Analysis of User Authentication Methods & Impact on Identification Especially in Banking

Abdul Samad Shaikh
Department of Computer Science & IT
GreenfoTech Education, Aurangabad, India
email:- *samadindia@gmail.com*

Mohammed Waseem Ashfaque
Department of Computer Science & IT
GreenfoTech Education, Aurangabad,India
email:- *waseem2000in@gmail.com*

Abstract- Today the web/online has become global way for people to communicate, transact, socialize and even do the business. Where everything is becoming online, internet-centric and 'E' enabled even the governance. Online transaction processing is a key element for every business / organization to run their activities smoothly and globally. Especially Banking and Financial organization are fully dependant on online transaction processing. But the biggest challenge in Online or E processing is Authentication of user and security. The first and foremost thing is to identify that the user requesting online is authentic and true. This is essential for every online transaction and cannot be ignored by anybody. Many technologies , methods, software's have been development for user authentication but 'login/password pair' and 'biometric signature' remains the leading and widely accepted method by industry. More advance way of authentication like Biometric Iris Reading, Thumb Impression Reading, Gesture Reading, Voice Recognition , Pattern based authentication and Tapping based login are being developed for identifying users and ensure his authenticity. But most popular and widely accepted authentication method still is 'login/password pair' and 'signature' though not 100% secure and tamperproof. Emphasis should be given by researcher to improve this popular method to make it at least 99% foolproof besides inventing to new methods.

Keywords-*Authentication; Security; User Login; Biometric; E-Banking; Identification, Password; Cryptography; Signature; Palm Vein Reading.*

*****

I. INTRODUCTION

In this age of Online World where everything is Online or becoming Online the greatest issue is still remains partially solved i.e. how to identify to user and perfectly authenticate him in a full proof manner. No method is 100% accurate and Full Proof to security threat of today. This paper analyses various user identification and authentication method being used today and what impact it has on identifying authentic user. To identify true authentic user without a mistake is real challenge and requirement of IT industry today. The industry has implementation numerous methods of Identification and Authentication of user typically from 'login/password' pair, Signature verification, Biometric Thumb Reading, Iris Reading to voice recognition and gesture reading. All have some or other flaws with less than 100% accuracy and are not fully secure to Fraud and other Security Threats. The various methods developed for Identification and Authentication of today are not fully Crack-resistant, Temper-resistant and do not automatically resist fraudulent usage of it. Let us see the following authentication methods popularly used in online and banking transaction today.

II. LITERATURE REVIEW

Authentication is the most important aspect in human life from the security point of view. Most of the existing mechanisms use the reference template for the final authentication. These templates are stored in the raw format or some encrypted format. There is possibility of getting this information by imposter and can change the information which leads to the leakage of information. If the authentication is not being done then there is compromise in security. The problem here is to authenticate using the information of the user without compromise in the security as well as the leakage of information of the individual. Authentication and User Identification are being leading technologies various research and solutions have been designed so far are good and accepted by industries. Researchers, Experts have been giving full attention to subjects about Online banking security, the research include Framework for the Governance of Information Security in Banking System[10] and the security issues Internet banking are facing today and solutions for online banking security threats. TC. Shan and WW. Hua summed up security issues in two categories: system security issues and information security issues [11] and the corresponding solutions are cryptography, identity authentication and the data transmission protection technology [12][13][14].Researchers also described current authentication threats and proposed solutions and new authentication protocol for online banking [15][16]and introduced new approaches for online banking security[17]. The survey conducted by Data Security Council of India (DSCI) in 2010 indicates that the focus of the data governance processes so far has focused on integrity of data, but there is a need to increase efforts in the direction of data privacy [18]. Laura Falk et. al found that 76% of the sites in their survey suffered from at least one design flaw that are not widely understood, even by experts who are responsible for web security and they present and discussed methodology for testing websites[19]. Kenneth Edge et.al, defined attack and protection trees and

discussed how they can be implemented in the security analysis of an online banking system to maintain user's trust and confidence in the security of their online bank accounts [20]. Many researchers have done studies of several banks in their countries to compare their systems, but in India research on online banking security is still in its infancy specially in User Authentication. Let us study and understand them so we could analyze and understand their impact on user.

