ATM Transaction using One Time Password (OTP)

Dr. K. Mohan Kumar[1] P. Vinothini[2]
[1]Research Guide & HOD of Department [2]Research Scholar
[1,2]Department of Computer Science & Engineering
[1,2]Rajah Serfoji Government college, Thanjavur 613 005. Tamil Nadu, India

Abstract— This study proposes a secured ATM (Anytime Money) System using a card scanning system along with OTP password received through SMS to improve security. Usual ATM systems do not contain the OTP feature for money withdrawal. If an attacker manages to get hold of ATM card and the pin Number, he may easily use it to withdraw money frequently. So this proposed system supports the ATM card scanning system along with an OTP system. The user may scan his card and login to the system. After entry into the system, the user can view the details. But the user can't do the transaction to withdraw the money. In this situation user should enter the OTP which is received from mobile phone. So, OTP should be generated and send to the user's authenticated mobile phone in order to withdraw money. Thus this new system provides a totally secure way to perform ATM transaction with two level security structure.

Key words: ATM, One Time Password, OTP

I. Introduction

An automated teller machine (ATM) is an electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller. Anyone with a credit card or debit card can access most ATMs. The first ATM appeared in London in 1967, and in less than 50 years, ATMs spread around the globe, securing a presence in every major country and even tiny little island nations such as Kiribati and the Federated States of Micronesia. There are two primary types of ATMs. Basic units allow customers to withdraw cash and receive reports of their account balances only. The more complex machines accept deposits, facilitate line of credit payments and report account information. To access the advanced features of the complex units, a user must be an account holder at the bank that operates the machine. Analysts anticipate ATMs will become even more popular and forecast an increase in the number of ATM withdrawals. ATMs of the future are likely to be full-service terminals instead of or in addition to traditional bank tellers. In some banking networks, the two functions of ATM cards and debit cards are combined into a single card, simply called a "debit card" or also commonly a "bank card". These are able to perform banking tasks at ATMs and also make point-of-sale transactions, with both features using a PIN.All ATMs, at a minimum, will permit cash withdrawals of customers of the machine's owner (if a bank-operated machine) and for cards that are affiliated with any ATM network the machine is also affiliated. They will report the amount of the withdrawal and any fees charged by the machine on the receipt. Most banks and credit unions will permit routine account-related banking transactions at the bank's own ATM, including deposits, checking the balance of an account, and transferring money between accounts. Some may provide additional services, such as selling postage stamps. Some ATM cards can also be used at a branch, as identification for in-person transactions [1].

Fig. 1: ATM Transaction

A. *Different Types of ATM Are as Follows [2]*

1) Onsite ATM -within the premises of bank
2) Off-site ATM - Outside the bank premises
3) Worksite ATM-Is located within the premises of an organization and is generally meant only for the employees of the organization.
4) Cash Dispenser-Allows only cash withdrawls,balance enquiry and mini statement requests, cash dispenser(CD)
5) Mobile ATM- refers to an ATM that moves in various areas for the customers. Few private banks have introduced ATM on wheels.
6) White Label ATM - Provided by NBFC
7) Green Label ATM - Provided for Agricultural Transaction
8) Orange Label ATM - Provided for Share Transactions
9) Yellow Label ATM - provided for E-commerce
10) PINK label ATM---women banking
11) BROWN label ATM-- ATM are those Automated Teller Machines where hardware and the lease of the ATM machine is owned by a service provider--but cash management and connectivity to banking networks is provided by a sponsor bank .

II. Problem in ATM transaction [3]

Life has definitely become simpler by using automated processes and one prime example of it is ATM facility. But unfortunately nothing in this world is fool proof. Many time users have faced problems in using ATM. A common problem faced by users is that the cash not being dispersed and account still being debited with equivalent amount. It becomes a very tedious process of getting this resolved.

