Public Key Cryptography in ATMs

Tanusshri Sivakumar
Department of Electronics and Communication Engineering, Easwari Engineering College
tanusshrisivakumar@gmail.com

Abstract --- As civilizations evolved, human beings split into tribes, groups, and kingdoms. This led to the advent of ideas such as power, battles, supremacy, and politics. The need to communicate secretly gave rise to cryptography or cryptology. We present an introduction to cryptography, followed by types of ATM attacks and technologies related to it are elaborately discussed too.

Keywords --- Cryptography, Encryption, Decryption, ATM, Elliptic Curve

I. INTRODUCTION

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries

- Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext).
- Decryption is the process of converting ciphertext back to plaintext.
- Ciphers use a "key" which is a secret that hides the secret messages. The cryptographic method needn't be secret. Various people can use the same method but different keys, so they cannot read each other's messages.

A. Components of a crypto-system

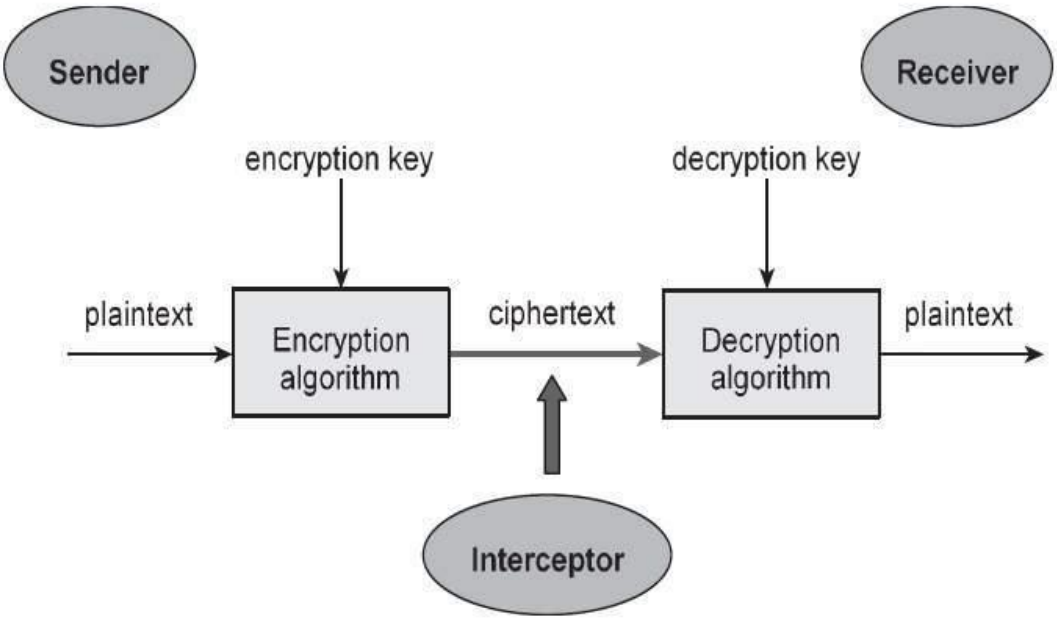

Fig. 1 Components of a crypto-system

B. Two Basic Types of Encryption

1) *Symmetric Algorithms*
It *is* also called as "secret key" and uses the same key for both encryption and decryption.
2) *Asymmetric Algorithms*
It *is* also called as "public key" and uses different keys for encryption and decryption.

C. Two Major Challenges

1) *Key distribution*
This involves how we convey keys to those who need them to establish secure communication.
2) *Key management*
This involves a large number of keys which is based on preservation of their safety and availability as needed.

D. Modern cryptography

It concerns itself with the following four objectives:

1) *Confidentiality*
The information cannot be understood by anyone for whom it was unintended.
2) *Integrity*
The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
3) *Non-repudiation*
The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
4) *Authentication*
The sender and receiver can confirm each other's identity and the origin/destination of the information.

E. Asymmetric cryptography

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key.