A-AUTHENTICATION METHODS [1]

Authentication is a critical part of any security system. For e-banking services, user authentication is done using login-password /cryptographic authentication scheme.

Password Authentication: Passwords are most common security mechanism but doesn't provide adequate protection and can be compromise by capturing keystrokes. In these cases dynamic password authentication can be better solution.

Cryptographic Authentication: This method provides the possibility of unique identification by generating unique access code each time by doing some Public-key/Private-key cryptographic operation and provides higher security. Both, public-key/private-key cryptography can provide authentication, data encryption and digital signature.

Classification of cryptographic authentication methods: Digital Signature: It provides authentication, no repudiation and data-integrity. It can be implemented with either public/private key encryption. Banking through E-channels has gained increasing popularity. As the use of the E-banking for financial transactions continues to grow, the number of authentication issues appears regarding to e-banking financial transaction security. Each authentication method has its strengths and weaknesses, which need to be weighed by the bank, including the impact on customers. In this paper a key focus is on strengthening the authentication credentials/factors, which are used to verify a bank customer's online-identity.

One-Time-Password generators: They are a good way to verify the identity of anyone, connects to a server. Hardware OTP generators are more secure than software OTP generators because they don't have to store data on the computer.

Challenge / response calculators: In this Method by taking a challenge value, corresponding response is calculated for individual user by using secret-key-cryptographic algorithm.

B-COMMON-STRATEGIES USED FOR SECURED-AUTHENTICATION

- Authentication mechanisms can be separated into these groups [2]:
- Password : arbitrary-secret-value
- Password + SSL : arbitrary-secret-value transmitted
- by secure channel (like SSL)
- SMS-Code : OTP sent by SMS
- PIN : short-secret-value
- Grid Card : paper-card with transaction-codes, user enters these codes in sequence
- PKC
- PKI
- based authentication system
- Token - trustworthy authentication device.

There are some threats applicable to the authentication mechanisms shown below [2] –

C-AUTHENTICATION METHODS WEAKNESSES [1]

System for remote authentication should consider few of the following security mechanisms [2]: User secure authentication (identity proof), Safe confidentiality of transferred data, Integrity of transferred data and Undeniable responsibility for transactions made. Thus each authentication method has its strengths and weaknesses, which need to be weighed by the bank, including the impact on customers.

POSSIBLE ATTACKS → / AUTHENTI-CATION METHODS SEARCH ↓	GUESSING	EXHAUST	EAVES-DROPING	MALWARE	PHISHING	MAL-WARE + PHISHING
PASSWORD	Y	Y	Y	Y	Y	Y
PASSWORD +SSL	Y	Y	N	Y	Y	Y
SMS-CODE	N	N	N	Y	N	N
PIN	N	Y	Y	Y	Y	Y
GRID-CARD	N	N	N	N	Y	Y
PKI	N	N	N	Y	N	N
TOKEN	N	N	N	N	N	N

D-ATTACKS ON AUTHENTICATION [3]

Internet banking systems must authenticate users before granting them access to particular services. More precisely, the banking system must determine whether a user is, in fact, who he
or she claims to be by asking for direct or indirect proof of knowledge about some sort of secret or credential. With the assumption that only an authentic user can provide such answers, successful authentication eventually enables users to access their private information.
The attack has been classified and categorized as a tree Fig. 1. An attack tree [4] has a root node and leaf nodes. The root node represents the target of the attack, while the leaf nodes represent the means for reaching the target, which are the events that comprise the attack. The attack tree has one root node, representing the final target of the attacker, which is the compromise of the user's bank account. An intruder may use one of the leaf nodes as a means for reaching the target. To categorize Internet banking attacks, each component of the process should be examined: the user terminal/user (UT/U), the communication channel (CC) and the Internet banking server (IBS). The following types of attacks are identified:

