International Journal of communication and computer Technologies, ISSN: 2278-9723

Available at http://www.ijccts.org

A Reliable ATM Protocol and Comparative Analysis on Various Parameters with Other ATM Protocols

Anurag Anand Duvey[1], Dinesh Goyal[2], Dr. Naveen Hemrajani[3]

[1, 2, 3]Suresh Gyan Vihar University, Jaipur

Received: 12-08-2012, **Revised:** 19-09-2012, **Accepted:** 22-10-2012, **Published online:** 06-12-2012

Abstract: An automated teller machine (ATM) is a new banking system in which an account holder can access his/her account anytime and anywhere with bank given ATM cum Debit card. User can interact with the bank through this card. Some more facilities are there by using this machine. But system has lacks of security issues like masquerading etc. for the user. Therefore this problem encourages us to introduce an efficient system to fight with the all possible threats by using DynaPass on existing mobile network. An efficient protocol proposed here to minimize these threats. This protocol has modelled through Petrinet diagram using Tina Pro under various parameters. And finally it compared with the existing protocols on the ground of security, delay and cost.
Index terms- ATM, biometric ATM, Debt card, Petrinet diagram, modelling, DynaPass, Mobile network

I. INTRODUCTION

There are very fast changes occur in the traditional banking operation system. Before a decade ago a bank was involved only with customers when they were at premises of bank. But during this new time a bank provides many more services to the customer's at their doorsteps. The entire system of banking has changed drastically. In traditional banking system a manual teller had worked.

But now scenario has changed and one of its most valuable services to customer is providing cash through Automatic Teller Machine (ATM) at anytime anywhere [4, 11]. Automated Teller Machines (ATM) offer significant benefits to banks and their customers. The machines can enable customers to withdraw cash at more convenient times and places than during banking hours at branches. By automating services that were previously completed manually, ATMs can provide some other services to some customers on their demands. How, and by whom, these services are to be used it decide by bank and customers [2].

On most modern ATMs, the customer is identified by inserting a plastic card called ATM cum Debit card with a magnetic stripe or a chip, that contains a unique card number and some security information such as an expiration date, CVV (Card Verification Value) etc. Authentication is provided by the customer entering a personal identification number (PIN). Using an ATM cum Debit card, customers can access their bank accounts in order to make cash withdrawals, and check their account balances. If the currency being withdrawn from the ATM is different from that which the bank account is denominated in (e.g. withdrawing US Dollars from a bank account containing Indian Rupees in USA), the money will be converted at an official wholesale exchange rate. Thus, ATMs often provide one of the best possible official exchange rates for foreign travellers and are heavily used for this purpose as well. ATMs rely on authorization of a financial transaction by the card issuer or other authorizing institution via the communication network. This is often performed through an ISO 8583 messaging system. ATMs typically connect directly to their host or ATM Controller via either ADSL or dial-up modem over a telephone line or directly via a leased line. Leased lines are preferable to plain old telephone service (POTS) lines because they require less time to establish a connection. Less-trafficked machines will usually rely on a dial-up modem on a POTS line rather using a leased line, since a leased line may be comparatively more expensive to operate versus a POTS line.

But there are some security constraints with ATM cum Debt card facility. Bank provides a 4-digits password called PIN with ATM cum Debit card which user can change at any time through ATM machine. This password is static type i.e. once set it; access will be done after using this. User set the password with easy going numbers like date of birth, vehicle number etc. in most cases so the chances to hack it more. This is the main problem by which this work can solve. There are various attacks like shoulder surfing, data skimming, fake machine etc. In this paper we proposed an efficient and reliable protocol to minimize these attacks using existing mobile network.

The remainder of the paper is organized as per following: In section II, we gave an overview of related work. Section III includes description of the work proposed and its methodology; in section IV, we have discussed about modelling and result analysis. Our proposed protocol compared with two existing protocols on three parameters- security, delay and cost. And finally in section V, we gave a conclusion of the work and a brief regarding the future work.

II. RELATED WORK

The modelling and description of an Automated Teller Machine (ATM) are a typical design case in safety-critical and real-time systems. As a real-time control system, the ATM system is characterized by its high degree of complexity, intricate interactions with hardware devices and users, and necessary requirements for domain knowledge. All these factors warrant the ATM system as a complex but ideal design paradigm in large-scale software system design in general and in real-time system modelling in particular.