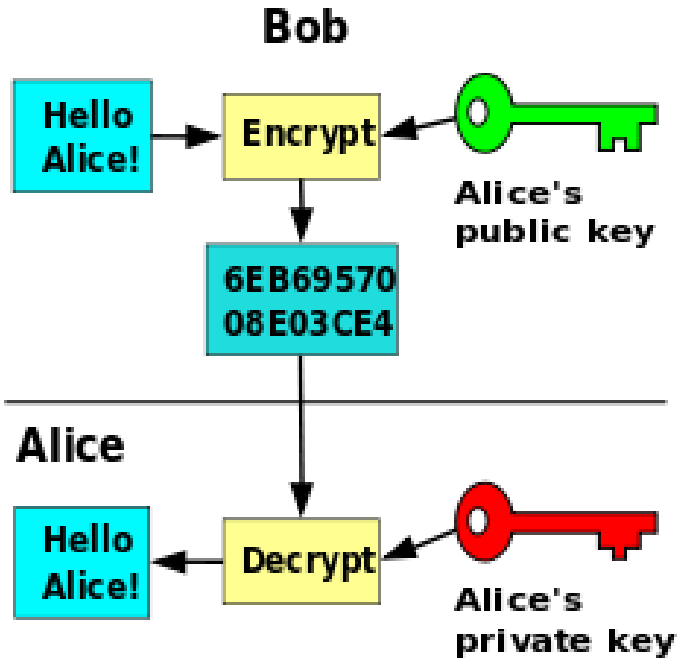

Fig. 2 Diagram illustrating public key cryptography

F. History of Public- Key Cryptography

The idea of public key cryptography was first presented by Martin Hellman, Ralph Merkle, and Whitfield Diffie at Stanford University in 1976. In Ralph Merkle's example, **A** begins creating random puzzles and sends them to **B. B** also creates puzzles and compares them to those of **A**, looking for a collision. When that collision occurs, **B** sends the common puzzle back to **A**. Since **A** and **B** both generated that puzzle, they can easily find its solution (in Merkle's scenario, a 40-bit number). This solution is their shared key. While it might take A and B 2^{20}=1,000,000 puzzles to hit a match, an eavesdropper would have to try all 2^{40}possibilities to solve the common puzzle and deduce the shared key. In other words, the eavesdropper would have to do a lot more work to reach the same conclusion. Contained within this realization were the seeds of public-key cryptography: the idea that puzzles—or keys—could be publicly known while the contents of the information exchanges they relate to would remain essentially secure.

II. ELLIPTIC CURVE

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography.

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,

E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit (This should be a prime number)

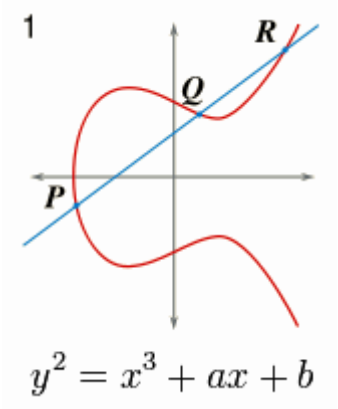

Fig. 3 Simple elliptical curve

A. Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number 'd' within the range of 'n'.
Using the following equation, we can generate the public key

Q = d * P
d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve.
'Q' is the public key and 'd' is the private key.

B. Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve.
Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 – (n-1)].
Two cipher texts will be generated and let them be C1 and C2.

C1 = k*P
C2 = M + k*Q

C1 and C2 will be sent.

C. Decryption

We have to get back the message 'm' that was sent to us,

M = C2 – d * C1

M is the original message that we have sent.

D. Proof

To get back the message,
M = C2 – d * C1

'M' can be represented as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P (cancelling out k * d * P)

= M (Original Message)

III. ATM's

A cash machine, also known as an automated teller machine or automatic teller machine. According to the ATM Industry Association (ATMIA), there are now close to 3 million cash machines installed worldwide.