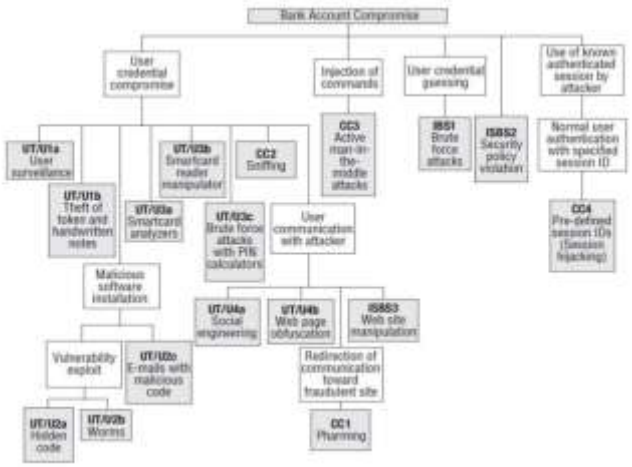

Figure 1. Hierarchy of attacks.

E-BIOMETRIC AUTHENTICATION - SIGNATURE

Biometric authentication is gaining popularity as a more trustable alternative to password-based security systems. Signature is a behavioral biometric: it is not based on the physical properties, such as fingerprint or face, of the individual, but behavioral ones. As such, one's signature may change over time and it is not nearly as unique or difficult to forge as iris patterns or fingerprints, however signature's widespread acceptance by the public, make it more suitable for certain lower-security authentication needs. Signature verification is split into two according to the available data in the input. Offline (static) signature verification takes as input the image of a signature and is useful in automatic verification of signatures found on bank checks and documents. Online (dynamic) signature verification uses signatures that are captured by pressure-sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number and order of the strokes, the overall speed of the signature, the pen pressure at each point, etc. and make the signature more unique and more difficult to forge. As a result, online signature verification is more reliable than offline signature verification. Fig. 2 shows sample signatures showing some very easy and very difficult signatures to forge, highlighting the fact that signature is a biometric the complexity of which can be adjusted; this is useful since one can use different signatures for different security applications. [5]

E-NATURE OF HUMAN SIGNATURE

It is supposed that the features of the process of signing originate from the intrinsic properties of human neuromuscular system which produces the aforementioned rapid movements. Knowing that this system is constituted by a very large number of neurons and muscle, fibers is possible to declare based on the central limit theorem that a rapid and habitual movement velocity profile tends toward a delta-log normal equation [6]. This statement explains stability of the characteristics of the signature. Thus, the signature can be treated as an output of a system obscured in a certain time interval necessary to make the signature. This system models the person making the signature [7]

F-TYPES OF FORGERIES

The main task of any signature verification system is to detect whether the signature is genuine or counterfeit. Forgery is a crime that aims at deceiving people. Since actual forgeries are difficult to obtain, the instrument and the results of the verification depend on the type of the forgery [8]. Basically there are three types that have been defined: Random forgery: this can normally be represented by a signature sample that belongs to a different writer i.e. the forger has no information whatsoever about the signature style and the name of the person. Simple forgery: this is a signature with the same shape or the genuine writer's name. Skilled forgery: this is signed by a person who has had access to a genuine signature for practice [9].

III. PRESENT METHOD

These are present encryption/decription Methods to be worked out for 'Login/password' and 'Signature' based Authentication.

A- SHA1 algorithm

SHA-1 [22] is a cryptography hash function designed by the United States National Security Agency that produces a 160-bit (20-byte) hash value. A SHA-1 hash value typically forms a
hexadecimal number, 40 digits long. The one-way hash function, or secure hash function, is important not only in message authentication but in digital signatures. The purpose of a hash function is to produce a" fingerprint" of a file, message, or other block of data. To be useful for message authentication, a hash function H must have the following properties:

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(x) is easy to compute for any given x, making both hardware and software implementation practical.
4. For any given code h, it is computationally infeasible

Fig. 2. Sample genuine signatures from the database. The topmost, left-most signature was very difficult to forge, while the right-most, bottom-most signature was quite easy.

to find x such that H(x) = h. A hash function with this property is referred to as one-way or pre image resistant.

5. For any given code h, it is computationally infeasible to find x such that y! = x with H(y) = H(x). A hash function

with this property is referred to as second pre image resistant, this is sometimes referred to weak collision resistant.

6. It is computationally infeasible to find any pair (x; y) such that H(x) = H(y).A hash function with this property is referred to as collision resistant. This is sometimes referred to as strong collision resistant.

