National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

On the Role of Finger Scanning in Fully Secured Online Transactions

V. Sarada Swetha[1], S. Ramu[2], U.V. Harika[3], U. V. S. Seshavatharam[4]

[1]HCL technologies, Flat No-304, Sangeeth Nagar, Kukatpally, Hyderabad, Andhra Pradesh, India

[2]SBI cards, Flat No-304, Sangeeth Nagar, Kukatpally, Hyderabad, Andhra Pradesh, India

[3] Department of ECE, S. V. Engineering College for Women, Tirupati, Andhra Pradesh, India

[4]Honorary Faculty, I-SERVE, Survey no-42, Hitech city, Hyderabad, Telangana, India

ABSTRACT

By registering user's smart phone and finger prints in the respective banks and by allowing a suitable decision making timer in online transactions - to the possible extent, online frauds can be minimized. Considering finger prints and virtual card system, online ease and security can be enhanced further.

I. INTRODUCTION

Nowadays, as smart phones are growing in number, day by day banking transaction number is also increasing. Parallel to this, online fraud activities are also increasing in number. To minimize and prevent the online fraud activities, we are working on implementing 'Online Finger Scanning' procedure.

II. Basic action plans

We propose the following action plans.

1) To register the smart phone device number [1] in the bank.
2) To register finger prints [2, 3] in the bank via the registered smart phone.
3) To initiate finger scanning for final approval of the online transactions [4, 5] through the registered mobile device.
4) To make some pre-defined and suitable time delay for each online transaction so that final online transaction approval decision can be made flexible.
5) Making debit cards and credit cards virtual.

III. Uses of the proposed action plans

With respect to the above action plans, collectively it is possible to say that,

1) User is restricted to make successful online transactions through his/her smart device only.
2) Online transactions cannot be made successful without finger prints.
3) User's credit or debit card cannot be handled by other users.
4) Even though scammers [6] are able to get one time passwords from victimized users, as the user is far away from the scammer and user finger prints are not being accepted by scammer's device, in any case, false transactions cannot be made successful.
5) In case of non-finger scanning, as there is a time

delay in finalizing any online transaction, as fraudster is supposed to wait for some time, mean while victimized user can become normal and can take a wise decision in stopping the supposed false transaction.

6) User can have a strong hold on his/her credit or debit card.
7) Apart from helping the user in activating the mobile device, finger scanner of the mobile device can be allowed to have a key role in securing the online transactions and thus finger scanner can be used to its full potential.
8) For a group of users or members of a family and joint bank account holders, with some flexibility in the above said action plans, online transactions can be made successful at their personal risk and understanding.
9) By making credit and debit cards virtual,
   a) There is no need for the user to carry any debit or credit card physically.
   b) There will be no point of damage of cards, misplacing of cards, forgetting of cards, loss of cards, thefting of cards.
   c) In case of any forced handling of any user by any scammer, it takes a long time for the scammer to find and operate the virtual card.
   d) In a phased manner, all debit and credit cards of any user can be made into a single virtual card with different set of codes.
10) Personal computers and laptops can also be equipped with finger scanning system and thereby online transactions can be made further secure and ease.
11) Switching and activating of personal computers and laptops with finger scanning helps in their secured time to time operations.
12) In a phased manner, one time password scheme can be eliminated.
13) Finger scanning can slowly be replaced with Eye scanning for ease and further secured online transactions.

IV. Mechanism

To register the smart phone IMEI number in the bank

The International Mobile Equipment Identity is generally a 15 digit code and is represented by IMEI. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dial pad or alongside other system information in the settings menu on smart phone operating systems. GSM networks use the IMEI number to identify valid devices and can stop a stolen phone from accessing the network. For example, if a mobile phone is stolen, the owner can have their network provider use the IMEI number to blacklist the phone. This renders the phone useless on that network and sometimes other networks, even if the thief changes the phone's subscriber identity module (SIM).

Devices without SIM card slot usually don't have the IMEI code. However, the IMEI only identifies the device and has no particular relationship to the subscriber. The phone identifies the subscriber by transmitting the International mobile subscriber identity (IMSI) number, which it stores on a SIM card that can, in theory, be transferred to any handset. However, the network's ability to know a subscriber's current, individual device enables many network and security features.