On most modern cash machines, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip that contains a unique card number and some security information such as an expiration date or CVVC (CVV). Authentication is provided by the customer entering a personal identification number (PIN).

Using a cash machine, customers can access their bank deposit or credit accounts in order to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones.

By the 1980s, these money machines had become widely popular and handled many of the functions previously performed by human tellers, such as check deposits and money transfers between accounts. Today, ATMs are as indispensable to most people as cell phones and e-mail.

ATMs eventually expanded beyond the confines of banks and today can be found everywhere from gas stations to convenience stores to cruise ships. There is even an ATM at McMurdo Station in Antarctica.

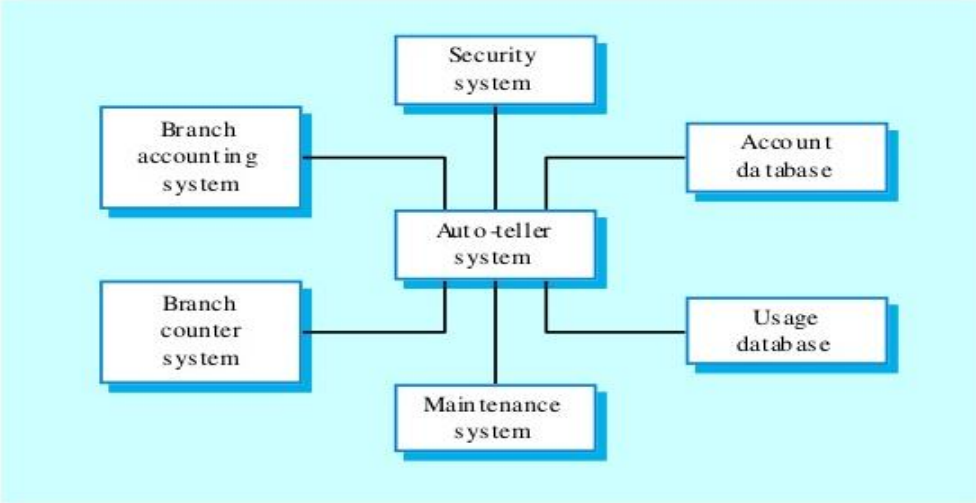

Fig. 4 ATM system

The framework was originally proposed by Klasen, Munzert and Nauer[KMN971] in February 1997. Based on the analysis of the objectives from the customer side, operator side and public community side, the draft identifies the main security objectives for ATM security: confidentiality, data integrity, accountability and availability.

Confidentiality and data integrity are obvious. Accountability means that all ATM network service invocations and network management activities should be accountable. Accountability includes both authentication and non-repudiation. It is extremely important for operators to manage the system and bill the services. Availability means all legitimate entities should be able to access ATM facilities correctly, no service denial should happen.

A. Principal Functions of an ATM Security System

1) *Verification of Identities*
Security system should be able to establish and verify the claimed identity of any actor in an ATM network.

2) *Controlled Access and Authorization*
The actors should not be able to gain access to information or resources if they are not authorized to.

3) *Protection of Confidentiality*
Stored and communicated data should be confidential.

4) *Protection of Data Integrity*
The security system should guarantee the integrity of the stored and communicated data.

5) Strong Accountability
An entity cannot deny the responsibility of its performed actions as well as their effects.

6) Activities Logging
The security system should support the capability to retrieve information about security activities in the Network Elements with the possibility of tracing this information to individuals or entities.

7) Alarm reporting
The security system should be able to generate alarm notifications about certain adjustable and selective security related events.

8) Audit
When violations of security happen, the system should be able to analyse the logged data relevant to security.

9) Security Recovery
The security system should be able to recover from successful or attempted breaches of security.

10) Security Management
The security system should be able to manage the security services derived from the above requirements.

Among the ten requirements, the last two won't provide security services. However, they are necessary to support the maintenance of security services.