B- RSA algorithm

RSA [23] is a block cipher in which the plain text and cipher text are integers between 0 and n for some n. Encryption and decryption are of the following form period for some plain text
block M and cipher text block C: $C = M^e \bmod n$ $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$. Both sender and receiver must know the values of n and e, and only the receiver knows the value of d. This is a public-key encryption algorithm with a public key of KU(e; n) and a private key of KR(d; n). For this algorithm to be satisfactory for public-key encryption, the following requirements must be met.

1. It is possible to find values of e,d, n such that $M^{ed} \bmod n = M$ for all $M < n$.
2. It is relatively easy to calculate M^e and C^d
for all values of $M < n$.
3. It is in feasible to determine d given e and n.

The first two requirements are easily met. The third requirement can be met for large values of e and n.

a-RSA key generation:

- Choose two large prime numbers p, q.(e.g., 1024 bits each)(Many tests like The Solovay-Strassen Primarily Test [24],Rabin-Miller Primarily Test[25], Ferment Little Test will check the primarily of number
- Compute n = p q, z = (p 1)(q 1)
- Choose e(with e < n) that has no common factors with z. (e, z are ”relatively prime”).
- Choose d such that ed 1 is exactly divisible by z. (in other words: e dmodz = 1).
- Public key is (n; e). Private key is (n; d).

b-RSA Encryption

Given (n; e) and (n; d) as computed above to encrypt [21] bit pattern, m,

- select random numbers,
- Shift the input text to (input value in ASCII+random number) value
- New value becomes the input text, then compute $c = M^e \bmod n$ (i.e., remainder when m^e is divided by n), for random number.

RSA Decryption: To decrypt [21] received bit pattern c, compute $m = c^d \bmod n$ (i.e., remainder when c^d is divided by n), for random number and then shift back to the (random number ASCII value of text) value.

C- Certificate

With the advent of public key cryptography (PKI), it is now possible to communicate securely with untreated parties over the Internet without prior arrangement. One of the necessities arising from such communication is the ability to accurately verify someone’s identity (i.e. whether the person you are communicating with is indeed the person who he/she claims to be). In order to be able to perform identity check for a given
entity, there should be a fool-proof method of binding the entity’s public key to its unique domain name (DN). A X.509 digital certificate [26] issued by a well known certificate authority (CA) [27], like VeriSign, Entrust, Thawte, etc., provides a way of positively identifying the entity by placing trust on the CA to have performed the necessary verification. A X.509 certificate is a cryptographically sealed data object that contains the entity’s unique DN, public key, serial number, validity period, and
possibly other extensions. [Note: Refer to RFC 3280 for a complete list of attributes and X.509 v3 extensions.] Certificates are typically stored in PEM (Privacy Enhanced Mail) format.

D- Signature algorithm

The algorithm to generate digital signature [28] is as follows: (Fig 3)

1. Open a input document to be signed.
2. Select the hash function to be used (Here its SHA1)
3. Generate the 160 bit hash value
4. Generate the keys (Here RSA keys)
5. Encrypt the hash value
6. Attach certificate for authentication
7. Generate signature and store in the document.

Signature will now contain: Signature, Length of signature, Encryption algorithm used, Hash function used, Key, Original message

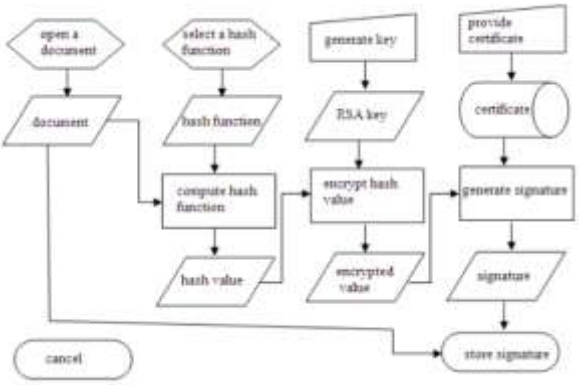

Figure 3: Signature Generation

IV. AUTHENTICATING SMART CARD

Most of the transaction in Banks is done using Smart Cards like Debit Cards/Credit Cards through ATM or other payment terminals. Smart Card is the technology that enables customers to access banking and financial services through the use of their credit/debit. It allows customers to withdraw, transfer and deposit money using cards. Although Smart Card may offer benefits, there are

risks involved. Card transaction like other types of traditional and online banking systems, is susceptible to security breaches. Accessing financial services through credit/debit cards may result in sensitive financial data falling into wrong hands. As Smart Cards are based on password authentication called PIN which is usually 4 digits has greater risks of loss/theft of PIN information or a customer's cards itself.
Smart Card fraud can happen in a variety of ways, from low tech diving to high tech hacking.

