ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

A Reliable Biometrics Based Multi Network Validation Prescript Using Smartcard

B.Preethi*[1], B.Padmaja*[2]

M.Tech, Dept of CSE, Institute of Aeronautical Engineering College, Hyderabad, Telangana, India

Assoc Professor, Dept of CSE, Institute of Aeronautical Engineering College, Hyderabad, Telangana, India

ABSTRACT: Access control systems provide security in wireless communication network and e-commerce application, such as e-Banking and transaction orientated services. Before Security was provided for authentication of user side verification only. In this project we are using secure biometrics based multi-server authentication protocol using smart cards which protect the sensitive information against a malicious adversary , a variety of security services such as mutual authentication, RFID, Finger prints, we show that our scheme provides secure authentication. In addition, we simulate our scheme for the formal security verification using the widely-accepted and used AVISPA (Automated Validation of Internet Security Protocols and Applications) tool, and show that our scheme is secure against passive and active attacks. Our scheme provides high security along with low communication cost, computational cost, and variety of security features. We have first reviewed the recently proposed He-Wang's scheme and then shown that their scheme is vulnerable to the known session-specific temporary information attack and thus, their scheme fails to prevent reply attack and cannot provide strong user anonymit.

KEYWORDS: RFID, Finger prints.

I. INTRODUCTION

Internet banking is more and more prominent both in Norway and elsewhere. Banks have actively determined this cost-saving trend by persuading customers to sign up. Customers, attracted by online banking convenience, seem largely unconcerned about identifying theft and phishing email scams. In fact, most client seem to believe that Internet banking is quite safe easily because their banks told them so. Net Banking System is well known automation commonly used by individuals to carry out a variety of personal and business financial transactions and banking functions by using finger print identification technique. Net banking system has become very attractive with the general public for their availability and general user friendliness. Net banking system is typically available to clients on a continuous basis such that consumers have the ability to carry out their ATM financial transactions or banking functions at any time of the day and on any day of the week.

II. EXISTING SYSTEM

In the old net banking system, the user can log on to the online banking. He/she can view his account details, loan details, transaction details etc., but they didn't have the facility of the fund transaction between one to one and third party transaction. So to overcome these drawbacks we move to the new system.Net banking system allows clients to commercial foundation to conduct commercial transactions on a secure website operated by the institution, which can be a retail or virtual bank, credit union or building society.

Disadvantages: We have to go to the bank for changing foreign money, so there will be waste of time. With hacking and identity theft on the rise, Internet banking customers have to place a certain amount of trust in the bank that their account information and personal information are safe. Security is less.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

III. PROPOSED SYSTEM

i. Proposed System

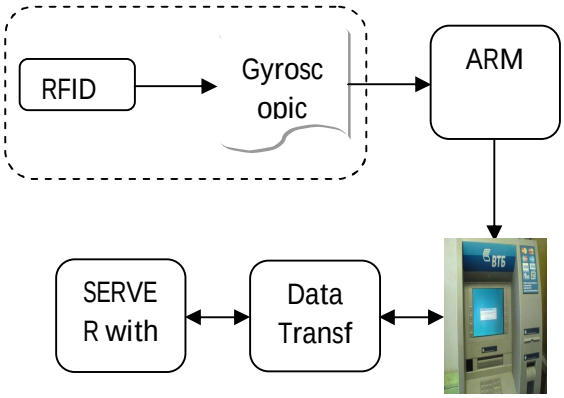
In this proposed system we have created the new generation ATM machine which can be accessed by RF enabled ATM card with 3D position based key generation. Working of RFID card with gyroscopic sensor was controlled by controller module in which Key generation done based on MEMS axis.If it gets verified a OTP will be generated and using MAC implementation. This OTP will be sent to requested user as SMS.

Advantages:

By using this system malfunctions can be avoided. Our transaction will be much secured. Multiple banks databases are inter connected with high security. It enables a visually and hearing damaged individual to conveniently and easily carry out financial transactions or banking functions.

Architecture Diagram:

Literature Survey:



Digital Single Lens Reflex Camera Identification from Traces of Sensor Dust

Digital single lens reflex cameras suffer from a well known sensor dust problem due to interchangeable lenses that they deploy. The dust particles that settle in front of the imaging sensor create a persistent pattern in all captured images. In this paper, we propose a novel source camera identification method based on detection and matching of these dust-spot characteristics. Dust spots in the image are detected based on a (Gaussian) intensity loss model and shape properties. To prevent false detections, lens parameter dependent characteristics of dust spots are also taken into consideration. Experimental results show that the proposed detection scheme can be used in identification of the source digital single lens reflex camera at low false positive rates, even under heavy compression and down sampling.