IV. ATM SECURITY SCOPE

To identify ATM security scope, let's first look at the architecture of ATM. ATM architecture (figure 5) includes three planes: user plane, control plane and management plane.

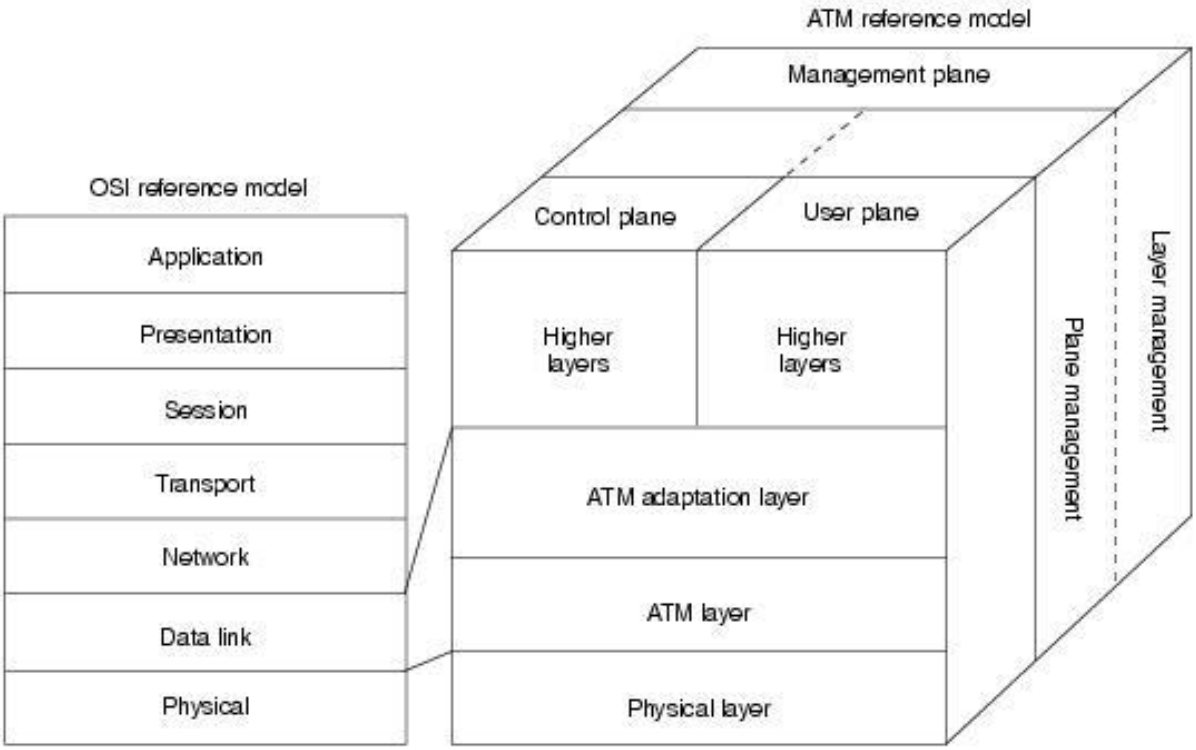

Fig. 5 ATM Architecture

Fig. 5 has a plane that includes entities. Entities in user plane are used to transfer user data. While the entities in control plane will deal with connection establishment, release and other connection functions. And the management plane entities perform management and coordination functions related to both the user plane and the control plane.