A- Personal Identification Number
B-

A personal identification number (PIN, pronounced "pin") is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. The user is granted access only when the number entered matches with the number stored in the system. Hence, despite the name, a PIN does
not personally identify the user. Financial PINs are often four-digit numbers in the range 0000-9999, resulting in 10,000 possible numbers[29]. Many PIN verification systems allow three attempts, thereby giving a card thief a 0.06% probability of guessing the correct PIN before the card is blocked.
The significant disadvantage of using a PIN is that the number can be stolen using skimmers. Using
pre-fabricated geared device perfectly matched to the hardware of Bank ATMs, they will be able to read magnetic stripe off of victims' cards and even record victims punching in their PINs as shown in figure 4. After this clones are made from their victims' cards, and are used with the recorded PIN.

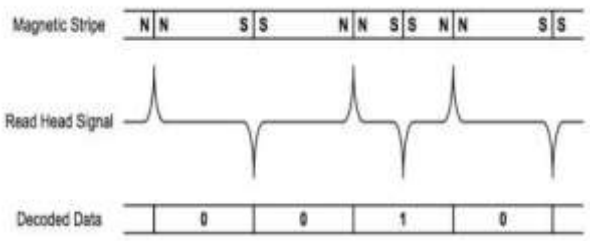

Fig 4: Recording the PIN using skimmers

B- Mechanical Imprint

Until the introduction of Chip and PIN, all face-to-face credit or debit card transactions used
a magnetic stripe or mechanical imprint to read and record account data, and a signature for verification. Under this system, the customer hands their card to the clerk at the point of sale, who either "swipes" the card through a magnetic reader or makes an imprint from the raised text of the card. In the former case, the account details are
verified and a slip for the customer to sign is printed[30]. In the case of a mechanical imprint, the transaction details are filled in and the customer signs the imprinted slip. In either case, the clerk verifies that the signature matches that on the back of the card to authenticate the transaction. This system has proved to be ineffective, because it has a number of security flaws, including the ability to steal a card in the post, or to learn to forge the signature on the card. More recently, technology has become available on the black market for both reading and writing the magnetic stripes, allowing cards to be easily cloned and used without the owner's knowledge.

C-Finger Print Authentication

Fingerprints are one of many techniques used to identify individuals and verify their identify.
Matching algorithms used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes. Pattern based algorithms compare the basic fingerprint patterns (arch, whole, and loop) between a previously stored template and a candidate fingerprint. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match. The major disadvantage here is that Finger print authentication cannot be successful if the user has a band aid on his finger. Another
disadvantage is fingerprint remains the same even if the person is unconscious or dead. This leads to unauthorized use of a person's fingerprint without his consent.

D-Palm Vein Technology

Users today mostly use textual passwords that follow an encryption algorithm. Mostly textual
passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, girlfriends etc. Years back Klein performed such tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has become a Child's Play. Therefore we use biometrics in our authentication which is more customizable and very interesting way of authentication.
The vein matching, [31] also called vascular technology is a technique of biometric identification through the analysis of the patterns of blood vessels visible from the surface of the
skin. An individual first rests his wrist, on some devices, such that the palm is held centimeters above the device's scanner, which flashes a near-infrared ray on the palm.
Unlike the skin, through which near-infrared light passes, deoxygenated hemoglobin in the blood flowing through the veins absorbs near -infrared rays, illuminating the hemoglobin, causing it to be visible to the scanner. Arteries and capillaries, whose blood contains oxygenated hemoglobin, which does not absorb near infrared light, are invisible to the sensor. The still image captured by the camera, which photographs in the near infrared range, appears as a black network, reflecting the palm's vein pattern against the lighter background of the palm.

