ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
Research Article
www.ijptonline.com

# SECURING METHODS OF E-BANKING

[1]Mulpuri. Sri Sai Kalyan, [2]A.K.Reshmy
[1]UG SCHOLAR,[2]ASSISTANT PROFESSOR
Department of Computer Science & Engineering, Saveetha School of Engineering, Chennai
Email:kalyanchowdary.5233@gmail.com

Received on: 02.10.2016 Accepted on: 28.10.2016

**Abstract:**

This paper tells about the security that should be provided for the e-banking. Now-a-days security has become an important aspect in internet banking and recognized as the main obstacle in the adoption of e-banking. This paper includes Fuzzy logic model which improves the security performance and quality. This model is based on FL operators and produces four measures of security attacks. The main aim is to push the electronic transactions into practice, but the off line system will cause a great loss to e-transactions in banking. The paper presents a multi bank and offline e-cash protocol that is based on smart cards.

**Keywords:** Fuzzy logic model, E-cash, smart card, Elliptic curve

## 1. Introduction

E-banking provides the customers with easy access to banking, retrieving the balance and retrieving the account history, money transferring between the accounts[4][5]. The number of users using the internet has increased a lot. Customers like to use new technologies in internet that includes internet banking and online shopping. Online shopping provides customers with flexibility and saves them time in shopping. Since e-banking is a complex and dynamic problem, Fuzzy logic model has become an effective tool in assessing e-banking security since FL offers an approximate value rather than exact values. As the technology has been advanced and the e-commerce has been increased rapidly, the security to the e-banking is needed more. The multi-bank system has more demand since the customers can have accounts in many banks and the off-line cash payment system is given the highest priority because of its convenience and off-line facility[4]. The prevention of double spending is very important while designing the multi-bank and off-line e-cash payment systems[4]. There are two methods to achieve that:

*1. Preventing in advance:* The customer is checked whether he spends same cash twice in payment phase by smart card[7].

*2. Examining in deposit phase:* The bank will search in its paid e-cash database when the customer deposits the money, if the same record exists, then the bank can identify the double spenders[5].

## 2. Internet Banking and Fuzzy Logic

### *2.1 Internet Banking Security Architecture*

There are many threats that any internet banking system can fall into. The threats can be spoofing, denial of service, sniffing, buffer overflows, phishing attacks, social engineering[11]. Financial institutions should have proper authentication methods for their customers. The authentication methods include passwords, PIN's, digital certificates, one time passwords and biometric identification.

### *2.2 FL Expert System*

This expert system uses FL instead of Boolean logic. This approach requires sufficient knowledge in formulating rules, combining sets and defuzzification[10][12]. The FL process includes four steps: Fuzzification, inference, composition, defuzzification.

### *2.3 Designing the system*

FL produces approximate values than exact values. So this is used to evaluate and assess the security of dynamic banking websites. This also classifies the security threats, risks and vulnerabilities. This classification produces overall security score. The system can be designed in MATLAB[9]using four risks criterias as shown in table 1: direct internal attack, communication tampering attack, code programming attack, denial of service attack. Calculation of assessment of these four criterias can be computed as: (1*1+2*2+2*3+3*4+2*5)/10 = 3.3.

### *2.4Primary Inputs and Output of the System*

There are four criteria and four components related to each criteria. So totally there are six components. Each component takes one integer value as primary input. There are five output fuzzy sets: annoying, harmful, destructive, safe, catastrophic[10].

**Table 1: Layers of e-banking risk attacks criteria.**

| Criteria | No | Component |
|---|---|---|
| Direct internal | 1 | Phishing attack |

| | | |
|---|---|---|
| attack | 2 | Social engineering |
| | 3 | Brute force |
| | 4 | Insider attack |
| Communication on tampering attack | 1 | Sniffing |
| | 2 | Spoofing |
| | 3 | Port scans |
| | 4 | Page hijacking |
| Code programming attack | 1 | Sql injection |
| | 2 | Buffer overflow |
| | 3 | Cross site scripting |
| | 4 | Trojan horse |
| Denial of service attack | 1 | Ping of death |
| | 2 | Ping flood |
| | 3 | Man in the middle |
| | 4 | Smurf attack |

*2.5 Deffuzification and experimental results*

Centroid deffuzification method is used .The equation in this method is expressed as $x^* = \frac{\int \mu}{\int \mu}$

Where x* is the defuzzified output, $\mu_i(x)$ is the aggregate membership function and x is the output variable. If the security rating is low, that means the website is more secure and highly protected. If the security rating is high, that means the website is not secure and can be easily attacked or hacked[11].

When the security rating is in equilibrium, that means the website is somewhat secure and protected but can lead to some attacks.

**3. Multi-Bank and E-Cash Approach**

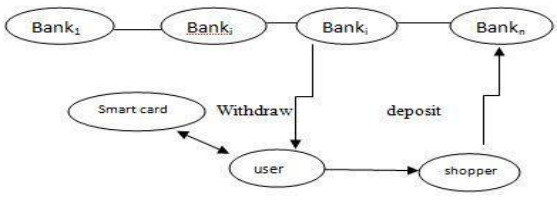


**Figure 1. Transaction flow of the multi-bank e-cash based on smart card**

*3.1 Basic description*

There are some components or parties based on this multi-banking. They are banks, the user, and the shopper. These all together completes the whole electronic trade by performing different activities.

1. Opening account: The user and shopper opens account in bank separately. The smart card is issued by the bank.
2. Withdraw: The user and the shopper withdraw the cash from their accounts on the authenticated communication.
3. Payment: The user and the shopper executes payment protocol. If it succeeds then it is ok otherwise he is the double spender.
4. Deposit: The shopper and $bank_j$ execute the deposit protocol, and the bank examines whether the transaction exists double-spending or double-depositing. If it does, the bank will reveal the user or the shopper's identity according to the different payment information; otherwise, the bank will deposit the e-cash to the shopper's account.