Many countries have acknowledged the use of the IMEI in reducing the effect of mobile phone thefts. For example, in the United Kingdom, under the Mobile Telephones (Re- programming) Act, changing the IMEI of a phone, or possessing equipment that can change it, is considered an offence under some circumstances. In the United States, changing the IMEI of a phone is not illegal. IMEI blocking is not the only way to fight phone theft. Australia was the first nation to implement IMEI blocking across all GSM networks, in 2003.

Keeping these points in view we emphasize that, based on the number of SIM(s), user must register IMEI number(s) in all of the respective banks in which user is having a valid accounts.

b) To register finger prints in the bank

A “fingerprint” is an impression left by the friction ridges of a human finger. The recovery of partial fingerprints from a crime scene is an important method of forensic science. Moisture and grease on a finger result in fingerprints on surfaces such as glass or metal. Deliberate impressions of entire fingerprints can be obtained by ink or other substances transferred from the peaks of friction ridges on the skin to a smooth surface such as paper. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. They may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster.

Since the late nineteenth century, fingerprint identification methods have been used by police agencies around the world to identify suspected criminals as well as the victims of crime. The basis of the traditional fingerprinting technique is simple. The skin on the palmar surface of the hands and feet forms ridges, so-called papillary ridges, in patterns that are unique to each individual and which do not change over time. Even identical twins who share their DNA do not have identical fingerprints. The best way to render latent fingerprints visible, so that they can be photographed, can be complex and may depend, for example, on the type of surfaces on which they have been left. It is generally necessary to use a ‘developer', usually a powder or chemical reagent, to produce a high degree of visual contrast between the ridge patterns and the surface on which a fingerprint has been deposited. The human skin itself, which is a regenerating organ until death, and environmental factors such as lotions and cosmet cs, pose challenges when fingerprinting a human.

In the Henry Classification System there are three basic finger print patterns: loop, whorl, and arch, which constitute 60–65 percent, 30– 35 percent, and 5 percent of all fingerprints respectively. There are also more complex classification systems that break down patterns even further, into plain arches or tented arches, and into loops that may be radial or ulnar, depending on the side of the hand toward which the tail points. Ulnar loops start on the pinky-side of the finger, the side closer to the ulna, the lower arm bone. Radial loops start on the thumb-side of the finger, the side closer to the radius (bone). Whorls may also have sub- group classifications including plain whorls, accidental whorls, double loop whorls, peacock's eye, composite, and central pocket loop whorls.

Fingerprint image acquisition is considered to be the most critical step in an automated fingerprint authentication system, as it determines the final fingerprint image quality, which has a drastic effect on the overall system performance. There are different types of fingerprint readers on the market, but the basic idea behind each is to measure the physical difference between ridges and valleys.

All the proposed methods can be grouped into two major families: solid-state fingerprint readers and optical fingerprint readers. The procedure for capturing a fingerprint using a sensor consists of rolling or touching with the finger onto a sensing area, which according to the physical principle in use (optical, ultrasonic, capacitive, or thermal) captures the difference between valleys and ridges. When a finger touches or rolls onto a surface, the elastic skin

deforms. The quantity and direction of the pressure applied by the user, the skin conditions and the projection of an irregular 3D object (the finger) onto a 2D flat plane introduce distortions, noise, and inconsistencies in the captured fingerprint image. These problems result in inconsistent and non-uniform irregularities in the image. During each acquisition, therefore, the results of the imaging are different and uncontrollable. The representation of the same fingerprint changes every time the finger is placed on the sensor plate, increasing the complexity of any attempt to match fingerprints, impairing the system performance and consequently, limiting the widespread use of this biometric technology.

In order to overcome these problems, as of 2010, non-contact or touchless 3D fingerprint scanners have been developed. Acquiring detailed 3D information, 3D fingerprint scanners take a digital approach to the analog process of pressing or rolling the finger. By modelling the distance between neighboring points, the fingerprint can be imaged at a resolution high enough to record all the necessary detail.

Keeping all of the above difficulties in view, we emphasize that, time to time at regular intervals, users must register and validate their finger prints in the respective banks with proper care and proper scanners to have smooth online transactions.

c) To combine the set of registered IMEI number and registered finger prints in the bank.

