International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 880-884 www.ijaem.net ISSN: 2395-5252

Privacy Preserving User Centric Fingerprint Biometric Authentication System

Prof .R.Abinaya B.E., M.E.,[1] Assistant Professor, S.Anbarasan,[2] K.Muruganantham,[3] T.Partha Sarathy,[4] K.Nagaraj[5]

Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur.

Submitted: 05-05-2021 Revised: 17-05-2021 Accepted: 20-05-2021

ABSTRACT: In this highly advancing digital world the level of security is getting breached and also the transaction fraud has increased. Existing security measures rely on knowledge based approaches like passwords, PIN numbers or token based approaches like passports, swipe cards. Such methods are not very secure. These can be easily accessed through number of ways for example by stealing or by sharing etc. Furthermore it is quite impossible to differentiate between authorized user and the person having access to the tokens or passwords. Biometric-based authentication is the perfect solution for this problem. Fingerprints are impression of the friction ridges of the finger. They are used as biometric feature for person identification and verification in the field of biometric identification. In spite of decades of research in fingerprints, reliable finger print recognition is still an open problem. Minutia based fingerprint recognition algorithms have been widely accepted as a standard for single finger recognition applications. This technology has proved to be a reliable form of enrollment and matching in a corporate environment under ideal circumstances. In this project, we present an efficient privacy-preserving fingerprint authentication system using Euclidean distance scheme in which fingerprint data are always stored and processed in an encrypted form. We implement a fully working fingerprint authentication system with a fingerprint database.

I. INTRODUCTION

1.1 BIOMETRICS

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are then distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behavior-metrics to describe the latter class of biometrics.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information

II. LITERATURE SURVEY

2.1 Title: Biohashing: Two Factor Authentication Featuring Fingerprint Data And Tokenised Random Number

Author: A. T. B. Jin

Human authentication is the security task whose job is to limit access to physical locations or computer network only to those with authorization. This is done by equipped authorised users with passwords, tokens or using their biometrics. Unfortunately, the first two suffer a lack of security as they are easy being forgotten and stolen; even biometrics also suffers from some inherent limitation and specific security threats. A more practical approach is to combine two or more factor authenticator to reap benefits in security or convenient or both. This paper proposed a novel two factor authenticator based on iterated inner products between tokenised pseudo-random number and the user specific fingerprint feature, which generated from the integrated wavelet and Fourier–Mellin transform, and hence produce a set of user specific compact code that coined as BioHashing. BioHashing highly tolerant ofdata capture offsets, with same user fingerprint data resulting in highly correlated bitstrings. Moreover, there is no deterministic way to get the user specific code without having both token with random data and user fingerprint feature. This would protect us for instance against biometric fabrication by changing the user specific credential, is as simple as changing the token containing the random data. The BioHashing has significant functional advantages over solely biometrics i.e. zero equal error rate point and clean separation ofthe genuine and imposter populations, thereby allowing elimination of false accept rates without suffering from increased occurrence of false reject rates.

DRAWBACKS:

- Difficult to separate the genuine and fake users

2.2 TITLE: GENERATING CANCELABLE FINGERPRINT TEMPLATES
AUTHOR: N. K. RATHA, S. CHIKKERUR

Securing information and ensuring the privacy of personal identities is a growing concern in today’s society. Traditional authentication schemes primarily utilize tokens or depend on some secret knowledge possessed by the user for verifying his or her identity. While these techniques are very popular, they have several limitations. Both token and knowledge-based approaches cannot differentiate between an authorized user and a person having access to the tokens or passwords. In case of knowledge-based authentication systems, managing multiple passwords (i.e., identities) presents usability problems. Biometrics-based authentication schemes using fingerprints, face recognition, etc., overcome these limitations while offering usability advantages and are therefore rapidly extending traditional authentication schemes. Biometrics-based authentication systems offer obvious usability advantages over traditional password and token-based authentication schemes. However, biometrics raises several privacy concerns. A biometric is permanently associated with a user and cannot be changed. Hence, if a biometric identifier is compromised, it is lost forever and possibly for every application where the biometric is used. Moreover, if the same biometric is used in multiple applications, a user can potentially be tracked from one application to the next by cross-matching biometric databases. In this paper, we demonstrate several methods to generate multiple cancelable identifiers from fingerprint images to overcome these problems. In essence, a user can be given as many biometric identifiers as needed by issuing a new transformation “key.” The identifiers can be cancelled and replaced when compromised. We empirically compare the performance of several algorithms such as Cartesian, polar, and surface folding transformations of the minutiae positions. It is demonstrated through multiple experiments that we can achieve revocability and prevent cross-matching of biometric databases.