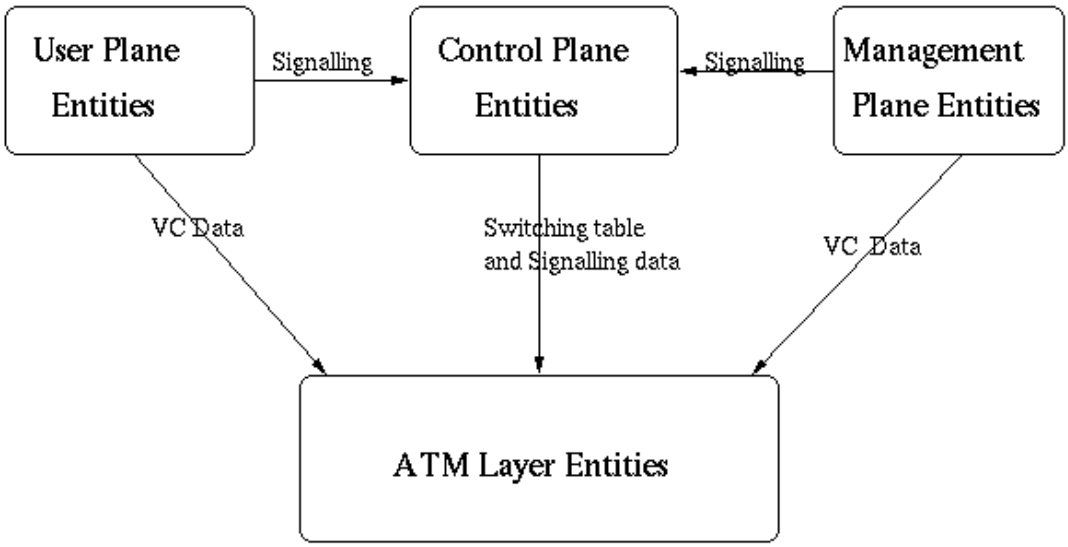

Fig. 6 ATM entities interaction model

V. ATM ATTACKS

ATM attacks and fraud continue to make headlines, despite the fact that the technology running ATM networks is becoming more secure and consumers are perhaps more vigilant than ever.

A. Card skimming

The act of using a skimmer to illegally collect data from the magnetic stripe of a credit, debit or ATM card. This information, copied onto another blank card's magnetic stripe, is then used by an identity thief to make purchases or withdraw cash in the name of the actual account holder.

B. Ghost ATM's

This ATM is created and built from scratch. It may incorporate a hybrid of parts from junked ATMs but is essentially a hand-crafted ATM. These ghost ATMs record all your data without allowing a transaction. At the conclusion of a transaction the machine reads "Can't complete transaction".

C. *Ram-raiding*

It is a variation on burglary in which a van, truck, SUV, car, or other heavy vehicle is driven through the windows or doors of a closed shop, usually a department store or jewellers shop, to allow the perpetrators to loot it.

D. PIN ID'S

One particular technique is where the criminal captures the magnetic stripe data from a retailer. They then go to an online bank site with a script written on several well-known PINs, and run it against the site until they get a match.

E. SMS Attacks

1) The attacker installs Ploutus on the ATM and connects a mobile phone to the machine with a USB cable.

The controller sends two SMS messages to the mobile phone inside the ATM.

2) SMS 1 must contain a valid activation ID in order to enable Ploutus in the ATM.
3) SMS 2 must contain a valid dispense command to get the money out.

The phone detects valid incoming SMS messages and forwards them to the ATM as a TCP or UDP packet.
In the ATM, the network packet monitor module receives the TCP/UDP packet and if it contains a valid command, it will execute Ploutus. It causes the ATM to spew out the cash. The amount of cash dispensed is pre-configured inside the malware. The cash is collected from the ATM by the money mule.

Analogous to Ploutus, there are many other malware software in existence.

