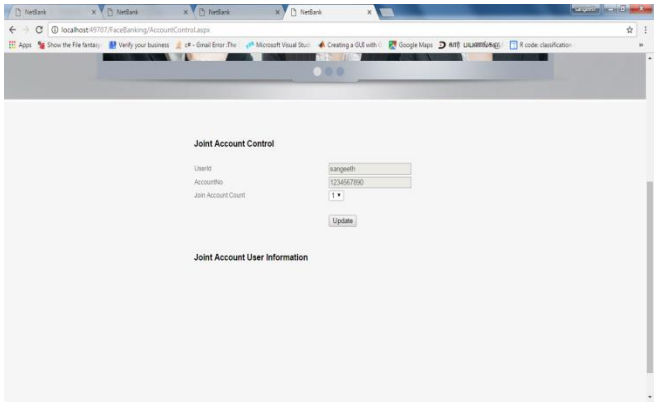


Fig 5.3 : Multi Party Access

This figure shows the multi party access system. Here primary account holder should mention the details of secondary account holder for account access.

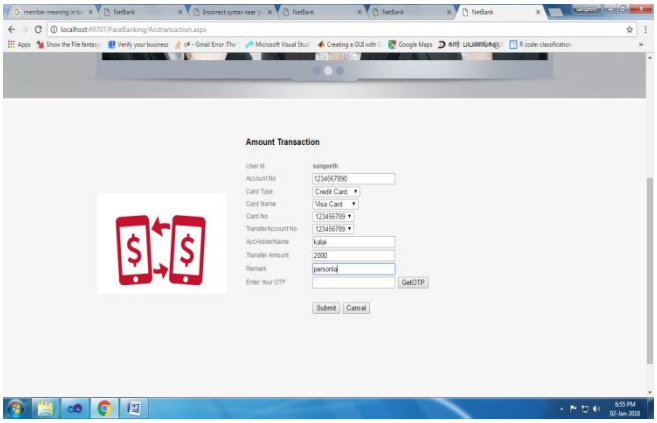


Fig 5.4 : Amount Transaction

Above figure shows the amount transaction details. User should enter the details like account number, card number, card type and amount details. Then OTP will be generating to verify the current transaction.

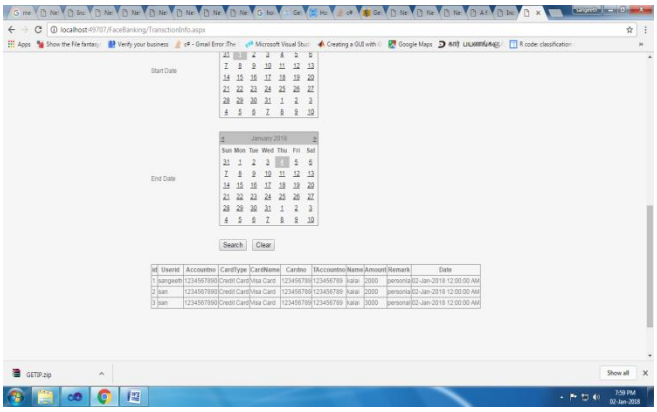


Fig 5.5 : Transaction Report

This figure shows the transaction details. Here admin can view the transaction details based on specific date.

VI. CONCLUSION

Biometric technology gives better safety whilst being handy to use. It ensures that statistics is accessed simplest via legal humans. The security system offers a dependable approach for authenticating users. It is strong answer to satisfy the stringent requirements of

restrained access for pinnacle secret records. Significantly, it reduces frauds and minimizes password administrator fees. When biometric technology is going principal-stream, banks can use biometrics in each transaction requiring the authentication of identity. Iris popularity is one of the maximum accurate protection systems to pick out a completely unique consumer, right away and quite simply. As the level of security breaches and transaction frauds growth day by day, the want for distinctly secure identity and personal verification information structures is turning into extremely essential particularly inside the banking and finance quarter. In this paper, we will put into effect face popularity device to on line net-banking application in IOT environments. Face Recognition capabilities can be used to make internet-banking structures more at ease for authentication purpose in banking primarily based safety systems. The ID can be stolen; passwords may be forgotten or cracked but the physical characteristics of someone can not be stolen or hacked. The Face Recognition identification overcomes all the above. And additionally provide multi-man or woman access control to offer get entry to privileges to users with progressed protection. Real time alert system about unauthorized access of entry to and multi party access system.

VII. REFERENCES

[1]. Visual Analytics for Fraud Detection and Monitoring Author: Roger A. Leite, Theresia Gschwandtner, Silvia Miksch, Erich Gstrein, and Johannes Kuntner Year: 2013

[2]. Visual Analytics for Fraud Detection: Focusing on Profile Analysis Author: Roger Almeida Leite, Theresia Gschwandtner, Silvia Miksch, Erich Gstrein & Johannes Kuntner Year: 2016

[3]. Data visualization for fraud detection: Practice implications and a call for future research Author: William N. Dilla a, Robyn L. Raschke b Year: 2015

[4]. Cross-Domain Deep Face Matching for Real Banking Security Systems Authors:Johnatan S. Oliveira, Gustavo B. Souza, Anderson R. Rocha, Flavio E. Deus and Aparecido N. Marana Year: 2018

[5]. Securing ATM by Image Processing – Facial Recognition Authentication, Authors: T. Suganya, T. Nithya C. Sunitha, B. Meena Preethi, Year: 2015

[6]. Secured Banking operations with face-based Automated Teller Machine, Authors: Olutola Fagbolu1, Olumide Adewale2 Boniface Alese2and Osuolale Festus2, Year: 2014

[7]. Face Detection based Locker Security System using Raspberry Pi Authors:Sandeep V, Guruprasad Hegde , Chetan N, Girish P Patil, Lad Bhavesh Year: 2016

[8]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787-2805, 2010.

[9]. S. Chen, H. Xu, D. Liu, and B. Hu, "A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective," IEEE Internet of Things Journal, vol. 1, no. 4, pp. 349-359, 2014.

[10]. H. Ning, H. Liu, J. Ma, L. T. Yang, and R. Huang, "Cybermatics: Cyberphysical- social-thinking hyperspace based science and technology," Future Generation Computer Systems, vol. 56, pp. 504-522, 2016.

[11]. T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, "Heterogeneous ad hoc networks: Architectures, advances and challenges," Ad Hoc Networks, vol. 55, pp. 143-152, 2017.

[12]. Yu, Lei, et al. "CoRE: Cooperative end-to-end traffic redundancy elimination for reducing cloud bandwidth cost." IEEE Transactions on Parallel and Distributed Systems 28.2 (2017): 446-461.

[13]. J. Yuan and S. Yu, "Efficient privacy-preserving biometric identificationin cloud computing," in

2013 Proceedings IEEE INFOCOM, 2013, pp. 2652-2660.

[14]. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A Privacy- Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2594-2608, 2016.

[15]. K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh, "On security and privacy issues of fog computing supported Internet of Things environment," in 2015 6th International Conference on the Network of the Future (NOF), 2015, pp. 1-3.

Cite this article as :

V. Manju, S. Madhumathi, "Improving Net Banking Security with Face Recognition Based Bio-Metric Verification", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 82-91, May-June 2019.
Available at
doi : https://doi.org/10.32628/CSEIT195335
Journal URL : http://ijsrcseit.com/CSEIT195335