CHAPTER 1

INTRODUCTION

Globally, banking system is working continuously from many years. Paper money or cash has been leading payment mechanism worldwide for the centuries. The measure works of a bank to deposits an amount of a customer and returns it to him when he needs. During deposits and withdrawal of the amount bank may use this money for itself as to given loans to other customers who wants to avail it. There are so many types of loan like home loan, agricultural loan, personnel loan, loan for industries and business houses etc. Banks give a particular interest for the depositors on his money and take a certain interest from loan account holder. 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 banking system there are two most frequent and important services- one is to deposit cash in the account and second to withdraw cash from the account. Both the service provided to a customer during a time in which banks are open and officials present at that time. Here in this work our main concern is about the withdrawal service provided by the bank. Banks normally provide this cash through teller counters. Only in the past century paper money or cash faced competition from mainly cheques, debit and credit cards. Previously this whole process was thoroughly manual and nowadays it is automatic. Banks try to improve the processes of cash supply chains to reduce the cost per processed banknote. Significant supply chain cost is incurred by ATMs related activities. So, at present one of its most valuable services to the customer is providing cash through Automatic Teller Machine (ATM) at anytime, anywhere [4, 8]. Look at to know what methods banks used or using for customers to withdraw cash from the account.

1.1 Teller in Traditional Banking

In traditional banking system, customer interacts with teller who was actually a cashier. Banks appoint a person to handle cash deposits or withdraw by customer. Whenever a customer needs to be withdrawing cash from his account, he had to fill a withdrawal request form and submitted it to the teller counter or window. A token had given to the customer from teller counter. Teller counter had sent it to the verification officer of the

bank. There were two verifications done- first signature verification and second ledger balance verification. If signature not matched with record, request rejected and customer had needed to start process again. Otherwise, it transferred to the second pass where ledger balance had checked. If enough balance had not in ledger request rejected. Otherwise it had returned to the teller counter after successful verification by bank officials. And then teller paid the cash to the customer when his token number appeared in the queue. The below mention flow chart describe it in details.