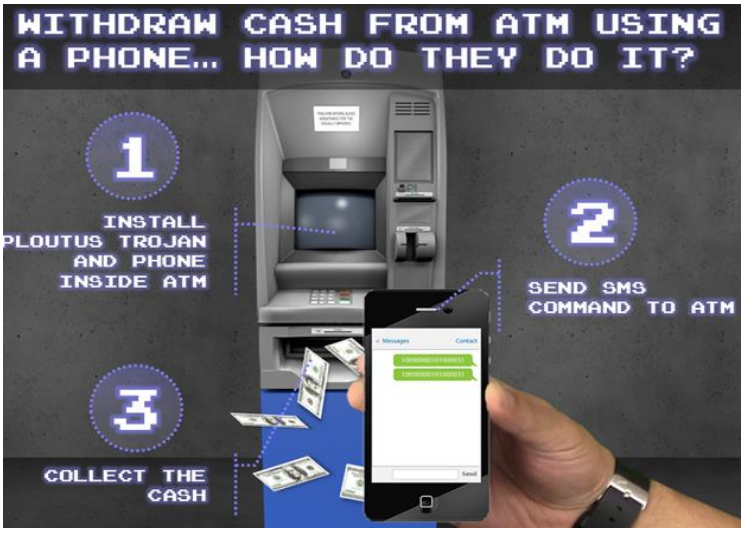

Fig. 7 ATM cash withdrawal using cash

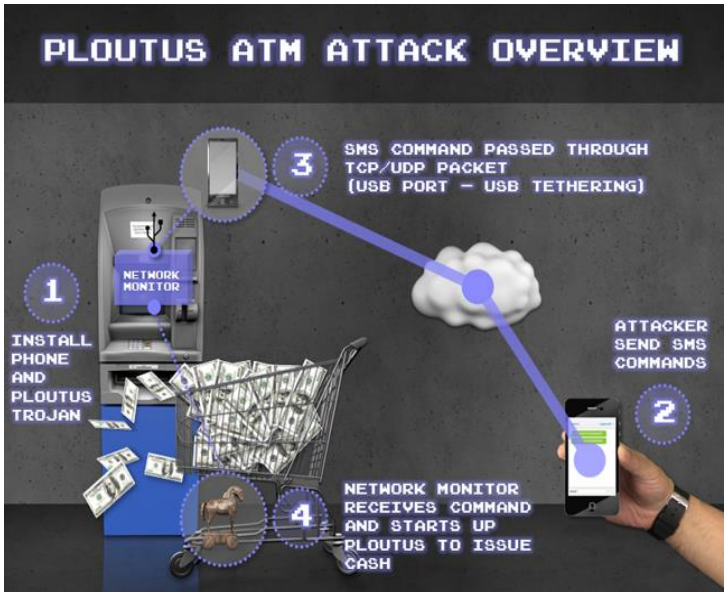

Fig. 8 Ploutus ATM attack overview

A number of measures could be taken to make things more difficult for the criminals. These include: Upgrading to a supported operating system, providing adequate physical protection and considering CCTV monitoring for the ATM and locking down the BIOS to prevent booting from unauthorized media, such as CD ROMs or USB sticks using full disk encryption to help prevent disk tampering

F. Logical Attacks

Logical attacks are becoming a major and growing attack vector, and one that has the potential to cause large amounts of losses. In this type of attack, external electronic devices, or malicious software in used in the crime. The tools are used to allow the criminal to take physical control of the ATM dispenser to withdraw money, which is often called "cash-out" or "jackpotting," as the machine starts spitting out bills like a casino gaming machine. The other version of malware attack on ATMs sees criminals using software to intercept the card and PIN data as customers use the machine. They can then use this to clone cards and commit fraud at point of sale terminals, ATMs and in 'card-not-present' scenarios.

Criminals are always looking for ways to get their hands-on card data or actual cash, however modern ATMs are designed to prevent attacks occurring, and the ATM industry constantly updates and evolves technology to thwart fraudsters at every possible step.

The good news is that there are solutions and practices that ATM manufacturers can and should do to protect the ATMs and the consumer who use them.

VI. RECENT ATM SECURITY TECHNOLOGY

With the growing security threats on banks, banking industries have been adopting new technologies to secure banking transactions. One of the recent technologies adopted by banks is the two-factor authentication which often combines the use of PIN and One Time Password (OTP) for user's authentication. In two-factor authentication method, first the customer enters the PIN, if the PIN is validated; the bank computer generates and sends an OTP to the customer's mobile phone via SMS. The customer enters the received OTP. If the OTP entered by the customer corresponds to the OTP generated by the bank computer, the customer is authenticated and the transaction is permitted. This OTP password is only valid for one log on after which it is discarded.