Since online banking transactions are being initiated and encouraged by banks, bank teams should take initiative to combine, store and process the registered IMEI number and registered finger prints of any user in order to have smooth transactions. In future with this kind of approach, one time password scheme can be eliminated.

d) To make some delay in finalizing any transaction

Users can be given a chance to set a timer for final approving of any transaction. This timer can be in between half an hour to one hour. This can be useful in judging or assessing the final transaction. As so many products are coming into market, sometimes or most of the times, users may not be having sufficient awareness or knowledge on the product and user may be in a state of confusion in purchasing the item online. The pre set timer may help in taking a firm decision in assessing the purchasing item.

Sometimes, when users are being tampered by scammers, as the pre set time is unknown to the scammer, he is forced to wait for some time. Mean while, the victimized user may come to a normal position and pre set timer allows the user to understand the scammer's cheating.

e) Virtual debit cards and credit cards

Either the bank authority or any virtual card issuing authority team can take initiative in developing and maintaining virtual credit cards and debit cards. As per the information given by bank authorities, virtual card authorities will create and maintain the user's virtual credit cards and debit cards. During online transactions, user is prompted to choose the desired card. After selecting the card, user's credit card number, expiry date and relevant information will be processed by the banking application software automatically. There is no need to enter the card information manually. After processing the card information, user is asked to confirm the same to make online payment. To have an unique identity card, virtual card issuing authority will issue a permanent physical card to the user with Aadhar number as the primary identification number. By inserting the Aadhar card in any ATM, user is asked to scan the finger and further operations can be carried out in smooth manner.

In case of loss or misplacing or forgetting the Aadhar card, at any ATM, for a very limited number of transactions in any month, user is asked to type the Aadhar number. After typing the Aadhar number, again user is asked finger scanning.

V. Discussion

As many people are not aware of the subject matter of IMEI and Finger prints, on behalf of this paper, we request Wikipedia to permit us to reproduce a part of the information for better presentation and clarity.

First four action plans seem to have some ease and control in minimizing online frauds. But coming to the 5th action plan, there seems to have security problems and needs further study.

During a journey or kidnap or any case of manhandling or threatening or at any remote ATM, there is a possibility for forced operating of all the virtual cards at a time by scammers. To avoid this, further high security action plans are required and we are working in this direction. In this context,

a) At ATMs - camera, alarm, emergency button for blocking all ATM transactions etc can be arranged.

b) Online transactions can be split into Safe mode and Unsafe mode. Unsafe mode transactions takes a minimum of 24 hours and safe mode transactions depends on pre defined delay timers.

c) Journey time transactions and other expected unsafe transactions can be put under Unsafe mode.

d) With some flexible rules, unsafe mode transactions can be converted to safe mode.

e) Long hour car driving and bike riding transactions during night and remote areas, can be put under Unsafe mode at the beginning of journey itself.

f) Security levels can be increased on roads connecting remote areas.

g) User can take the help of any call center for unexpected emergency.

VI. CONCLUSION

If banking units and smart phone manufacturing units come forward to implement the above action plans, in a phased manner, certainly online scams can be minimized, fraudsters number can be reduced, bank money can be secured, user can avail the maximum benefits of credit and debit cards without any hindrance.

VII. Acknowledgements

Authors are thankful to the conference committee for encouragement. Authors are very much thankful to their well wishers, Mr. K.V.Sripathi, Mr. K.V.Srinivas, Mr. B. Vamsi Krishna and Mr. U.V.Hareesh for their encouragement and valuable guidance.

VIII. REFERENCES

[1]. GPP TS 22.016: International Mobile Equipment Identities (IMEI)" (ZIP/DOC; 36 KB). 2009-10-01. Retrieved 2009-12-03.

[2]. Wang, Yongchang; Q. Hao; A. Fatehpuria;

[3]. D. L. Lau; L. G. Hassebrook (2009). "Data Acquisition and Quality Analysis of 3- Dimensional Fingerprints". Florida: IEEE conference on Biometrics, Identity and Security.

[4]. Fingerprint Alteration Archived June 2, 2012, at the Wayback Machine Biometrics research group, Michigan State University.

[5]. “Online Transaction Processing vs. Decision Support". Microsoft.com. Retrieved 2018-05- 07.

[6]. https://ieeexplore.ieee.org/document/7724963/authors#authors

[7]. https://en.wikipedia.org/wiki/Internet_fraud

Cite this article as : V. Sarada Swetha, S. Ramu, U.V. Harika, U. V. S. Seshavatharam, "On the Role of Finger Scanning in Fully Secured Online Transactions", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 127-131, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194723