DRAWBACKS:

- Performance is low at the time of verification

III. SYSTEM ANALYSIS

EXISTING SYSTEM

In present system for ATM banking,the user opens his account using his login which contains a username and the password provided by the bank for first time logging in. After opening the account he/she can compose of his own password. When logging in every time he/she has to enter the username and password for accessing the account. After opening the account for doing transaction the user has to enter a one time password (OTP) which will be send by the bank to the user mobile number. Once the OTP is entered the transaction is done successfully. Complex encryption software is used to protect account information. However, there are no perfect systems. Accounts are prone to hacking attacks, phishing, malware and illegal activities. Learning – Banks with complicated sites can be cumbersome to navigate and may require one to read through tutorials to navigate them. Transaction problems – face to face meeting is better in handling complex transactions and problems. Customary banks may call for meetings and seek expert advice to solve issues. User-ID and password can be captured using Trojan Horse programs. And also in existing system use single fingerprint recognition system to secure transactions. Fingerprint templates are stored in database and easily hacked by third parties. Then extend the approach to use mixed fingerprint templates are recognized, but difficult to separate the templates of fingers.

DISADVANTAGES

- An impostor steals the Hash key or the pseudo-random numbers of a party
- Still not practical for arbitrary arithmetic computation over encrypted data
- Accuracy is less to implement distance based authentication
- Time complexity is high

IV. PROPOSED SYSTEM

Banking is not only focused on transferring money, but also to conduct many banking transactions with minimum time. Banking means any user can get connected to his bank's system with personal computer. But many hacking process is done in banking. To avoid these problems, novel algorithm has been developed for secure internet banking with finger print recognition. Therefore, there should be strong authentication provided for the Transaction process. Our system provides this authentication by using the biometrics of the User. The biometrics is in the form of Fingerprint of the user. In our system along with the Username and Password of the User he needs to provide his double fingerprints biometric for the transaction. For this the bank initially stores all the user details along with his double fingerprints. Our system will check for the biometrics of the user and match it with the original biometrics stored in the bank's Database. In this database, we can store the fingerprint features such as island, ridge end, and core and delta values. These are maintained for double fingerprints instead of templates. If a valid match is found then only the user is Authenticated and treated as valid. Otherwise even if there is a small mismatch in the fingerprint the user is not allowed to access the Bank Account. The matching can be done using neural network algorithm to authenticate people who want to accede to an automated fingerprint system for Banking. The idea is to apply back propagation algorithm on a multilayer perceptron during the training stage. One of the advantages of this technique is the use of a hidden layer which allows the network to make comparison by calculating probabilities on template which are invariant to translation and rotation. Our system mainly focuses on the objective to provide security for online transaction and to see that the valid User should always get access to his account without any inconvenience.