   The properties of this protocol are as follows:

   1. Many banks cooperate with each other,transmit information mutually, and complete the task together.
   2. Adding a tamper-against smart card to the user's electronic wallet, the smart card and the PC complete the protocols together and restrict each other[2].

*3.2 Proposed protocol*

According to the flow of transaction, the paper proposes a security multi-bank and off-line e-cash payment based on smart card using elliptic curve system. The smart card prevents the double spending by checking it in the e-cash payment database.

*3.2(a) Opening account*

To open the account, the user first has to identify himself to the bank by means of official documents like the ID card or passport, and then sign the contract.

$Bank_1$ issues a smart card to the user in which stores the smart card's private key $S_S$ ($0 \le S_S \le L$), system parameters, etc. $S_S$ is randomly generated by $bank_1$ and can't be changed or tempered. The smart card's public key $P_S=S_SP_1$ can be printed in its surface. The PC calculates and stores the user's public key $P_U=P_C \oplus P_S$ , it is easy to see that $P_U$ includes the PC and the smart card's information, so $bank_1$ can't imitate the user to withdraw the e-cash. In addition, the PC can't complete the trade independently without the smart card's participation. $Bank_1$ calculates $P_U$ as the user's account number. It is necessary to keep account number uniquely, because the account number can distinguish the users in the situation of double-spending. Each bank has a database to storage accounts. $Bank_1$ adds a new account in its database, stores $P_U$ and the user's identity information, such as ID number, balance of the account.

*3.2(b) Withdraw protocol*

When the user wants to withdraw the e-cash from his account, he must prove himself as the legitimate owner first, e.g. the user signs a withdrawal request using digital signature. The withdrawal request contains the amount of the e-cash, then $bank_1$ should judge whether $balance \geq amount$ if the smart card is forbidden to overdraw. If it doesn't hold, the protocol stops.

*3.2(c) Payment protocol*

The details of the payment protocol are described as follows:

1. The user sends the e-cash and the shopping demands to the shopper, also sends the e-cash's mark *R* to smart card.
2. The user examines $I_{pay}$.
3. The smart card searches the corresponding e-cash's sequence number $y_0$ according to *R*, if it exists the pair (*R*, $y_0 \neq 0$), shows the e-cash has not been spent yet.

*3.2(d) Deposit protocol*

The shopper transmits a copy of the payment protocol to the bank, and transmits the copy to bank 1. Bank1 verifiesand checks the validity of bank's signature, and searches in the paid e-cash database.

*3.3 Detection of double spending*

If the smart card is broken unexpectedly or the shopkeeper tries to store repeatedly, the system can still detect the double spender's identity in deposit phase and provide security to bank.

*3.4 Efficiency and security analysis*

Thus protocol is based on elliptic curve cryptography. This technique has an advantage of having a shorter key, higher security. So this is mostly used in smart cards. This also reduces the cost and complexity of the smart card and increases its performance

**4. Conclusion**

Since we are using FL model in design phase and MATLAB was used in implementation phase, the results indicate worst security rating is 87.5% and best rating is 15.6%. This also helps the banking customers to avoid direct internal attacks and secure themselves. And this paper also proposed multi-banking and offline e-cash payment schemes based on

smart card. This scheme helps in identifying the double spenders. So it is more secure. Finally this paper tells about how to secure our bank accounts, avoid and prevent the security attacks.

## 5. References


1. Wenyuan Liu, Chengyu Deng, Jingjing Zuo, et al, "Research of AFAP protocolrealizing atomicity and fair anonymity", Chinese Journal of Computers, Vol 27, No.3, pp. 413-419, Mar. 2004.
2. Xiaosong H, Chik H T, "Fair traceable off-line electronic cash in wallets with observers", Proceeding of the 6th International Conference on Advanced Communication Technology, Korea, pp. 595-599, 2004.
3. Brands S, "Untraceable off-line electronic cash in wallet with observers", Proceeding of Cryptology-Crypto1993, German, pp. 302-318, 1993.
4. Yacobi Y, "On the continuum between on-line and off-line e-cash systems", Proceeding of Financial Cryptograhpy1997, Anguilla, pp. 193-202, 1997.
5. Wenyuan Liu, Guoyu Zhao, Che7ngyu Deng, et al, "Design of multi-bank e-cash payment protocol based on elliptic curves", Journal of Beijing Electronic Science and Technology Institute, Vol 11, No. 2, pp. 19-23, Dec. 2003.
6. Haeryong P, Kilsoo C, Seungho A, "The security requirement for off-line e-cash system based on IC card", Proceeding of the 11th International Conference on Parallel and Distributed Systems, Japan, pp.260- 264, 2005.
7. A. R. Ahmad and O. Basir. Fuzzy Inferencing in the Webpage Layout Design. Working Paper. System Design Engineering University of Waterloo, Waterloo, Canada, 2003.
8. L. Zhang, P. Zhang, Y. Gong. "Flight data remote integrated analysis system based on Matlab Web Server," ELECTRONICS OPTICS & CONTROL, vol. 12, 2005, pp50-52.
9. J. Buckley and D. Tucker. Second generation fuzzy expert system. *Fuzzy Sets and Systems*, 31:271{284, 1989.
10. J. Claessens, B. Preneel and J. Vandewalle. ATangled World Wide Web of Security Issues. First Moday,Vol. 7, No. 3, 2002.
11. J. J. Buckley, , "Fuzzy complex analysis II: Integration" , *Fuzzy Sets Syst.* , vol. 49 , pp.171 -179 , 1992.