 ISSN: 2321-8169
391– 398

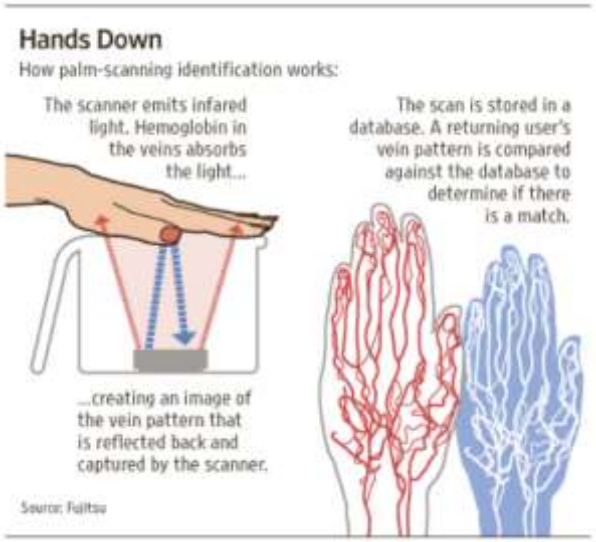

Fig 5: Scanned vein pattern

An individual's palm vein image is converted by Iterative Closest Point algorithms into data points, which is then compressed, encrypted, and stored by the software and registered along with the other details in his profile as a reference for future comparison. Iterative Closest Point is an algorithm employed to minimize the difference between two clouds of points. ICP is often used to reconstruct 2D or 3D surfaces from different scans, to localize robots and achieve optimal path planning (especially when wheel odometry is unreliable due to slippery terrain), to co-register bone models, etc. The algorithm is conceptually simple and is commonly used in real-time[32]. It iteratively revises the transformation (translation, rotation) needed to minimize the distance between the points of two raw scans as in Fig 5.Thus, each time a person logs in attempting to gain access by a palm scan to a particular bank account or secured entryway, etc., the newly captured image is likewise processed and compared to the registered one or to the bank of stored files for verification, all in a period of seconds. Numbers and positions of veins and their crossing points are all compared and, depending on verification, the person is either granted or denied access. Compared with a finger or the back of a hand, a palm has a broader and more complicated vascular pattern and thus contains a wealth of differentiating features for personal identification. The palm is an ideal part of the body for this technology; it normally does not have hair which can be an obstacle for photographing the blood vessel pattern, and it is less susceptible to a change in skin color, unlike a finger or the back of a hand. Even if one has registered as a child, and uses it after a very long period, it still remains the same because the vein pattern is established in the uterus even before birth.

Palm vein authentication has a high level of authentication due to the uniqueness and the complexity of the vein pattern. It is better than finger print scanning because a fingerprint remains the same even if the person is dead. Thus there are a lot of chances for the unauthorized user to hurt or kill the card holder for the finger print.

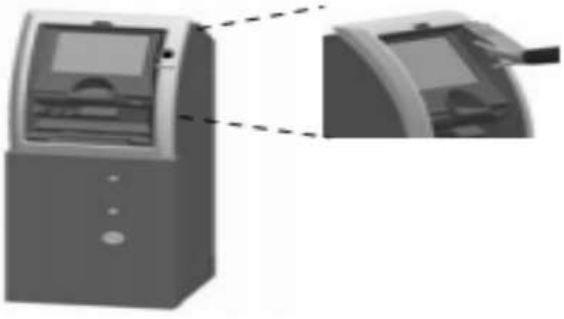

Fig 6: ATM for convenience stores with downsized palm vein pattern sensor unit.