A. *Things to be kept in Mind While doing ATM Transactions*

Firstly, the transaction slip is a very important document which comes to help. This slip come handy coz it contains all the important information about your ATM transaction as given below. Name of the ATM Bank –This refers to the ATM of the corresponding bank in which the transaction was made. Location –The ATM branch. Date of transaction –The date at which the transaction was made Time of transaction – The time at which the transaction was made Transaction reference number –This is generally an 8-9-digit number which appears on the transaction slip. Response Code Card No/Account Number– only the last 3-4 digits will be visible Nature of Transaction – Nature of transaction refers to the activity which was carried out while using the card, such as withdrawing cash, updating account details etc.

B. *Money Transfer Problem is Another Big Problem*

It generally happens for three reasons.

1) Payment Declined

By Your Bank The most common reason for an unsuccessful card payment is that your bank has declined it. This means they have sent a 'Do Not Honour' response to Transfer Wise. It's normal for them to stop a payment that they might perceive to be unusually large or to a new and unknown recipient - just in case.

2) Browser Issues

Some anti-virus or firewall software can affect your card payment. With anti-virus software, please add Transfer Wise to the list of "safe merchants". Please also make sure that any anti-virus or firewall software that you have installed will allow pop ups.

3) Insufficient Funds

Your bank might also stop your card payment if there isn't enough money in your account or if you have a per-transaction limit. They could also be treating your payment as 'cash withdrawal'. The card limits vary from card to card and from bank to bank

C. *Machine don't Accept the ATM Cards*

Some time machine doesn't accept the ATM cards. A variety of factors can disrupt this process and result in the card being declined.

1) Inadequate Balance

A common reason for a card being declined is a balance that is too low to support the requested transaction. You may have less money in your account than you thought, or a previously-made transaction, like a deposit, may not have cleared. Take into consideration both your request and the associated ATM fee.

2) Account Changes

If your account is frozen for any reason, your ATM card will likely be declined. For example, if you recently experienced a number of overdrafts, reported a card missing or stolen, or had a fraud alert put on your card, a machine will likely decline it and, in some cases, even retain the card and not give it back to you. If your card has expired, this, too can trigger a decline notice. Many financial institutions also limit how much money you can take from an ATM in a 24-hour period. If you've surpassed this number, your card may be declined.

3) Wrong PIN

If you enter the wrong PIN, or personal identification number, your card may be declined. In most instances, the machine will prompt you to retry the PIN, but if you enter it wrong repeatedly, the ATM may hold your card in an effort to ensure that it is not being used illegally by someone else.

D. *Problems Faced by BANK*

1) Theft Money from ATM's

Bank thefts are getting sophisticated by the day. Let alone retrieving your money the customer know how it was stolen in many cases. Some customers even lost lots of amount after using that ATM.

2) Cloning Problem in ATM

A type of fraud which occurs when an ATM is compromised by a skimming device, a card reader which can be disguised to look like a part of the machine. The card reader saves the users' card number and pin code, which is then replicated into a counterfeit copy for theft. Cloning occurs mainly by replicas presented in ATM system. It will extract the data presented in the magnetic tape of a card .The data is send to the memory chip which is attached to the replica The closed circuit camera will extract the password which are entered in our ATM system. They will prepare fake ATM's cards and draw the money from those cards.

3) Problems of Sms Alert of Aim's

If server gets down. This kind of problem occurs in ATM system. You will be very disappointed when you didn't get any sms regarding whether your money debited or credited.

4) Problem of Skimmers

Credit card skimming is a type of credit card theft where crooks use a small device to steal credit card information in otherwise legitimate credit or debit card transaction. Credit card skimmers are often placed over the card swipe mechanism on ATMs and gas stations, but they skimmers can be placed over almost any type of credit card reader. ATMs, the crooks may also place a small, undetectable camera nearby to record you entering your PIN. This gives the thief all the information needed to make fake cards and withdraw cash from the cardholder's checking account. There is more problem too. These are, system problem ATM (including server down), system failure (system crash or the software not work properly), hack the bank's site which affect whole banking system.