The OTP technology includes the use of SMS message for delivery of the OTP from banks to customers. The security of OTP is based on the security of SMS which is extremely vulnerable to variety of attacks. SMS usage is threatened with security concerns such as eavesdropping, interception and modification. SMS messages are transmitted as plain text. The A5 algorithm which is the GSM standard for encrypting transmitted data has been compromised. Encryption and decryption is done just between the base transceiver station and the mobile station. Since SMS messages can easily be wiretapped, intercepted, and modified, it can be envisioned that OTP send via an SMS can easily be compromised by man-in-the-middle attack. If the PIN to

an ATM card is earlier compromised, and the mobile number of the customer is known, compromising the OTP can be done by intercepting the OTP sent via SMS. The OTP and the PIN can then be used to make banking transactions without the customers' and banks' spotting any abnormalities.

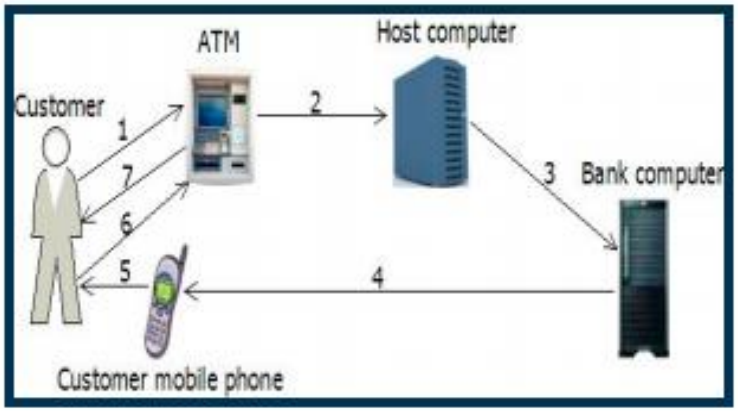

Fig. 9 Two factor authentications in ATM

VII. THE PROPOSED SECURITY SCHEME

After thorough study of the security features in ATM transaction, a security scheme is proposed. My proposal is not replacing the existing security technology; rather it serves as an additional layer of security that protects the existing authentication system from frauds and crimes. My concern is to provide a secure end to end communication of OTP to customers' by encrypting the SMS message used to send the OTP from the bank server to the customer's mobile phone. There are two banking modules in the proposed secure model, one at the bank server and the other on customer's mobile phone. The module at the bank server will contain a database where the entire customer's encryption key will be stored. This encryption key will be used to encrypt SMS message containing the generated OTP before it is sent to the customer's mobile phone. The module on the customer's mobile phone will contain the decryption key for decrypting received encrypted SMS from the bank server. This module is password based, the customer needs to enter a password before access is granted to the module. This is done in order to secure the module from unauthorized users.

Both modules use Elliptic curve encryption for encrypting and decrypting the SMS message containing the OTP. Elliptic curve is an asymmetric encryption technique.

The study in section II. Elliptic Curve explained that Elliptic curve encryption technique is a suitable asymmetric encryption technique for encrypting SMS transmitted message due to its ability of using smaller key size to obtain the same security as compared to other asymmetric encryption techniques.

Asymmetric encryption technique is used in the proposed model in order to prevent the decryption key from being compromised. Unlike the symmetric encryption technique which uses the same key for encryption and decryption, the Asymmetric encryption uses two related keys; public and private key. The public key will be stored in the bank server database while the private key will be stored in customer's mobile phone. If the database containing the customer's encrypting key is compromised, the decryption key will definitely not be compromised since the decryption key is stored in the customer's mobile phone. This employs encryption to encrypt the SMS message containing the OTP at the bank computer and decrypting it after it is received at the customer's mobile phone, which will prevent the OTP against eavesdropping and interception, thereby providing security to ATM transactions. Customer's public and private keys can be generated by physically connecting the customer's mobile phone to the bank computer using a cable. The public key is stored in a database at the bank server as the encrypting key while the private key will be stored in the customer's mobile phone as the decrypting key. These keys can only be renewed if the customer's mobile phone is physically connected to the bank's computer. In the proposed technology, if the customer initiates a transaction at the ATM, after entering the PIN and if the PIN is authenticated, the bank server generates the OTP, gets the customer's public key from the database, encrypt the OTP and send it to the customer's mobile phone via SMS. Customer on receiving the encrypted SMS decrypts it using the private key to get the OTP. This additional layer in the existing