Determining Digital Image Origin Using Sensor Imperfections

In this paper, we demonstrate that it is possible to use the sensor's pattern noise for digital camera identification from images. The pattern noise is extracted from the images using a wavelet-based demon string filter. For each camera under investigation, we first determine its reference pattern, which serves as a unique identification fingerprint. This could be done using the process of flat-fielding, if we have the camera in possession, or by averaging the noise obtained from multiple images, which is the option taken in this paper. To identify the camera from a given image, we consider the reference pattern noise as a high-frequency spread spectrum watermark, whose presence in the image is established using a correlation detector. Using this approach, we were able to identify the correct camera out of 9 cameras without a single misclassification for several thousand images. Furthermore, it is possible to perform reliable identification even from images that underwent subsequent JPEG compression and resizing. These claims are supported by experiments on 9 different cameras including two cameras of exactly the same model.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

A. Study of the Robustness of PRNU-based Camera Identification

We investigate the robustness of PRNU-based camera identification in cases where the test images have been passed through common image processing operations. A specific question we aim to answer is how camera identification can be circumvented by an nontechnical user, applying only standard and freely available software. We study demonizing, recompression, out-of-camera demos icing. We measure the beneficial effect of JPEG block artifact removal on camera identification accuracy. We examine the extent to which JPEG block artifact removal helps circumvention by improving the performance of a denier that is used to remove PRNU features. We evaluate the effectiveness of the Stir Mark watermark remover as a tool for circumventing camera identification, and we examine the similarities and differences between watermark circumvention and camera identification circumvention.

An Improved Camera Identification Method based on the Texture Complexity and the Image Restoration: The identification of source camera is useful to improve the capability of evidence in the digital image such as distinguish the photographer taking illegal images and adopting digital images as evidence of crime. Lukas, et al. showed the method for source camera identification based on the correlation of PNU (pixel non-uniformity) noise. However, the wavelet-based demonizing filter for suppressing the random noise reduces the accuracy of camera identification. It is caused by the fact that the demonizing filter diffuses the edge and makes the PNU noise less pronounced. Moreover, it is difficult to extract PNU noise from the images taken by cameras which are equipped with the image improvement functions such as motion blur correction, contrast enhancement, and noise reduction. In this paper, we propose a method for improving the camera identification accuracy by selecting pixels based on the texture complexity. We also propose a method for improving the identification accuracy by applying the image restoration method.

IV. ALGORITHM

MD5 Algorithm Description:

- We begin by supposing that we have a b-bit message as input, and that we wish to find its
- Message digest, Here b is an arbitrary nonnegative integer; b may be zero, it need not be a.
- Multiple of eight, and it may be arbitrarily large. We imagine the bits of the message written
- down as follows:
- m_0 m_1 ... m_{b-1}

The following five steps are performed to compute the message digest of the message.

Triple DES (Data Encryption Standard):

Descriptions:

Triple DES uses a "key bundle" which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits. The encryption algorithm is:

Cipher text = $E_{K3}(D_{K2}(E_{K1}(plaintext)))$

I.e., DES encrypts with K_1, DES decrypt with K_2, then DES encrypt with K_3. Decryption is the reverse:

Plaintext = $D_{K1}(E_{K2}(D_{K3}(cipher\ text)))$

I.e., decrypt with K_3, encrypt with K_2, then decrypt with K_1. Each triple encryption encrypts one block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying options 2, and provides backward compatibility with DES with keying option.

Triple DES Algorithm:

In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

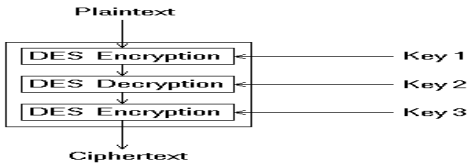
Triple DES uses a "key bundle" which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits). The encryption algorithm is:

$$\text{cipher text} = E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$$

Step 1 : DES encrypt with K_1, DES decrypt with K_2, then DES encrypt with K_3. Decryption is the reverse:

$$\text{plaintext} = D_{K1}(E_{K2}(D_{K3}(\text{cipher text})))$$

Step 2 : Decrypt with K_3, encrypt with K_2, then decrypt with K_1. Each triple encryption encrypts one block of 64 bits of data.