V. E-PROPOSED METHOD

To overcome the limitations mentioned above, we proposed an idea of using two techniques of authentication. The first is conventional PIN based authentication and second is the palm vein technology.

a- Finger Print Authentication

Fingerprints are one of many techniques used to identify individuals and verify their identify. Matching algorithms used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes

b- The Palm Vein Technology

The palm vein technology is an authentication scheme that scans a person's palm and authorizes him based on his vein pattern. The device sends out infrared radiations that pass deep into the person's palm and scans his vein pattern. This would make the use of smart card well secured. Also the already discussed risk of possibility of others accessing one's bank account when his smart card is

VI. CONCLUSION

In spite of various methods of Authentication are available and worked out today the most popular and widespread method still remains 'login/password pair' and 'Signature Biometrics'. Most of Banks and other sectors still are heavily depend on these two methods and even these are more comfortable and convenient to the users of all categories, types and ages. Beside all weaknesses and attack proneness of these methods still it is preferably accepted by industry especially banking worldwide today. More research and updating of these prominent methods are needed today beside development other new methods of authentication. First reason for this is because it is quite comfortable and habitual to users today and secondly it is easy and widespread. Any of these two authentication methods preferably password/pin, should be primary way to first authentication and 'The palm vein technology' should be secondary way of authentication .Other new methods can be used as supplementary for advance authentication. These methods have more impact on users and industry especially banking sectors today. They have become habitual and natural to the people especially banks users.

Fig 7: ATM authentication with PIN and Palm Vein Pattern sensor unit.

REFERENCES

[1] e-Banking Security and Authentication Issues by Raksha Chouhan - Research Scholar, Suresh Gyan Vihar University Jaipur , Dr. Vijay Singh Rathore- Supervisor Suresh Gyan Vihar University,Jaipur (International Referred Research Journal, August, 2011. ISSN-0974-2832, RNI-RAJBIL 2009/29954 ; VoL.III *ISSUE-31)

[2] Hanaek, P.; Malinka, K.;Schafer, J.(2008); "E-banking security - comparative study", Security Technology. 42nd Annual IEEE Carnahan Conference.Page(s):326 - 330.

[3] Client Authorization and Secure Communication in Online Bank Transactions - Vyshali Rao K P*, Adesh N D**, A V Srikantan*** *M.Tech, CSE Department, Srinivas Institute of Technology, Valachil, Mangalore - corresponding author **Asst. Professor, CSE Department, Srinivas Institute of Technology, Valachi, Mangalore***Divisional Engineer(TM), RTTC, BSNL, Mysore. (International Journal of Scientific and Research Publications, Volume 4, Issue 5, May 2014 ISSN 2250-3153)

[4] Christos K. Dimitriadis, ”Analyzing the Security of Internet Banking Authentication Mechanisms”2007 ISACA

[5] Identity authentication using improved online signature verification method Alisher Kholmatov, Berrin Yanikoglu* Sabanci University, Faculty of Engineering and Natural Sciences, Istanbul, 34956 Tuzla, Turkey

[6] Plamondon, “The Handwritten Signature as a Biometric Identifier: Psychophysical Model & System Design” IEE Conference Publications, R.1995,Issue CP408, 23-27

[7] Pacut, A. and Czaja,”Recognition of Human Signatures. Neural Network”, A. 2001,in proceedings of the International Conference on Neural Network, IJCNN’01, vol.2, pp 1560-1564.

[8] Kalenova,” Personal Authentication using Signature Recognition”, D.2005

[9] Aykanat C. et. al ,(Eds). 2004. Proceedings of the 19th International Symposium on Computer and Information Sciences, ISCIS 2004. Springer-Verlag Berlin Heidelberg New York. pp. 373-380.

[10] Munirul Ula, Zuraini bt Ismail2 and Zailani Mohamed Sidek,”. A Framework for the Governance of Information Security in Banking System ”, Journal of Information Assurance & Cybersecurity ,Vol 2011, Article ID 726196,

[11] TC. Shan and WW. Hua,” Service-Oriented Solution Framework for Internet Banking”, International Journal of Web Services Research,vol.3, issue 1, 2006, pp. 29-48.

[12] M. Nilsson, A. Adams and S. Herd,” Building Security and Trust in Online Banking. Conference on Human Factors in Computing Systems”, Portland, USA, pp. 1701-1704, 2005.

[13] E. Kaynak and T.D. Harcar,” Consumer Attitudes towards Online Banking: A New Strategic Marketing Medium for Commercial Banks”,.International Journal of Technology Marketing”, vol. 1, no.1, 2005, pp.62-78.

[14] K.J. Hole, V. Moen and T. Tjostheim. “Case Study: Online Banking Security. Security & Privacy”, IEEE, vol.4, issue.2, 2006 April.

