ISSN:0975-9646

Smart Card Fraud Prevention Scheme Using Fingerprinting Authentication

Jayesh Gaurav[1], Sanjive Tyagi[2], Dr Jayanthi Ranjan[3]

[1] Mr.Jayesh Gaurav, Lawyer and Cyber Law Adviser, Supreme Court of India, Delhi-01(India),
(Research Scholar Singhania University, Jhunjhunu, Rajsthan)

[2] Mr.Sanjive Tyagi, Associate Professor, Radha Govind Group of Institutions, Meerut, U.P.(India),
(Ph.D. (Submitted in 2011) from Singhania University, Jhunjhunu, Rajsthan, India)

[3] Dr Jayanthi Ranjan, Professor- Institute of Management Technology, Ghaziabad, U.P.(India),

Abstract—**E-commerce payment system have become progressively popular due to wide spread use of the internet-based shopping and banking. Nowadays, smart card payment systems for e-commerce are being used much more extensively than in the past. With the growing use of electronic payment system, risk of fraud in e-payment is also increasing. Frauds in e-commerce payment are may be of different type like as by stolen of smart card, by internet hackers; who break into computers and computers networks, and can access identity information of card system. A serious weakness of this system is that criminals who obtain the correct personal information can impersonate an honest consumer and commit payments fraud. This paper explores how smart cards with additional fingerprint verification, have the potential to provide strong payment authorization and thus put a substantial solution into the problems of e-payments fraud. The combination fingerprint identity and password would be a key to improving security and reducing e-payment fraud.**

Keywords— **E-commerce, E-payment, E-crime, E-fraud, Hackers, Authentication, Smart-card, Architecture, Biometric, Fingerprint.**

I. Introduction

E-commerce has gained a continuous growth with increasing application of internet world wide. In the current internet community, secure data transfer is limited due to its attack made on data communication. Due to this reason the success of the electronic commerce depends upon effective e-payment systems. E payment is a subset of an e-commerce transaction to include electronic payment for buying and selling goods or services offered through the Internet [1].

The Internet and on-line businesses are growing exponentially. Due to this explosive growth, electronic commerce on the Internet uses various electronic payment mechanisms. We may use sophisticated methods to prevent smart card fraud such as combining it with biometric technologies which offer protection against illicit criminal activity, such as identity theft, account manipulation, and fraud. While many of biometric technologies are currently available, each has varying degrees of acceptance, and some require substantial direct investments, fingerprinting is the most suitable authentication application because of its reliability and cost effectiveness.

II. Related Work

A. *J. Raja et al* [2] carried out a research work to identify and explain the different methods of e-payment the authors analyses the challenges of electronic payments from different perspective and provide preliminary security countermeasures for each of the issues. Finally a number of solutions have been proposed based on the problem and discussed on the prospect of electronic payment

B. *K. A. Akintoye et* al [3] proposed electronic payment system based on a broad definition of both e-crime and e-fraud, the resultant model describes the five key elements of e-fraud: perpetrator, mode of attack, target system, target entity and impact. It is envisaged that the model will allow the mechanics and context of e-fraud to be more fully understood, thus assisting in the development and implementation of effective countermeasures.

C. *PyaePyae Hun* [4] proposed architecture of electronic payment system is to be secure for clients such as customers and shop owners. The security architecture of the system is designed by RC5 encryption / decryption algorithm. This eliminates the fraud that occurs today with stolen credit card numbers. The symmetric key cryptosystem RC5 can protect conventional transaction data such as account numbers, amount and other information.

D. *Dileep Kumar et al* [5] have suggested after survey on biometric payment system that biometric payment system issued for various kinds of payment system instead of the tension of cards to put with them and to memorize theirs difficult passwords and pin numbers. Biometric payment system is much safe and secure and very easy to use and even without using any password or secret codes to remember as compare with previous system like credit card payment system, wireless system and mobile system etc.