There is a lack of systematically and detailed documentation of design knowledge and modelling prototypes of ATM systems and a formal model of them in denotation mathematics and formal notation systems. This paper presents the formal design, specification, and modelling of the ATM system using a denotation mathematics known as Real-Time Process Algebra (RTPA) [1]. According to the RTPA methodology for system modelling and refinement, a software system can be specified as a set of *architectural* and *operational components* as well as their interactions. The former is modelled by *Unified Data Models* (UDMs), which is an abstract model of system hardware interfaces, an internal logic model of hardware, and/or an internal control structure of the system. The latter is modelled by *static* and *dynamic processes* using the *Unified Process Models* (UPMs) [4]. If we are looking for related problems in financial transaction by wireless network, we came to know about the facts as under below. According to Gao et al.[5], mobile payment refers to wireless-based electronic payment for m-commerce to support point-of-sale/point-of-service (POS) payment transactions using mobile devices. As discussed in [4], the existing m-payment systems can be classified into three major types. The first type is account-based payment systems which can be mobile phone-based, smart card or credit-card m-payment systems [6, 7, 8, 9 and 10].

Apart then it, there is a technique for ATMs and it is biometric. The main cause to use biometrics is to uniquely identify or verify an individual through the characteristics of the human body. Biometrics uses characteristics that can be physical like finger prints, facial characteristics, voice, iris scan, or DNA. Biometric technology should first gather information into a computer database i.e. a database of finger prints or thumb impressions. The computer will compare this with new sample and recognize if matches. Now it can be used for both identification as well as verification.

For biometric identification, a biometric system searches the database for a match with newly captured sample and grants to access if it is found. The login process to a computer using a finger print or thumb impression is an example of this mode. For biometric verification, a biometric system searches the database for a match to the newly captured sample, and authenticates an individual's claimed identify from his or her previously enrolled pattern. Unlock a door using palm scanner or iris scanner is an example of this mode. The current biometric technologies are palm print recognition, fingerprint recognition, hand geometry, dynamic signature, vascular pattern recognition, iris recognition, face recognition, speaker recognition.

Nowadays the maximum numbers of biometric ATMs are used in Japan. Banks in Mexico, South America, Africa and the Middle East are also moving toward the new technology. In the current market, Western banks and financial institutions are already set to integrate biometric technology with mass market banking.

Today's biometric scanners go far beyond basic fingerprint recognition. According to security experts, fingerprints can easily be lifted and replicated. The most secure biometric technology uses a device designed to perform an Iris scan based on more than 2000 unique measurement points.

A. Fake ATM:- A fake ATM tells the machine which is similar to genuine machines. Attacker may install it in place of genuine machine. Nowadays, user can not authenticate the ATM. If user will use this machine definitely he should share all his account information and PIN also. No doubt it is a big threat but in India, it is very typical task to perform. In the survey we have not found any case of this type.

B. Shoulder Surfing:- Through a video camera or directly, it is possible to an attacker to know the PIN. It is easier to know at merchant's machine where a user gives to the ATM card for payment and video cameras capture a video for the same. Sometimes using skimming machines attacker can record all account information and forge an ATM card.

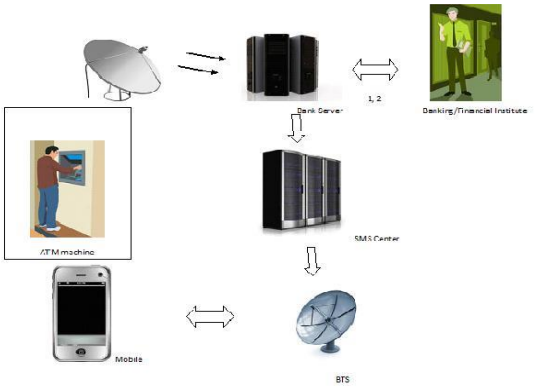
C. Skimming Devices:- The skimming devices can be attached with ATM machine and steal data of multiple ATM cards. Mostly this type of attack is to be done at merchant's machine where user gives ATM card for payment purpose. In the survey, Reserve Bank of India reports told that this is very common threatening in India last many years.

D. Fake key-pad overlay attack:- Attacker may place a fake keyboard overlay upon a real keypad. Then this fake overlay stores pressed key-pad buttons with time. This information can be used to compromise PIN. Now it is easy to an attacker to use an ATM card of any user.