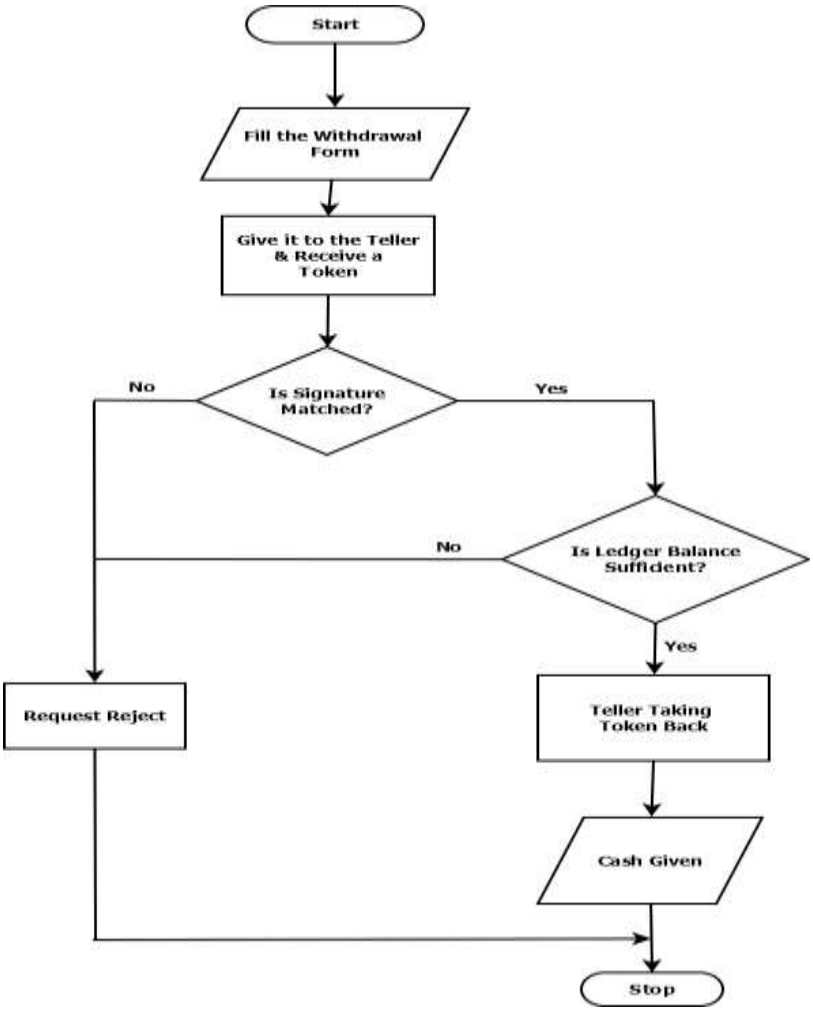

Fig1. Flow chart for traditional withdrawal process in banking

1.2 Half Automated Teller

When computers were used in banking system to maintain a ledger and signatures records electronically and the computer kept with Teller, a teller counter called as half automated teller. There was no need to verify signature and ledger as teller himself capable to check both by the help of computer. Teller counter personnel needed to pass it by bank officials

for verification and to make a payment to the customer. This is known as single window teller counter also. But this system was for very short time since technology grew very fast.

1.3 Automatic Teller Machine

Automated Teller Machines (ATM) give valuable payback to the banks and the customers. The ATMs allow bank customers to withdraw cash conveniently anytime and anywhere other than actual bank location by automating few of banking transaction services. The customers also get real time help on other services like balance enquiry, short statement, application for cheque book, e-cash transfer to other account, and more to customers. How, and by whom, these services are to be used it decide by bank and customers [6]. This ATM interact with a card called ATM card or ATM-cum-Debit Card. Initially this card used to interact with ATMs only but nowadays the card can use to purchasing, make payments for the services etc. also.

If we go in history of ATM, Luther George Simjian from USA has developed the first Cash Dispenser Machine. In 1959, the first ATM was introduced in Kingsdale Shopping Center Ohio, Canada. In the early 1960s, innovative engineers in Sweden, Japan, and Britain created and developed their own cash machines. A British engineer Mr. James Goodfellow has involved development of the security convention of PIN and he developed a card which has PIN stored in the card itself in 1965. This invention was to facilitate the authentications/verification of the user any human intervention. After looking first hand experiences in Europe, in 1968 the networked ATM was established in US, by Donald Wetzel.

In 1972, the first modern ATM came into operations in UK; the IBM 2984 was designed at the request of Lloyds Bank. The 2984 CIT (Cash Issuing Terminal) was the first true Cashpoint, similar in function to today's machines; Cashpoint is registered trademark of Lloyads TSB in the UK. The All ATMs were operational online and issued required cash to the customer and it was instantly deduct from his bank account. An US bank also has ordered to place these 2984 machines for its customer. A couple of well known prestigious historical models of ATMs include the IBM 3624 and 473x series, Diebold 10xx and TABS 9000 series, NCR 1780 and earlier NCR 770 series. Till these days a lot

of older generation who were using the conventional way of receiving the money from the teller at the branch rarely used to go to the bank machines.

In India ICICI Bank first introduced ATMs in 1998 at Mumbai. It was a new concept for Indians. In Mumbai, people accepted this service and bank has established new ATMs in various big cities to all over India. After that some other banks like HDFC bank, HSBC bank, and Axis Bank (formerly known as UTI Bank) opened ATMs.

Interbank networks provide the facility to connect many of ATMs from different banks, facultative individuals to get cash from any machines. But for deposits, in India ATMs accept cash from machines belonging to only that bank wherever customer has the account. NYCE, PULSE, PLUS, Cirrus, AFFN, Interac, Interswitch, STAR, LINK, MegaLink and BancNet are some examples of interbank network.