E. *Chin-Chen Chang et al* [6] in propose a novel remote password authentication scheme that overcomes the security weaknesses of Hwang-Li's scheme [7]. The proposed scheme provides mutual authentication between the remote system and the user such that the server spoofing attack cannot have an effect. Proposed scheme is increasing the authentication efficiency, and allowing the user to choose and change his/ her password at will.

III. PRELIMINARIES

A. *Smart Card*

A **smart card, chip card**, or **integrated circuit** card (ICC), is any pocket-sized card with embedded integrated circuits. A smart card or microprocessor cards contain volatile memory and microprocessor components. The card is made up of plastic. Smart cards may also provide strong security authentication for single sign-on (SSO) within large organizations [8].

B. *Credit Card Fraud:*

Credit card is one of the biggest challenges to online business establishment today. Frauds are committed by use of unauthorized account and personal information, by misrepresentation of account information to obtain the benefits, it may be by stolen the card is the most common type of fraud, others include identity theft, skimming, counterfeit card, mail intercept fraud and others. Summaries the modus operandi for credit card frauds and their percentage of occurrence as lost or stolen card is 48%, Identity theft is 15%, Skimming (or cloning) is 14%, Counterfeit card is 12%, Mail intercept fraud is 6% and other is 5% [9].

C. *Biometric-based authentication:*

Biometric-based authentication schemes along with passwords have several advantages of using biometric keys (for example, fingerprints, faces, irises, hand geometry and palm-prints, etc.) as compared to traditional passwords because biometric keys are very difficult to copy or share, extremely hard to forge and cannot be lost or forgotten. Biometric-based authentications are more reliable and secure than usual traditional password-based user authentication methods [10].

IV. *OUR APPROACH*

Due to rapid progress e-commerce, the electronic payment is one of the biggest technological innovations in the area of banking, finance and commerce. E-payments have several advantages, which were never available through the traditional modes of payment. But we should remember with the increasing use of e-payment also lead our society with e-fraud, which is a biggest challenge. Over the last few years, maximum threats are from credit card frauds, thus, we have proposed smart card with biometric authentication which is a key for improving security and preventing e-payment fraud.

Biometric technology is advancing rapidly for several reasons. The first is that the cost of biometric technologies is becoming less to use. The second is the improved ease of integrating a high level of security by matching individual attributes such as fingerprint, which is one of the most suitable from facial expression, voice pattern, eye tissues etc. So, in order to get high level security we proposed biometric-based (fingerprint) authentication method along with password, which is secure remote authentication scheme integrated with fingerprint authentication. Therefore, we have introduces next generation of smart card with temper-proof biometric (fingerprint) smart card and consequently, not only reduce the fraud, but increase the trust of users.

V. THE PROPOSED SCHEME

In proposed system we are using mathematical representation of fingerprint MRFP= ⍰ (DCFM) generated by Fingerprint-Capture Procedure. In order to prevent smart card fraud, we are incorporating password base mutual authentication scheme with fingerprint identity (MRFP). The use of one's fingerprint as identification of smart card makes electronic payment system more reliable i.e. smart card owner should present at the time of using it, which avoids stolen of smart card. Biometric payment technology allows the consumer to pay with the touch of a finger on fingerprint scanner linked to fingerprint template at remote server. The fingerprint template is typically linked to remote system through secured channel to verify the transaction through mutual authentication between remote system and user. Therefore, we propose an efficient password authentication scheme with the combination of fingerprint verification that not only ensures mutual authentication between remote system and the user to enhance the security but also prevent stolen or theft of smart card.

In this scheme, if a user User_s stolen the smart card of user User_i with all information required to access the smart card. The user User_s is illegal user of smart card can access its benefits. So to prevent illegal use of smart card, we attach biometric authentication. There are several human distinguishable characters that fit the definition of biometrics. In order to recognizing a person, the human character needs to be unique and not to be changed in future. Fingerprint have been used for over hundred years and therefor generally fit to recognize a user and well accepted by technology.