security technology will help protect the OTP's transmission from malicious attack and eavesdropping, thereby providing security to ATM transactions.

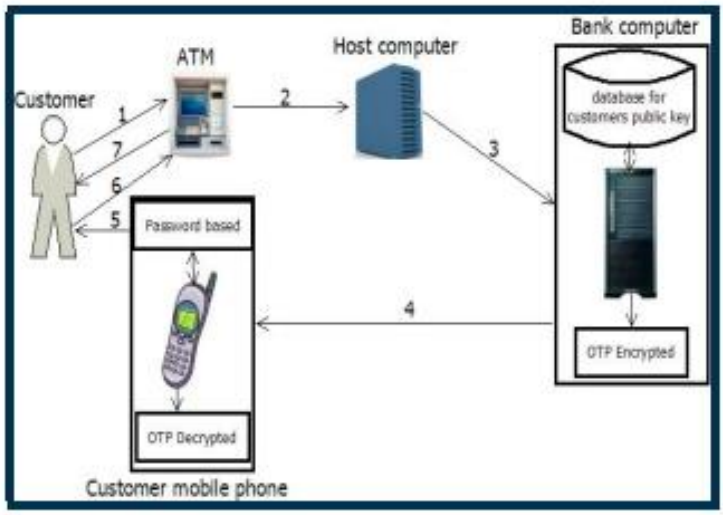

Fig.10 Two factor authentications in ATM

VIII. CONCLUSION

An asymmetric based encryption solution for securing OTP transmitted via SMS is introduced in this study. It is a scheme that provides an end to end security for SMS message containing the OTP sent by the bank server to customers for authentication, thereby providing security to ATM banking transactions. This scheme can be used by banks to provide confidentiality and authenticity to the bank-customer's communications through ATM. However, this scheme is not limited to ATM security, it can also be used to provide secured communication links in mobile and online banking.

REFERENCES

[1] J. Deutzman, FBI investigates million ATM scams, Feb 2009, available at http://www.myfoxny.com/dpp/news/090202_FBI _Investigates_9 _ Million_ATM_Scam (10 -09-2010)
[2] Barbara and D. P. Milkkelson, ATM Camera, Feb. 2010, available at http://www.snopes.com/fraud/atm/atmcamera.asp (10-09-2010)
[3] F. Klein, ATM fraud on the rise, Jun. 2010, available at http://www.silverplanet.com/scams/scam-alerts/atmfraud-rise/56867 (10-09-2010)
[4] Bithin Alangot, Simple explanation of elliptic curve at https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/ (22-02-2012)
[5] Coron,J.S" What is cryptography?", IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73
[6] eSTREAM - The ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream/
[7] National Institute of Standards and Technology, Advanced Encryption Standard, FIPS-197, http://csrc.nist.gov/archive/aes/index.html, 2000.
[8] Andy O'Donnell, Protect yourself from SMS Text Phishing attacks at https://www.lifewire.com/protect-yourself-from-smishing-sms-phishing-attacks-2487626
[9] Owen Wild, Six types of ATM attacks and fraud at https://www.ncr.com/company/blogs/financial/six-types-of-atm-attacks-and-fraud
[10] Tom Roeder, Asymmetric key cryptography at https://www.cs.cornell.edu/courses/cs5430/2013sp/TL04.asymmetric.html