An ATM i.e. automated teller machine or automatic teller machine is also acknowledged as automated banking machine (ABM) or a Cashpoint or cash machine or a hole in the wall etc., which is basically a computerized telecommunications device. It helps customers by providing access to the financial transaction in a public space without any human intervention.

On the modern ATMs, the user identification happens through a plastic card which is called as ATM cum Debit card. The ATM cum Debit Card contains a magnetic stripe or a chip, which has a unique number for the card and a little security information such as an expiry date, CVV (Card Verification Value) etc. Once the user authenticates the transaction by providing a personal identification number (PIN) a valid transaction takes place through an ATM. If user has withdrawn currency from the ATM is different from in the currency user is operating on (e.g. withdrawing US Dollars from a bank account containing Indian Rupees in USA) then the currency will be converted at an official wholesale exchange rate. The ATMs provide the best possible official exchange rates and are significantly used for this service as well. ATMs are placed generally inside the premises of banks, but they locate outside the bank also such as shopping centers, big commercial malls, airports, railway stations, petrol pumps, restaurants, or the place where large numbers of people visit frequently. Mostly ATM installations are of two types one is on premise and second is off premise. On premise ATMs are expensive installations since these ATMs are technically more advance and support multiple services to

complement a bank branch's capabilities. Whereas Off premise machines are less expensive since these machines are single function devices installed by financial institutions and Independent Sales Organizations (ISOs) where there is a simple need for cash.

CHAPTER 2

LITERATURE REVIEW

2.1 Previous work

The explanation and modeling of an Automated Teller Machine (ATM) are a distinctive design case in safety significant and real time systems. An ATM is characterized by its high degree of complexity, intricate interactions with hardware devices and users, and compulsory necessities for functional or domain knowledge. All these factors give surety the ATM system as an intricate but perfect design prototype in comprehensive software system design in common and specifically in real-time or instantaneous system modeling.

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 Kanwal et al [1], Automatic Teller Machines (ATMs) are self service banking machines which allows customers to access their bank account with no help of a bank teller. Most of ATM machines allow customers of various banks to operate basic banking transactions without going to their bank or their banks ATM machine. Regardless of all these benefits, like any other technology invention there are a few disadvantages of ATM; very often it has been reported [7] that customers and banks are facing lots of issues regarding ATM frauds and security breaches. So that there is a strong requirement to offer a provision for secure ATM transaction adjacent to scams and fraud. There is no availability of systematic and comprehensive records of design facts; only modeling prototypes is available for ATM systems. This research work presents the formal design, specification, and modeling of the ATM system using a denotation mathematics known as Real-Time Process Algebra (RTPA) [9]. The RTPA methodology for system modeling and refinement suggests that, a software system can be developed as a collection of architectural and operational components as well as their systematic interactions. Earlier this was modeled by Unified Data Models (UDMs), also known as the component logical model (CLM)), which is an abstract model of system hardware interfaces, an internal logic model of hardware, and/or an internal control structure of the system. Latter it was modeled by static and dynamic processes using the Unified Process Models (UPMs).

Apart from a mathematical/logical model there is another technique available for ATMs which is known as biometric technique. As we all know the biometrics uniquely identifies or verifies an individual through the characteristics of his/her unique human body. The Biometrics uses characteristics that can be physical and unique like finger prints, facial characteristics, voice, iris scan, or DNA. If someone steals the debit card and it's PIN also, he can easily access the account and withdraw cash by using it on any ATM. But in case of biometric ATM he can't because this type of ATM takes a sample of thumb impression or finger prints or palm scan or iris scan and then compare it with stored biometric data. It is been noted that nowadays biometric scanners go far away from critical fingerprint recognition. Security experts of this field told that it is very easy to lift and replicate the fingerprints of anyone. Highly safe biometric technology uses a apparatus designed to achieve an Iris scan based on more than 2000 sole measurement points.