III. PROPOSED METHODOLOGY

Main objective of this work is to enhance the security of customers using ATM. If there is an additional security of getting dynamic password on mobile phone called DynaPass for each and every transaction with account generated then it will give at least hundreds times secure operation for an individual who has lost his/her ATM at any instance. In addition to that the operation will be secured by misusing after the incomplete operation since on transaction the operation will demand new dynamic password. So that in this proposed work we are introducing new authentication system which is secure and highly usable, based on multifactor authentication approach. It uses a novel approach to create an authentication system based on DynaPass and SMS to enforce an extra security level over the traditional login in an ATM machine. The DynaPass is most sensitive data for any financial transactions, so we are storing

DynaPass in encrypted format on user's cell phone. The Bank or Financial institutions are responsible for DynaPass generation and distribution to their customers.

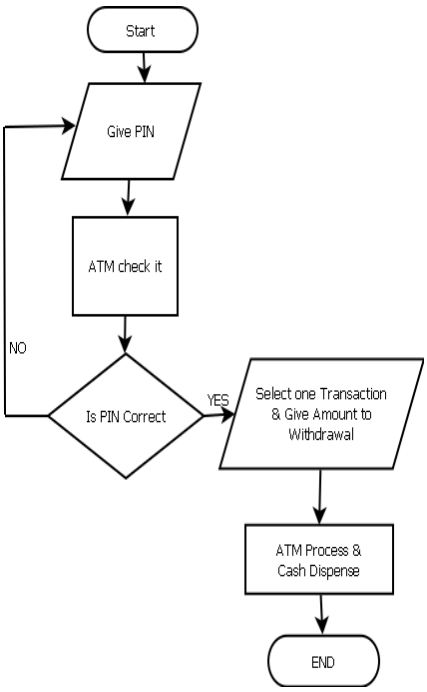


The customer goes to the ATM machine insert the card to the machine and enter the pin number. The Bank (Control system) authorizes the user and if that is a valid customer let the customer to enter the value for the withdrawal otherwise, the transaction ends and the machine returns the card.

For the next step the control systems checks the available balance and process the transaction if possible (assuming the system does not let the balance to become negative). If the transaction is impossible, an error message is displayed and the system prompts to enter another transaction. At any time when prompted to enter a transaction, the user may cancel, at which point the ATM machine will close the session and eject the card. Finally, ATM machine prints the receipt and ejects the card.

Fig. 1 Proposed Process of ATM transaction

A. The Flow Chart and the Algorithm for ATM transaction is as follows:



Step 1. User accesses his account using Debit card through ATM machine with help of PIN.

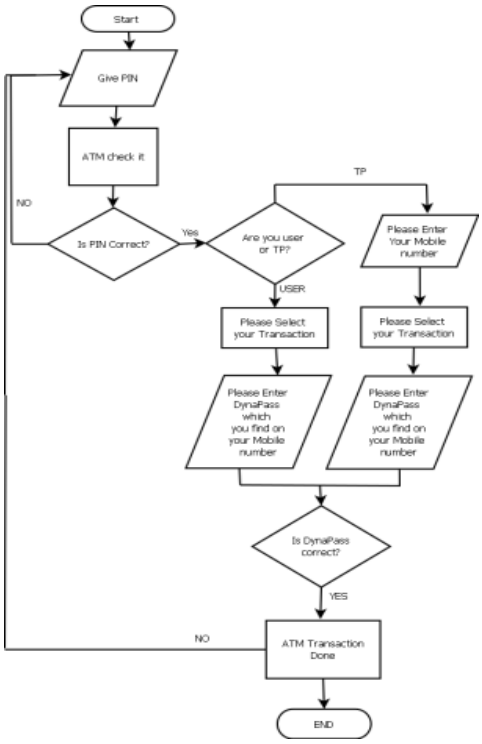
Step 2. ATM machine reads this card and check it with Bank server.

Step 3. And now ATM waits to enter the transactions request.

Step 4. User may use ATM now and transact.

Fig2. Flow chart for ATM using PIN

B. The flow chart and the Algorithm for proposed model for ATM transaction is as follows:



Step 1. User accesses his account using Debit card through ATM machine with help of PIN.

Step 2. ATM machine reads this card and it checks the PIN with Bank server through dedicated network.

Step 3. Bank server now connects to SMS center with an arbitrary password which called DynaPass (Dynamic Password).

Step 4. SMS center now send this password to BTS (Base Transceiver System) with the help of mobile phone network.

Step 5. BTS then deliver it to user's cell phone.

Step 6. And finally user gets this dynamic password (DynaPass) and will be entered it to ATM machine.

Step 7. ATM machine again confirms this DynaPass with Bank server and now it responds to Banking Institute.

Step 8. Now required financial transaction will be successfully done.