ADVANTAGE

- Proposed system can be reduce false acceptance rate
- Extend the framework to implement in sensors to capture biometrics in real time
- Improved accuracy
- Time and computational complexity can be reduced

SYSTEM IMPLEMENTATION MODULE

- Fingerprint acquisition
- Finger features extraction
- Enrollment in database
- Authentication
- Features matching

V. MODULES DESCRIPTION

1 FINGERPRINT ACQUISITION:

In this module, image of Fingerprint is first acquired with the help of sensors. Captured images may be blurred or may contain noises, which Detroit the quality of an image and affect the performance of Fingerprint recognition system. The fingerprint image acquired may vary by location of finger placed, direction and stretching degree. After acquiring the image through sensors, preprocessing or image enhancement is done on the image. Sometimes image may contain noise while enrollment process, noise can be remove with help of filters utilized in processing/enhancement part of the processing. Sometimes there is a need of images normalization. A live-scan image is acquired by sensing tip of finger directly, using a sensor. Live-scan is done with the help of sensors. There are three types of sensors used. They are optical sensors, ultrasonic sensors and capacitance sensors. Our system uses Optical sensor (Fingerprint scanner).

2 FINGERPRINT FEATURES EXTRACTION:

An image, such as that of a fingerprint, may be considered as a two-dimensional continuous signal. By this, it can have an infinite number of brightness intensities in an infinitesimal area. In order for an image to be handled by a computer, it must first be digitized. For this study, the image had to be sampled in a different manner. In feature extraction phase, features of image are extracted such as Ridges, valleys, minutiae and singular points (loops, core, whorls and delta). These features are helpful for unique identification or verification of an individual. The features obtained from captured images are stored in database for further process of matching. The major minutia features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges.

3 ENROLLMENT IN DATABASE

In this module, fingerprint features are stored in database. We can store double fingerprint entity for improved authentication. Then we stored these features numerical values instead of templates. These featured are saved along with registered details such as name, id, phone number, email and so on. The procedure to store the data as

4 AUTHENTICATION

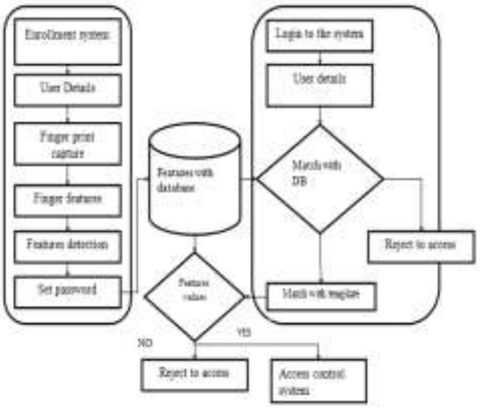
This phase is known as login phase. User can enter into the system using user name and password. After that sensing fingerprints of same person with sub sequence press. Minutiae matching are required to check whether the input image is same as that stored in the bank database. Minutiae matching can be done using different techniques as Point matching i.e. the matching is done by comparing pixel by pixel. One pixel from the input image is taken and compared with one pixel from the reference image, Segment Creation the minutiae points extracted from the stage II are connected with each other using segments. The distance between each segment is calculated for both query and reference images.

5 FEATURES MATCHING

Feature matching phase identifies similarities between current fingerprints features and previously stored features. Input images provided to the system are matched with previously stored features present in database. Matching is entirely dependent on whether the system Performs identification or verification. If it performs identification i.e. one-to-many matching approach is used, where fingerprint of an individual matches with all available templates in database otherwise one-to-one match is done for verification, where input image of a person is matched with double fingerprint features. It can be done by back propagation neural network algorithm which is the standard way of training neural networks. It works basically like this: The input pattern on which the network is to be trained is presented at the input layer of the net and the net is run normally to see what output it actually does produce. The actual output is compared to the desired output for that input pattern. The differences between actual and desired form an error pattern. Extract the features for both fingers at testing side. These features are matched with data base using classification approach. If there is match found means, user can be register into system, otherwise rejected

VI. SYSTEMDESIGN

SYSTEM ARCHITECTURE



SOFTWARE DESCRIPTION

.NET FRAMEWORK

The .NET Framework (pronounced dot net) is a software framework developed by Microsoft that runs primarily on Microsoft Windows. It includes a large library and provides language interoperability (each language can use code written in other languages) across several programming languages. Programs written for the .NET Framework execute in a software environment (as contrasted to hardware environment), known as the Common Language Runtime (CLR), an application virtual machine that provides services such as security, memory management, and exception handling. The class library and the CLR together constitute the .NET Framework.