E. *Different types of ATM Fraud [4]:*

1) Card skimming
2) Salisi gang
3) Cash Trapping
4) Fake assistance
5) Shoulder surfing
6) Eavesdropping
7) Fake PIN Pad Overlay
8) Hold-Ups

1) Card Skimming

This is done by using a card reader that can capture the data in the magnetic strip of a card. One bold move done by these criminals includes installing a card reader right on top of the ATM's card slot. With this device, once a card is inserted, data will automatically be captured. Such card readers, measuring 1″ x 1″ are being sold in the internet for a very low price and with complete instructions. This scheme, though, is more popular in credit cards because the 'take' is higher compared to ATM cards.

2) Salisi Gang

Another type of ATM fraud is called the Salisi Gang aka I pit Gang or Laglag Barya Gang. This is fairly common during paydays when there is a long line of cardholders at the ATM.

a) How the Salisi Gang Works

When the cash being withdrawn is about to be dispensed by the ATM, a member of the gang will drop several loose bills and then point to the unsuspecting cardholder for help. Once the cardholder tries to pick up the bills, another gang member will immediately get the cash waiting at the cash out shutter and then disappear out of sight as fast as he can. It will be too late when the cardholder realizes what actually happened when he/she tries to get the money being withdrawn.

b) Another Version of This

When the cardholder is about to retrieve his/her ATM card right after withdrawal, one of the gang members will cut-off, get the card coming out of the card slot, and replace it with a similar looking card. All of these will happen in just a split second. The unsuspecting cardholder, without realizing what had just happened, will get his/her 'card 'and immediately leave. The gang member, who had already seen the PIN during withdrawal, will then use the stolen card in other ATMs and try to withdraw the remaining balance before the card is reported as 'stolen '.

3) *Cash Trapping*

The proliferation of fraud and crimes committed in the ATMs have surfaced anew and become more sophisticated and the perpetrators bolder than before. The most common is the so-called cash trapping perpetrated by the notorious group called Ruler Gang. They were given that name because of the device they use in trapping the cash that looks like a ruler. In the U.S., the device is called the False ATM Presenter.

a) How Cash Trapping Works

A member of the gang will install a specially fabricated "ruler" device onto the cash out shutter of the ATM and leaves it there. This device looks exactly like the cash out shutter of the machine. When an unsuspecting cardholder tries to withdraw, the cash will be trapped inside (it is actually glued at the back of the device). After a while, the cardholder, thinking there is something wrong with the machine or with his/her transaction, will leave frustrated and disappointed. Thereafter, the gang will remove the device with the cash still glued on it using their special prying tool.

F. *Fake Assistance*

"May I Help You?" is another ATM fraud employed by notorious elements preying on the elderly and those new in having an ATM card. Once these perpetrators spotted one, they will appear to be very helpful and offer assistance to the unsuspecting cardholder but in truth, these perpetrators are already memorizing the card number and PIN. With the card number and PIN, the gang can easily transfer the funds to their own bank account using the internet or mobile phone or a clone ATM card. There are other fraud and crimes committed in the ATM because of the fact that it is where the money is. Listed below are other fraud and crimes, although not as popular as those discussed above, which are committed at the ATMs.

G. *Shoulder Surfing*

That's why it is very important to be aware of the person or people around the ATM machine when you transact. If a person or people is too near to you when you transact you can advise them to move a little bit backward. This is literally looking over the shoulder of the cardholder to see the PIN as it is being keyed in. This compromises the PIN of the cardholder without his/her knowledge. There is a high-tech, knowledgeable group which is popular in the internet that installs small cameras to see the actual PIN being keyed-in by the cardholder.

H. *Eavesdropping*

This is similar to the scheme above although this time, the PIN is determined by the culprit thru deciphering the tone denoting a particular number with each press of the keypad.