So nowadays it is not easy to access someelse's account since authentication is going to be a challenge. It is very important in the Biometric technology to 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. Thus computer database should be leveraged for both identification as well as verification. For biometric identification, a biometric system searches the database for a match with recently/newly captured sample and grants the access if at all match is found by authenticating individual identity. The login process to a computer using a finger print or thumb impression is an example of this mode. Accessing a door using palm scanner or iris scanner is an example of this mode. The current biometric technologies are palmed print recognition, dynamic signature fingerprint recognition, hand geometry, iris recognition, face recognition, vascular pattern recognition and speaker recognition.

Nowadays the maximum numbers of biometric ATMs are used in Japan. The banks across APAC & EMEA regions are also moving towards the new biometric technology. In the recent markets the Western banks and various financial institutions are already set to incorporate biometric technology with mass market banking.

2.2 Problem and Issues Domain

Nowadays people using their banking experiences with ATM cum Debit card through

ATM machines provided by banks. All banks issue a Debit card to the account holder when open an account. Using this card, account holder can access his account with ATM machines which located various places and working 24 x 7. A user may use this debit card for purchasing also. The ATM machine provides facilities to the account holder like cash withdrawal, cash deposits, mini statement, account balance, PIN change etc. Nowadays an account holder can use his debit card anytime anywhere and of any bank.

But there are some security constraints with this facility. Bank provides a 4-digits secret number to the user called PIN with ATM cum Debit card which user can change at anytime through ATM machine. This secret number, PIN, is static type i.e. once set it; access will be done after using it in each ATM transaction. So a user keeps the PIN secret and not to share anyone. An unauthorized access may possible if anyone steals the Debit card with PIN or guess the PIN. It is possible, generally users set the PIN with easy going numbers; like date of birth, vehicle number, house number, etc. in most cases so the chances to hack it more. This is the main threat to use ATM-cum-Debit card. To minimize this problem here a protocol is proposed by which it can solve. A very common problem is also faced by users. If the real user get ill or there is any circumstances in which the user may not in the position to transact through ATM user can authenticate another one to transact his account on behalf of him/her. The person called bearer or third party who is authenticating to transact account. It is the process just like a user gives the bearer cheque to a person for withdrawing the amount on behalf of the user. There are many different attacks such as shoulder surfing, data skimming, fake machine etc. These attacks will be discussed on next page.

Authentication technologies through finger vein, palm scan etc. are realistically being used in the banks. One of the Biometrics techniques is the Finger vein authentication. As described in the previous section Biometrics is personal authentication technology based on the unique physical characteristics or the behavioral characteristics of the human. The Finger vein authentication technology verifies an individual’s identity according to the vein pattern image of fingers analyzed by near-infrared transmission. This technique is very much complicated to forge, because of using the vein patterns which are unique in each body. Additionally both the false rejection rate and the false acceptance rate are low so that the technique is highly accurate. However, Matsumoto et al [17] stated that the artificially formed fake finger was registered on finger vein authentication device and tried to verify, the fake finger was verified high probability. It cannot refuse the

possibilities to be cheated the finger vein authentication. Because an artificial finger can be formed this is verified. So this simply means that the biometric ATMs are also not secure also. And maintain a huge data is also a big challenge for biometric ATMs.

2.3 Importance of a solution

This type of act is dangerous and a card holder can lose his/her money through ATM machine by using fake or stolen card or incomplete operation by somebody else. In computer security, we call it as masquerading. Masquerading means any person approaches himself like the other person means using masque of other person. ATM only recognizes the person after inserting PIN and it will allow the debit card holder to access the account.

The solution of this problem is to using a dynamic password through existing mobile network. Every time a card holder using his ATM cum debit card gets an arbitrary password for each transaction separately generated from bank server. First ATM gets authentication through PIN inserting and then inserting this dynamic password on ATM machine, it can validate to user to process the operation. The full process of this operation can be described as in Figure 7.