Fig3. Flow chart of Mobile DynaPass for user & TP

C. The Algorithm for proposed method for ATM transaction using third party authentication is as follows:

We here proposed third party authentication also. For the same it is required to register three or four persons including their mobile numbers through his debit card. Only these registered people may do the financial transactions on behalf of the user. User may fix their limit also for per day transactions.

Step 1. Bearer accesses user's account using Debit card through ATM machine with help of password (PIN).

Step 2. ATM machine reads this card and after giving password it connects with Bank server through dedicated network.

Step 3. Now ATM gives options – A. USER & B. BEARER. Chose B and enter the mobile number on which user registers him previously to get dynamic password (DynaPass).

Step 4. Bank server now checks this mobile number and then responding to SMS center with an arbitrary password which called DynaPass and sends an informative message to the user.

Step 5. SMS center now send password and message to BTS with the help of mobile phone network.

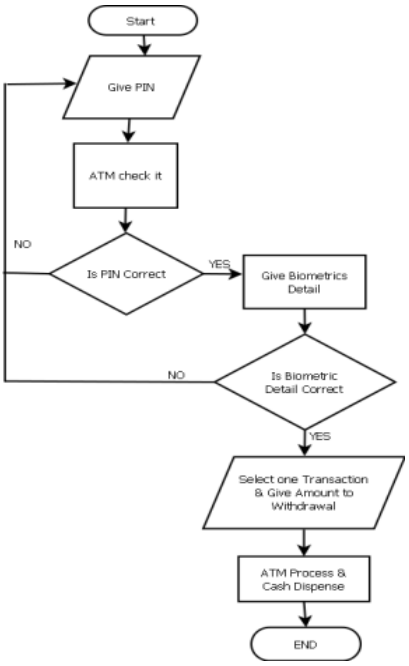
Step 6. BTS then deliver these to bearer and user's cell phone respectively.

Step 7. And finally bearer gets this dynamic password and he will be entered it to ATM machine.

Step 8. ATM machine again responds with Bank server and now it connects to Banking Institute.

Step 9. Now required financial transaction will be successfully done.

D. The Algorithm of Biometric based ATM transaction is as follows:



Step 1. User accesses his account using Debit card through ATM machine with help of PIN.

Step 2. ATM machine reads this card and check it.

Step 3. If PIN found ok, now it asks for biometric data.

Step 4. If PIN not matched go to Step 1.

Step 5. Now this new data will check with the stored biometric data on bank server.

Step 6. If both are same Now ATM waits to enter the transactions request.

Step 7. If there is some difference between biometric data go to Step 1.

Step 8. User may use ATM now and transact.

Fig 4. Flow chart of Biometric ATM

IV. RESULT ANALYSIS

1. Protocol validity- We have used Tina 2.1.0 to check validity of trio protocols. Using Petrinet diagrams those protocols check on three parameters-bounded, live and reversible.

- **Bounded** means protocol ends in certain a time.
- **Live** means all transactions in Petrinet diagram are in working.
- **Reversible** means protocol may use reverse path if there is any problem at any transition.

2. Comparative performance analysis for these protocols as per followings-

a. **Delay-** In data communication a complete data reached at its destination in a certain time. This time is known as delay.
b. **Security-** How secures the transactions of ATM machines in terms of customer point of view and bank point of view also?
c. **Cost-** What installation cost for the ATM machines will paid by banks and customers.

Table-1

Parameters → / Protocol ↓	Delay	Security	Cost
Using only PIN	Less	Less	Less
Using Biometric	More	More	More
Using DynaPass	Moderate	More	Moderate

Table-2

Parameters → / Protocol ↓	Bounded	Live	Reversible
Using only PIN	Yes	Yes	Yes
Using Biometric	Yes	Yes	Yes
Using DynaPass	Yes	Yes	Yes

Delay calculation of the data on the basis of per transaction by ATM machine in those trio protocols.