The proposed scheme divided in three phases:

1) Registration phase

2) Login Phase

3) Authenticate phase

A. Registration phase:

Registration phase is divided in two phases:

Phase I:

- Assume n and m be secrete key maintained system.
- H(#) is the one way hash function, where r and s are very large prime numbers.
- *g* is a primitive element in *GF* (num) , where num = r · s.
- For registration,
    - A new user $USER_i$ has to submit his/her $IDENTITY_i$
    - Password PW_i taken by himself/ herself to remote system through a secure channel.
    - Input fingerprint thorough scanner device, store it on remote server and $MRFP_i$ is corresponding mathematical representation obtained by Fingerprint-Capture Procedure.

After receiving the registration request, the remote system processes the following procedure:

Fingerprint-Capture Procedure:

1. Read fingerprint using fingerprint scanning device.
2. Captured digital image of fingerprint (DIFP) is stored as biometric algorithm (BA).
3. Algorithm (BA) analyze more than forty data points of DIFP
4. Determine the measurements of analyzed data points and store them as data coordinates.
5. Encrypt data coordinates into digital certificates (DCFP).
6. Transform digital certificates (DCFM) into mathematical representation (MRFP).

   MRFP= ⍰ (DCFM)
7. Mathematical representation MRFP of DCFM is used as unique identity of smart card holder.

Phase II

Registration-Procedure:

1. $USER_i$ input fingerprint (biometric) as B_i
2. $USER_i$ input identity $U(IDENTITY_i)$
3. Compute $MRFP_i$= ⍰ ($DCFM_i$).
4. Compute $FP_i=H(MRFP_i)$
5. Generate a random number R for $USER_i$
6. Computes screened (Encrypted) password $NPW_i = H(PW_i \| R \oplus MRFP_i)$.
7. Compute $n_i = H(NPW_i \oplus FP_i)$
8. Compute $p_i = H(U(IDENTITY_i) \oplus n_i)$
9. Sends Fingerprint (biometric) as B_i, FP_i, n_i, p_i and NPW_i of $USER_i$ to remote server through secure channel and store them to remote server and smart card of $USER_i$.
10. Random number R is also stored on smart card of $USER_i$

B. Login Phase:

- In login phase, user $USER_i$ wants to utilize the facilities offered by smart card.
    - He/She has to insert the smart card into the input device.
    - Submit $U(IDENTITY_i)$ and PW_i.
    - Input fingerprint (biometric) B_i thorough scanner device

- *The smartcard then executes the following procedure*:

1. Verify fingerprint (biometric) $B_{i.}$ If the B_i of $USER_i$ matches the template stored in the system then carry-out the following steps otherwise reject it.
2. $USER_i$ input the password PW_i and $U(IDENTITY_i)$ then smart card computes NPW_i and n_i' as
    a. $NPW_i = H(PW_i \| R \oplus MRFP_i)$
    b. $n_i = H(NPW_i \oplus FP_i)$ and
    c. $p_i = H(U(IDENTITY_i) \oplus n_i)$
3. Then smart card compares that if n_i equals to n_i' then only proceeds step 4, otherwise system terminates the process unsuccessfully after displaying password error message.

4. After successful comparison of step 3, then smart card computes as follows
    i. $S1=((p_i \oplus n_i') \oplus R_c)$, Where R_c is random number generated by user.
    ii. $S2= H(R_c) \oplus NPW_i$

5. After calculating S1, S2 then $USER_i$ sends the messages S1, S2, and U ($IDENTITY_i$) to the remote registration Server.