[15] Alain Hiltgen,Thorsten Kramp and Thomas Weigold.,” Secure Internet Banking Authentication”, IEEE COMPUTER SOCIETY 2005

[16] Xing Fang, Justin Zhan.,” Online Banking Authentication Using Mobile Phones”,IEEE 2010.

[17] A. Hisamatsu,D.Pishva,,G.G.D. Nishantha.,” Online Banking and Modem Approaches Toward its Enhanced Security”, ICACT 2010.

[18] State of Data Security and Privacy in the Indian Banking Industry DSCI-KPMG Survey by DSCI 2010

[19] Laura Falk,Atul Prakash,Kevin Borders,”Analyzing Websites for User-Visible Security Design Flaws”

[20] Kenneth Edge, Richard Raines, Michael Grimaila, and Rusty Baldwin Robert Bennington and Christopher Reuter,” The Use of Attack and Protection Trees to Analyze Security for an Online Banking System”, Proceedings of the 40th Hawaii International Conference on System Sciences – 2007 Air Force Research Laboratory.

[21] Rajan.S.Jamgekar, Geeta Shantanu Joshi, ”File Encryption and Decryp-tion Using Secure RSA”. International Journal of Emerging Science and Engineering (IJESE) ISSN: 23196378, Volume-1, Issue-4, February 2013

[22] Nalini C. Iyer and Sagarika Mandal, Implementation of Secure Hash Algorithm-1 using FPGA, International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 8 (2013),

[23] P. Kitsos, N. Sklavos and O. Koufopavlou, An efficient implementation of Digital Signatire algorithm. VLSI Design Laboratory Electrical and Computer Engineering Department University of Patras. Patras, GREECE

[24] Yung-Chieh Lin; Yi-Ping Hung, Zen-chung Shih, The Solovay-Strassen Primality Test ,12 October, 1993 Burt Rosenberg Re-vised: 6 October, 2000

[25] Rudin,S. Osher. Rabin-Miller Primality Test.

[26] S Beucher, ”X.509 Certificate Generator User Manual”,

[27] ”Types of certification authorities”, Microsoft Certificate Authorities from Microsoft Technet.

[28] “S.R. Subramanya and byung K. YI ”Digital signatures”, IEEE March/April 2006.

[29] Murdoch, Steven J.; Drimer, Saar; Anderson, Ross; Bond, Mike; , "Chip and PIN is Broken," Security and

Privacy (SP), 2010 IEEE Symposium on , vol., no., pp.433-446, 16-19 May 2010

[30] Nasir, M.H.N.; Hamid, S.; Hassan, H.; , "Thread-Level Parallelism & Shared-Memory Pool Techniques for Authorization of Credit Card System," Communications and Information Technologies, 2008. ISCIT 2008. International Symposium on , vol., no., pp.447-452, 21-23 Oct. 2008

[31] Xiangqian Wu; Enying Gao; Youbao Tang; Kuanquan Wang; , "A Novel Biometric System Based on Hand Vein," Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on , vol., no., pp.522-526, 18-22 Aug. 2010

[32] Shitu Luo; Yanling Wang; Yin Liu; Xiaopin Hu; , "Research on geomagnetic-matching technology based on improved ICP algorithm," Information and Automation, 2008. ICIA 2008. International Conference on , vol., no., pp.815-819, 20-23 June 2008

Abdul Samad Shaikh-
obtained his Master in Management Science (MMS) from Dr. BAMU, Aurangabad, Maharashtra. He has contributed in development of new language called 'XBRL' and written 23 books which are being used as courseware in various educational institutes and colleges. He is a software developer and excellent corporate I.T. Trainer having more than 24 years of experience in the same. His research area includes Authentication Methods, Mobile based application, Clouds and eCommerce Application development.
(*email*:- samadindia@gmail.com)

Mohammed Waseem Ashfaque -

completed his graduation and post Graduation in Computer Science in 2002, and now he is perusing Ph.D in Computer Science, he has sound and peer experience in teaching at various National colleges and International Universities since 2002.He attended various research seminars and fully involved in various research activities. Near about 10-16 research paper he has credited in his own academic account.
(*email:*- waseem2000in@gmail.com)