I. *Fake PIN Pad Overlay*

A device similar to the machine's keypad is placed right on top of the ATM keypad and captures the PIN entered by the cardholder. Before you transact to the ATM machine, kindly inspect anything that is suspicious on the machine itself.

J. *Hold-Ups*

A scheme that is similar in a way to the one above but here, the cardholder is held-up at gunpoint or with a knife by a hold-upper after withdrawing from the ATM. This is very common ATM fraud here in the Philippines.

This usually happens in paydays like 15th and 30th of the month. We need to be aware of this to help prevent happening to us. Best way to prevent this is to transact on ATM machine that are in safe places like banks (inside), malls and other places that has security and well lighten. Now that we know the different types of ATM fraud and crimes, this will really help us be aware of our activity when transacting thru the ATM. This information can help us identify and detect ATM fraud activities and take necessary action.

Fig. 2: Secure ATM Transaction

III. METHODOLOGY

The following Figure-3 depicts the new proposed method to do transactions using ATM [2].

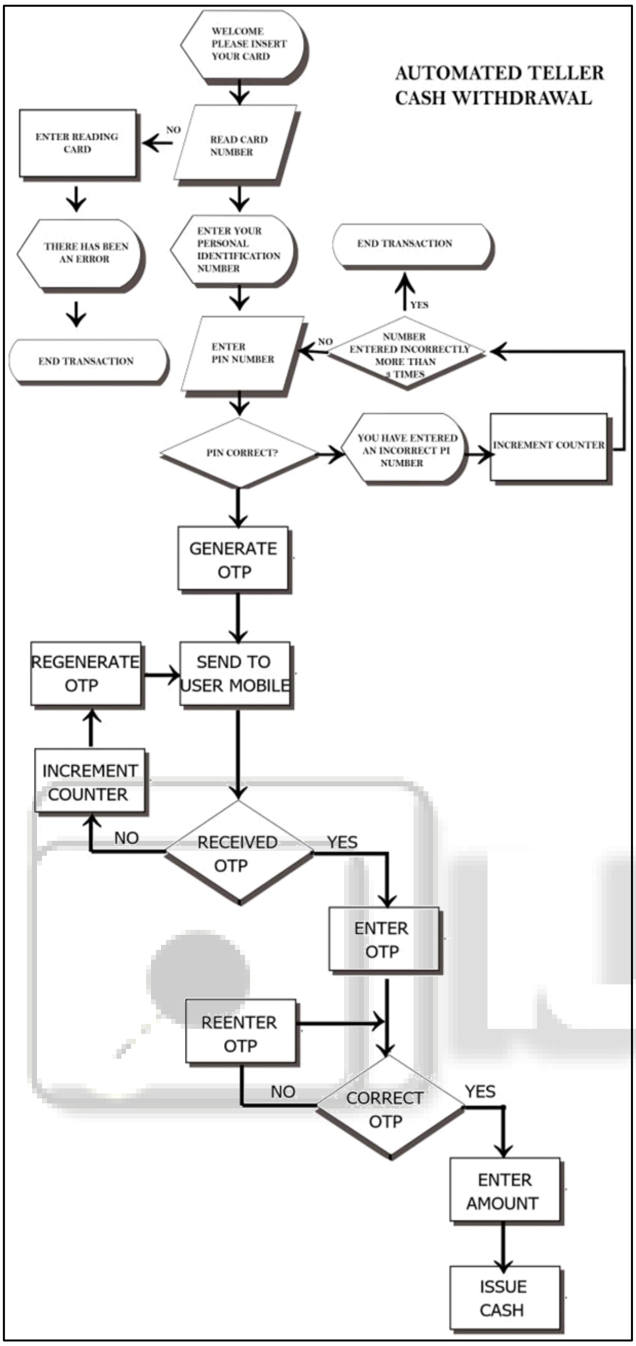

Fig. 3: ATM Transaction

A. The following Steps are needed to Perform ATM Transactions

1) Step 1: Read card number: Number is a credit card number having 16 digits. The entire digits don't have a meaning. First digit is 4 for VISA, 5 for MasterCard, 6 for Discover/Diners Club, 3 for American Express/Diners Club (those are shorter than 16). Also, first 6 digits for Visa and MasterCard are code numbers for the issuing institution.
2) Step 2: Enter your personal identification number: A personal identification number (PIN, pronounced "pin"; is often spoken out loud "PIN number" by mistake) is a numeric or alpha-numeric password or code used in the process of authenticating or identifying a user to a system and system to a user. PIN is commonly used in mobile phones where after three tries of entering the pin code the user is asked to inter the Personal unblocking code. The personal identification number has been the key to flourishing the exchange of private data between different data-processing centres in computer networks for financial institutions, governments, and enterprises. PINs may be used to authenticate banking systems with cardholders, governments with citizens, enterprises with employees, and computers with users, among other uses.
3) Step 3: Pin Correct: A personal identification number (PIN) is a secure alphanumeric or numeric code used for authenticated access to a system. The PIN provides security when a credit/debit card is lost or stolen because the PIN must be known prior to making money withdrawal.
4) Step 4: Number entered incorrectly more than times: If you enter the wrong iCloud Security Code too many times when using iCloud Keychain, your iCloud Keychain is disabled on that device, and your keychain in iCloud is deleted. You might see one of these messages. “Security Code Incorrectly Entered Too Many Times. Approve this iPhone from one of your other devices using iCloud Keychain. If no devices are available, reset iCloud Keychain.”. “Your iCloud Security Code has been entered too many times. Approve this Mac from one of your other devices using iCloud Keychain. If no devices are available, reset iCloud Keychain.”
5) Step 5: Generate OTP: A one-time password or pin (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cell phone) as well as something a person knows (such as a PIN).The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.
6) Step 6: How OTPs are generated and distributed: OTP generation algorithms typically make use of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict

future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below: Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter. There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging. Finally, in some systems, OTPs are printed on paper that the user is required to carry.

7) Step 7: Send mobile OTP: MSGWOW OTP (one-time password) solution allows enterprises to power their mission-based messaging in line with the customer’s requirements and preferences. SMS based confirmatory solutions that outweigh heavy data volumes, message latency and geographies, OTP (one-time password) are immensely useful in online transactions like account activation, bill payment confirmation, verification of user registration, mobile number validation, etc. wherever trustworthy authentication support is important.
8) Step 8: Enter OTP: It is a unique 6-character code that can only be used once and is sent only to your registered mobile number in BDO Online Banking. After encoding your user ID and password, you will also be required to enter the correct OTP to complete the login process.
9) Step 9: Correct OTP: What is One-Time Password (OTP)? It is a unique 6-character code that can only be used once and is sent only to your registered mobile number in BDO Online Banking. After encoding your user ID and password, you will also be required to enter the correct OTP to complete the login process.
10) Step 10: Re Enter OTP: It is a unique 6-character code that can only be used once and is sent only to your registered mobile number in BDO Online Banking. After encoding your user ID and password, you will also be required to enter the correct OTP to complete the login process.
11) Step 11: Deposit money: Put money in your account, either by going to the bank and filling in a form, or through the ATM. This will show up as a credit.
12) Step 12: Withdraw money: Take money out of your account, either through an ATM, or from a teller at the bank, or by asking for cash when you buy something. This will show up as a debit.
13) Step 13: Balance: The amount of money you have in your account on a particular date. Savings account: An account that lets you leave money with the bank and which pays you interest (a percentage of the amount you have in your account).
14) Step 14: Cheque account: An account for everyday transactions that also comes with a cheque book.
15) Step 15: Deposit money: Put money in your account, either by going to the bank and filling in a form, or through the ATM. This will show up as a credit.
16) Step 16: Withdraw money: Take money out of your account, either through an ATM, or from a teller at the bank, or by asking for cash when you buy something. This will show up as a debit.
17) Step 17: B-alance: The amount of money you have in your account on a particular date. Savings account: An account that lets you leave money with the bank and which pays you interest (a percentage of the amount you have in your account). Cheque account an account for everyday transactions that also comes with a Cheque book.
18) Step 18: Internet banking: A way of managing your bank accounts on the internet. You can make payments to other people and to companies directly from your account. Different banks have different security measures to keep your money safe Bank fees and charges: An amount of money that you must pay on every transaction, or a fixed monthly fees.
19) Step 19: Teller: Employee at the bank who can help you with everyday transactions such as withdrawing or depositing money. You may also have a personal banker who can help you decide on what accounts you want.
20) Step 20: International money transfer: A way of transferring money from an account in one country to another. Banks and other institutions will charge fees for doing this.