C. *Authentication Phase:*

1. After accepting request for login data S1, S2 and U($IDENTITY_i$) from the $USER_i$ then remote server system and the user $USER_i$ execute the following procedure to authenticate each other.
2. Verification of U($IDENTITY_i$) takes place.
3. If the U ($IDENTITY_i$) is valid then remote server computes S3 = H (U($IDENTITY_i$) $\oplus$ n_i), S4 = S3 $\oplus$ S1, S5 = H(R_c) $\oplus$ NPW_i , S6 = (($p_i \oplus n_i$') $\oplus R_c$), S7 = S5 $\oplus$ S6 and then compare whether S1 = S4.
4. If above comparison is true then further verify S2= H(S6 || S7) if it is also true then remote server maintained (U ($IDENTITY_i$), S4,S7).
5. If above any one step does not true, then it implies that $USER_i$ is not a valid user.
6. Otherwise remote server accept the login request and thus $USER_i$ is authenticated as valid user.
7. Finally, after successful authentication the user $USER_i$ can process the benefits of smart card

VI. Conclusions

The proposed scheme provides strong authentication of the owner by verifying user's personal biometrics i.e. fingerprint, password, and random numbers generated by the user and server. Significance of our proposed scheme is security, based on biometric-fingerprint information, which cannot be stolen, forgotten or lost, so our scheme provides the ability to prevent fraudulent and genuine transactions. Besides this, our scheme is efficient and secure against various attacks, low computational workload on the smart card, and no need of password table or verification table. The proposed scheme is also user friendly and effective.

References

[1] http://www1.american.edu/initeb/sm4801a/epayment1.htm.

[2] J. Raja, M. Senthilvelmurgan, "E-payments: Problems and Prospects", Journal of Internet Banking and Commerce, Volume 13, No 1, April 2008.

[3] K. A. Akintoye, O. I. Araoye, "Combating E-Fraud on Electronic Payment System", International Journal of Computer Applications (0975 – 8887), Volume 25– No.8, Jul y 2011.

[4] PyaePyae Hun. "Design and Implementation of Secure Electronic Payment System (Client)",World Academy of Science, Engineering and Technology, 48, 2008.

[5] Dileep Kumar, YeonseungRyu. "A Brief Introduction of Biometrics and Fingerprint Payment Technology", International Journal of Advanced Science and Technology, Vol. 4, March, 2009.

[6] Chin-Chen CHANG and Jung-San LEE, "An efficient and secure remote authentication scheme using smart card", Information & Security, An International Journal, Vol.18, 2006, 122-133.

[7] Hwang and Li, "A New User Authentication Scheme Using Smart Cards".

[8] http://en.wikipedia.org/wiki/Smart_card, January 2010.

[9] http://www.popcenter.org/problems/credit_card_fraud/PDFs/Bhatla.pdf, June 2003.

[10] Giampaolo Bella, Stefano Bistarelli, and Fabio Martinelli, "Biometrics to Enhance Smartcard Security Simulating MOC using TOC", Institute of Informatics & Telematics, CNR, Pisa, Italy.

Jayesh Gaurav, Master of Computer Application. Birla Institute of Technology, Mesra Ranchi, Deemed University, Ranchi (Jharkhand), INDIA in 2005. Pursuing Ph.D. from Singhania University, Jhunjhunu, Rajsthan, INDIA. He has more than five year experience as lawyer and cyber law adviser, training and research in cyber-security and cyber laws. He is working as Lawyer and Cyber Law Adviser, Supreme Court of India.

Sanjive Tyagi, Master of Technology from V.M.R.F. Deemed University, Salem (T.N.), India in 2007, M.Sc. (Physics-Specialization in Solid State Physics) from Meerut University, Meerut (UP), India and MCA from Maharishi Dayanand University, Rohtak, (India). Ph.D. (Submitted in 2011) from Singhania University, Jhunjhunu, Rajsthan, India. The major field of study is Digital Image Processing- Steganography, cryptography and network security. He has more than ten year experience in teaching and research as Associate Professor. He is working at Radha Govind Group of Institutions, Meerut (U.P.), and India. The current research area is cyber-security.

Dr Jayanthi Ranjan, Ph.D., Chairperson-International Relations, Editorial Member: International Journal of E-CRM, International Journal of Computational Vision and Robotics, Journal of Software. Editor: International Journal of Computer and Communication Technology, Associate Editor: Journal of Applied and Theoretical Information Technology. Professor-Information Management and Systems, Institute of Management Technology-IMT.