2.4 About ATMs

An ATM has following parts in it:

- **CPU**- It is used to control interfacing of user and transaction devices through specific software. Most of ATMs are using Windows 2000, Windows NT operating system.
- **Card Reader**- There is a card reader. It reads user's card from magnetic strip or chip. This is the process to identify the user. The magnetic strip or chip has a little information about the user.
- **PIN Pad**- It is an alphanumeric key pad. A user provides the PIN and other instructions through it.
- **Display terminal**- There is a display panel which is useful to interact with the user. All given instructions appeared on this terminal. It has some function keys on both sides to give necessary inputs to the CPU. Some of the ATMs have touch screen terminals also.

- **Printer**- There is a printer to provide actual status report or last transaction report to the user for his record. It is an integrated device with ATMs.
- **Security Camera**- Nowadays a hidden camera is also an integrated part of this ATM to upgrade physical security. This camera works 24 hours continuously and records all activities done in ATM cabin by incoming person.
- **Vault**- It is a placeholder to store the parts of the machine that is access restricted.
- **Housing**- Housing is a hard cover which protects all inner parts and cash from theft.

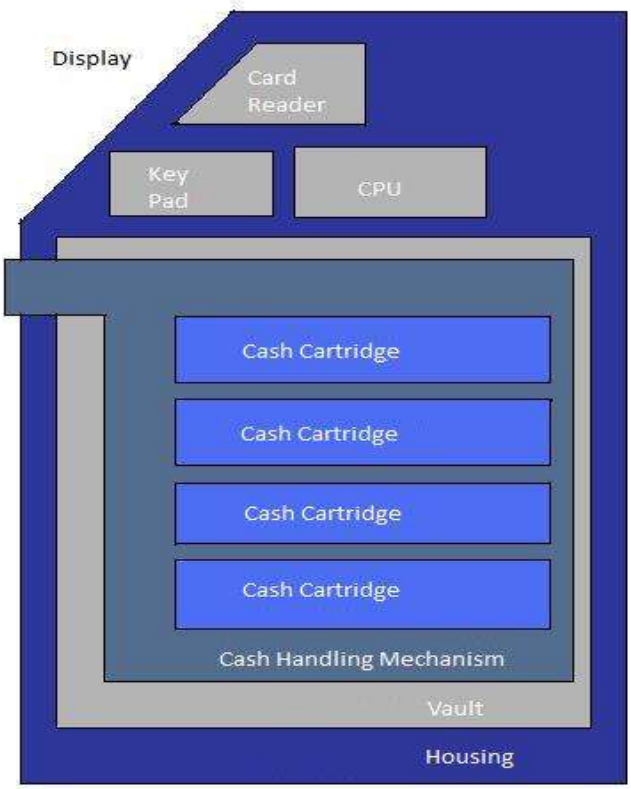

Fig 2. Block Diagram of an ATM

Authentication of a transaction by the card issuer or anyother authorization institute through the different communication networks for ATMs. These networks set ups will be discussed in detail in the later part of the report. Generally this authentication process is performed by a standard that known as ISO 8583 messaging system. More details are available at International Organization for Standardization (ISO) website regarding this standard. There is no need to study in details here but a quick reference to ISO 8583 here (for reader's benefit) - It has 3 parts:

Part1- Message, data element and code values,

Part2- Application and registration methods for Institution Identification Codes,

Part3- Maintenance methods for messages, data elements and code values.

This ISO 8583 platform is an essential part of the transaction processing and this platform routes transaction between Acquirers and Issuers via its global transaction processing network. ISO 8583 platform supports-

- Check verification only transactions
- Traditional electronic check conversion (ECC) transactions
- Debit card transactions based on PIN
- Visa POS check electronic check conversion transaction
- Credit and Debit card transaction based on individual's signature

All of the above mentioned transactions are processed through ISO 8583's authorization, clearing, and settlement services. There are three fundamental services-

1. Authorization; when purchase has completed and then for finalization of this purchase and disbursed the cash the issuer accepts or rejects this sales transaction;

2. Clearing; when a purchase transaction is completed and delivered from an user to an issuer for posting it to the account of Cardholder;

3. Settlement; when merchant presents all transaction details to the issuer after the process of calculating and determining the net financial position for all transactions that are cleared.