– Automated Teller Machines (ATM)

It is very easy to use and convenient way to access your bank account. If you're newly get your ATM card from bank and it is not working, don't worry. Some bank takes 24 hours to active their ATM cards. So now you can withdrawal cash from your bank account from almost anywhere. Try to use your ATM cards and your ATMs from the same bank, otherwise some services may not be available if your card and ATM don't match.

21) Step 21: Insert Card-ATM cards comes in two types — debit cards and credit cards. Debit cards are mostly used in ATMs, and it offers you to withdrawal cash which you have in your savings account. Vice versa from credit card you could credit money from your account. But in today’s topic we will discourse about the process of withdrawal money from ATM through your card. Now first insert your ATM card in the ATM machine. (you may see a blinking green light in the machine, where you have to put your card.) Please mind to insert your card as the picture shows; otherwise the machine could not be able to read your card.
22) Step 22: Select your language - This is the easiest task to do me think. Select the language you like.

IV. RESULT & ANALYSIS

The following Table-1 shows the performance analysis of proposed and existing method used in ATM transaction to receive the money from the ATM machine.

METHOD	TIME	SECURITY
Existing Method	Less (1)	Not Adequate (1)
Proposed Method	More (2)	Better (2)

Table 1: Performance analysis

The following figure 4 shows the graphical representation of the above table-1

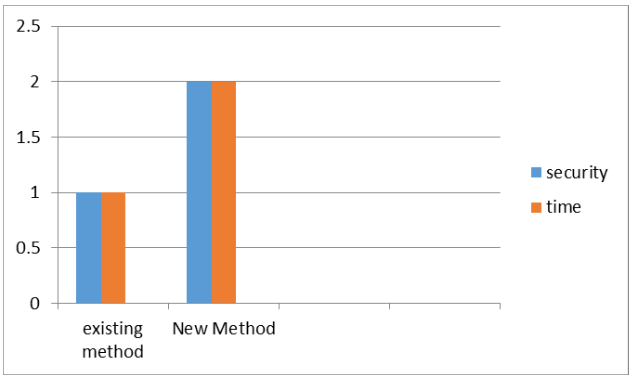

Fig. 4: Performance Analysis

The above Figure4 give an idea that in the new method security aspects is doubled compare with the existing method. Even though the time factor is increased it will not be considered while thinking about the severe attacks will cause the loose of money at great extent.

V. CONCLUSION

ATM security is one of the important thing for every human being. Normally the user enters the ATM PIN number to withdraw the money. In this case OTP is needed in every transaction to withdraw money in addition to the normal PIN number. This increases the security aspect tremendously. This idea assures more security and better performance after the implementation. In this way the ATM user can escape from the problems created by malicious hackers.

REFERENCE

[1] http://www.investopedia.com(InvestopediaonFacebook)
[2] www.quora.com
[3] http://Trak.in
[4] https://www.thinkpesos.com