SYSTEM TESTING

Software testing is a method of assessing the functionality of a software program. There are many different types of software testing but the two main categories are dynamic testing and static testing. Dynamic testing is an assessment that is conducted while the program is executed; static testing, on the other hand, is an examination of the program's code and associated documentation. Dynamic and static methods are often used together.

Testing is a set activity that can be planned and conducted systematically. Testing begins at the module level and work towards the integration of entire computers based system. Nothing is complete without testing, as it is vital success of the system.

Testing Objectives:

There are several rules that can serve as testing objectives, they are

1. Testing is a process of executing a program with the intent of finding an error

2. A good test case is one that has high probability of finding an undiscovered error.

3. A successful test is one that uncovers an undiscovered error.

Tests used for implementation efficiency attempt to find ways to make a correct program faster or use less storage. It is a code-refining process, which reexamines the implementation phase of algorithm development. Tests for computational complexity amount to an experimental analysis of the complexity of an algorithm or an experimental comparison of two or more algorithms, which solve the same problem.

The data is entered in all forms separately and whenever an error occurred, it is corrected immediately. A quality team deputed by the management verified all the necessary documents and tested the Software while entering the data at all levels. The development process involves various types of testing. Each test type addresses a specific testing requirement.

VII. CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

We have implemented a system for providing strong authentication for online banking transactions using fingerprint biometrics. Fingerprint recognition has various phases as image enrollment, preprocessing or enhancement, feature extraction and matching. The singular points are quite frequently features for classification. In a similar fashion, the rule based and neural network classifiers have been frequently used. It describes in brief about the enhancement, extraction and matching of fingerprint images. It contains the details of types of biometrics, its advantages over password/key authentication. It briefs about the image pre-processing techniques. The method has been used for feature extraction of minutiae. This method is able to detect accurately all valid bifurcations and ridge endings from the thinned image. For matching purpose back propagation neural network algorithm, has been trained as a fingerprints classifier to identify fingerprints with time effective preprocessing, which greatly increases the performance of the network. The recognition rate of fingerprints depends on the quality of fingerprints and effectiveness of preprocessing system. In this, input minutiae are aligned with the template by estimating the parameters between an input and features. The input which satisfies the matching score is declared as a matched fingerprint with the features

FUTURE ENHANCEMENTS

Nowadays everyone is using Internet on mobiles. So we can develop an android App for scanning the fingerprint biometric. We can use our inbuilt mobile camera for capturing fingerprint image and build up algorithms for improving the image enhancement

REFERENCES

[1]. A. T. B. Jin, D. N. C. Ling, and A. Goh, “Biohashing: two factor authentication featuring fingerprint data and tokenised random number,” Pattern Recognition, vol. 37, no. 11, pp. 2245–2255, 2004.

[2]. A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, “An analysis of biohashing and its variants,” Pattern Recognition, vol. 39, no. 7, pp. 1359–1368, 2006.

[3]. N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, pp. 561–572, 2007.

[4]. C. Lee, J.-Y. Choi, K.-A. Toh, S. Lee, and J. Kim, “Alignment-free cancelable fingerprint templates based on local minutiae information,” IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 37, no. 4, pp. 980–992, 2007.

[5]. M. Ferrara, D. Maltoni, and R. Cappelli, “Noninvertible minutia cylinder-code representation,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1727–1737, 2012.

[6]. C. Li and J. Hu, “A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 543–555, 2016.

[7]. A. Ross and A. Othman, “Visual cryptography for biometric privacy,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70–81, 2011.

[8]. A. Nagar, K. Nandakumar, and A. K. Jain, “Biometric template transformation: A security analysis,” in Proceedings of SPIE, 2010.

[9]. K. Simoens, C. Chang, and B. Preneel, “Reversing protected minutiae vicinities,” in Proceedings of IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2010

[10]. A. Othman and A. Ross, “On mixing fingerprints,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 260–267, 2013.