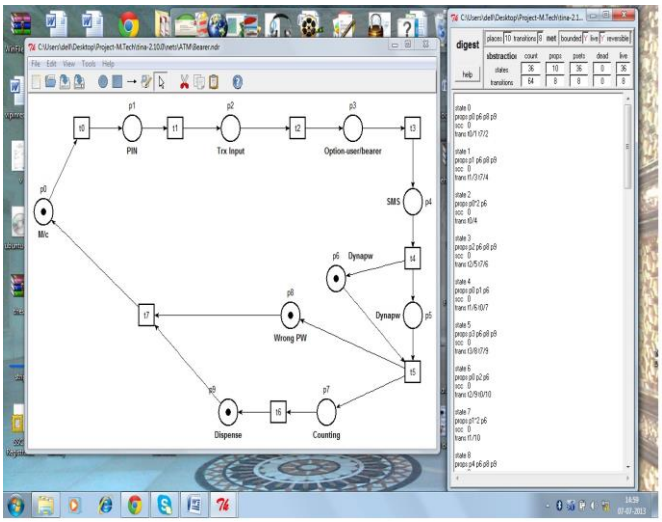


Fig 5. TiNA tool –network design for dyna pass

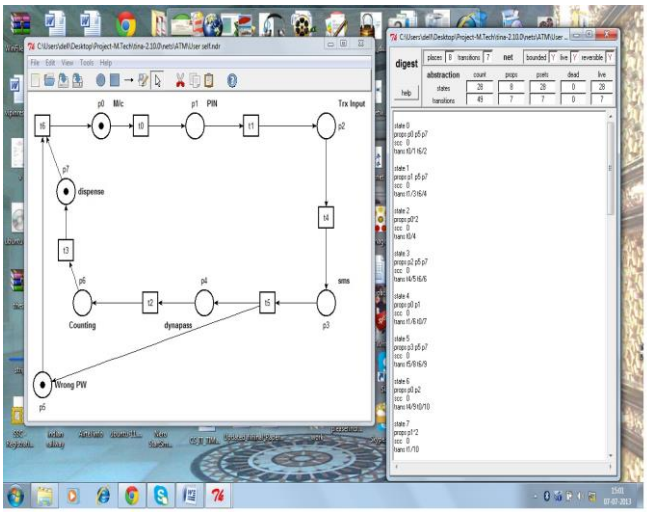


Fig 6. TiNA tool –network design for biometric ATM

Data length varies in these protocols and only this is the main cause for delay time. So following comparison assume for the same.

V. CONCLUSION & FUTURE WORK

In this paper the proposed protocol is proved through Petrinet diagram. From above mentioned tables we can understand that the transaction through DynaPass is very much secure as compared with conventional and less storage space complex with biometric ATMs. Transaction time and cost for per transaction is moderate in this protocol. Biometric ATMs have more cost because of heavy storage space for the biometric data. Proposed technique is fruitful to the banks as well as customers due to use of existing mobile services.

As we know the security threats in banking systems are increasing day by day. It is a measure challenge to banks to maintain it at appropriate level. In future customers have no debt cards i.e. card less banking and ATM will respond with their mobile smart phones. They only have a unique number and getting DynaPass through mobile every time they want to transaction with the ATM.

VI. REFERENCES

1. *Nitin Munjal and Rajat Moona. "Secure and Cost Effective Transaction Model for Financial Services". OPNTDS-09, 2009*
2. *James J. MCAndrews "Automated Teller Machine Network Pricing – A Review of the Literature" Review of Network Economics Vol.2, Issue 2 – June 2003*
3. *A. Gaurav, A. Sharma, V. Gelara, and R. Moona. "Using Personal Electronic Device for Authentication-Based Service Access". In Communications,2008, pages 5930–5934. ICC"08, IEEE International Conference, May 2008*
4. *Wang Y., An operational semantics of real time process algebra (RTPA), International Journal of cognitive informatics and natural intelligence, p.p. 71-89, July-Sept 2008*
5. *Wang Y., Zhang Y., The formal design model of an automatic teller machine (ATM), 2(1), p.p. 102-131, January-march 2010*
6. *White paper: AEP Smartgate Security, Strong Multi Factor User Authentication for secure information haring, white paper, AEP Networks, December 1998, http://www.aepnetworks.com/products/downloads*
7. *J. Gao, J. Cai, K. Patel, and S.Shim: (2005), Wireless Payment, Proceedings of the Second International Conference on Embedded Software and Systems (ICESS05), China, pp. 367-374, .December 2005.*
8. *S. Kungpisdan, B. Srinivasan and P.D. Le: (2004), A Secure Account-Based Mobile Payment Protocol, Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE CS press, Las Vegas USA, volume 1, pp. 35-39. April 2004.*
9. *Y.B. Lin, M.F. Chang, H. C.H. Rao: (2000), Mobile prepaid phone services, IEEE Personal Communications, vol. 7, pp. 6-14, June 2000.*
10. *A. Fourati, H.K.B. Ayed, F. Kamoun, A. Benzekri: (2002), A SET Based Approach to Secure the Payment in Mobile Commerce, In Proceedings of 27th Annual IEEE Conference on Local Computer Networks, Florida, pp. 136 - 140, November 2002.*