Modules

Finger Print Enrolment:
Fingerprint enrolment is a process of registering user's bio-metric data for verification purposes. The quality of the fingerprint enrolment is fundamental for the work of the matching algorithm. The number of false rejects is very much dependent on the quality of the enrolled fingerprint template

User Authentication:
In user verification method, one time password (OTP) is generated during registration process. One time password is generated using random number generation algorithm. That password is sent to the user's mobile number for authentication. After that the user should give that one time password to access net banking process.

Finger Print Verification:
In fingerprint verification process the user application sends the fingerprint image of the person being verified. In finger print enrollment module the user's finger print is stored in the database in .fpt format. In verification process the user will give their finger print and that is compared with the finger print which is already stored in the database by using SDK tool. If the finger print matches then only the user can access their net banking process.

Key Pair Generation:
In this module public key and private key is generated for every users to access their banking process. The user's information is encrypted by using public key and private key. AES (Advanced Encryption Standard) Algorithm is used for encryption and decryption.

Security Verification:
In security verification module, user's public key and private key is verified by the admin. All users may know every user's public key and only the especially user knows the private key. The encrypted data is decrypted by using key pairs. The generated key pair is verified in this module.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

Fund Transfer:

In this module, the users account is managed by the admin. The user can transfer, withdraw, deposit amount to any other account by using the key pairs and one time password. One user can transfer money to another user by using public key and private key.

Log Maintenance:

This module is maintained by the admin. It shows the every user's information and details about amount deposit, withdraw, transfer to some other account. Every user's details, information and what they used in net banking process is viewed by the admin.

V. CONCLUSION

In this paper, we have addressed security problem for net banking system. In this we are implementing finger print recognition technique for high security. By using this finger print sensor the user only can get authorized and will be able to login, the unauthorized user can't be able to login. Also in this paper we are encrypting the fingerprints and storing into the database. In this way we are providing high security for the net banking system. In this way if we use biometrics we can provide high security.

REFERENCES

[1]. S.Abolfazli, Z. Sanaei, E. Ahmed, A. Gani and R.Buyya, "Cloudbased augmentation for mobile devices: Motivation, taxonomies, and open challenges," IEEE Communications survey and Tutorials, Vol.16, no.1, 2014.
[2]. J.L.Tsai,N.W.Lo and T.C.Wu, "Novel anonymous authentication scheme using smart cards", IEEE Transaction on industrial informatics, vol.9, no.4, 2004-2013, 2013.
[3]. R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in Advances in Cryptology–EUROCRYPT 2001. Innsbruck (Tyrol), Austria: Springer, 2001, pp. 453–474.
[4]. M. Bellare, R. Canetti, and H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols," in Proceedings of the thirtieth annual ACM Symposium on Theory of computing (STOC). Dallas, TX, USA: ACM, 1998, pp. 419–428.
[5]. E. Brickell and J. Li, "Enhanced privacy id: A direct anonymous attestation scheme with enhanced revocation capabilities," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 3, pp. 345–360, 2012.
[6]. X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1767–1175,2014.
[7]. D. Wang, P. Wang, and D. He, "Anonymous two-factor authentication: Certain goals are beyond attainment," IEEE Transactions on Dependable and Secure Computing, 2014, DOI: 10.1109/TDSC.2014.2355850.
[8]. S. Wu, Y. Zhu, and Q. Pu, "Robust smart-cards-based user authentication scheme with user anonymity," Security and Communication Networks, vol. 5, no. 2, pp. 236–248, 2012.
[9]. S. Kumari and M. K. Khan, "Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme'," International Journal of Communication Systems, vol. 27, no. 12, pp. 3939–3955, 2014.
[10]. D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," IEEE Transactions on Wireless Communications, vol. 10, no. 2, pp. 431–436, 2011.
[11]. L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for sip using ecc," Computer Standards & Interfaces, vol. 31, no. 2, pp. 286–291, 2009.
[12]. L. Lamport, "Password authenticat-ion with insecure communication" Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981..

BIOGRAPHY

B.Preethi is currently pursuing her M.Tech(CSE) in Computer Science and Engineering Department, Institute of Aeronautical Engineering College , she received her B.Tech in Computer Science and Engineering from Institute of Aeronautical Engineering College , Hyderabad, Telangana, India.

B.Padmaja is currently working as an Associate Professor in Computer Science & Engineering Department, Institute of Aeronautical Engineering College .Her research interests include Network Security, Data Warehousing and Data mining, RDBMS.