It is a separate process in which the actual exchange of funds makes. The transactions can be authorized settled as dual message or single message transactions. Note that a dual message transaction is sent two times- the first time when only the information is required for an authorization decision and then next time when additional information required for clearing and settlement. Generally authorization occurs online while clearing and settlement occur later offline i.e. credit card and traditional ECC check transactions. A single transaction message is sent out only for one time to do authorization which contains clearing and settlement information alongwith authorization information. These

transactions are known as full financial transactions. In single message transaction typically, authorization and clearing occur online while settlement occurs later offline. For example debit card based on PIN and Visa POS check transactions.

2.5 Required Infrastructure for ATMs

2.5.1 Switching

Assume that some nodes are physically connected to one another according to a specific topology and that a specific addressing method has been detected. For long distance direct connection is not possible between nodes so that a new technology was developed that is known as Switching in which at long distance two nodes are not directly, For connection they can use switching means connection will be establish using other nodes that are present between them. Data exchange between an arbitrarily selected pair of nodes (ATMs) generally must take place via transit nodes. It is been noted that switches are devices which may be hardware or software. These are capable to create a time being interface between two or more nodes connected with swich. The switching can be represented as a process below:

- Determining the information flows by defining routes
- Routing of information flows
- Flow forwarding
- Flow multiplexing and demultiplexing

There are two types of switching- circuit switching and packet switching.

2.5.1.1 Circuit Switching

Circuit switching was invented long before packet switching. Circuit switching is a methodology of applying a telecommunication network wherein two network nodes establish a dedicated communication channel through the network before the nodes may communicate. The circuit gives assurance to use the full bandwidth of the channel and remains connected for the full time of the entire communication session. In this technology whole data is transferred only once. Before the data transmission takes place the connection path should be established between the nodes. When path is establish between two nodes than a logical channel on physical link is dedicated to this connection

and now dedicated communication path between two nodes is created means no other connection can be established between this paths whenever it is terminated.

Communication via circuit switching has three steps:

1. Establishment of the circuit
2. Transferring the data
3. Circuit Disconnect

In circuit switching transmission medium is separated into Frequency division multiplexing (FDM), Time division multiplexing (TDM) or Code division multiplexing (CDM). In this technique information flow in a string form and for this channel bandwidth is reserved. It provides need not buffering, Processing or scheduling in data path. The circuit functions just like the nodes were actually connected with an electrical circuit. This principal originates from the first telephone networks. The example of a circuit switched network is an early analog telephone network. A call is to be established from one telephone to other telephone; switches provide a continuous wire circuit within the telephone exchange between the two telephones for the entire call duration.

2.5.1.2 Packet Switching

Packet switching is a new methodology by which establishment of digital networking communications achieved. This technique was designed specially for the efficient transmission of digital data. It groups all transmitted data into predefine small fragments known as packets. And These are also known as frames or cells also. Header is provided with each packet which containing an address. This address is necessary to packets delivery to the destination node. This type of data transmission is one of the fundamental networking technologies which support the local area networks (LANs). One of the most frequent used features of Packet switching is to deliver variable bit rate data streams over a shared network. Packets are supplied to the network without previously reserving communication links, and at the rate at which the source generates them. This rate is not exceed the bandwidth of the access link. It is presumed that packet switched network is always ready to collect the packets from any of its end nodes. There are two types of packet switching- one is connectionless and second one is connection oriented. In connectionless packet switching, the transmission takes place without establishing a connection and all transmitted packets are forwarded independently of one another using

the same rules. Each packet is stamped with a target address, origion address and port numbers. It may also carry the sequence number of the packet. Each packet is forwarded and may go through various routes. At the destination the original data or message is reassembled in the appropriate order as per the packet sequence number. In connection oriented method of data transmission is divided into sessions or logical connections. The entire set of the packets transmitted as part of the session rather than for an individual packet. Routing a packet is very simple as it just requires the node to look up the previous session history. It contains the connection ID instead of address so that the packet header can be small.

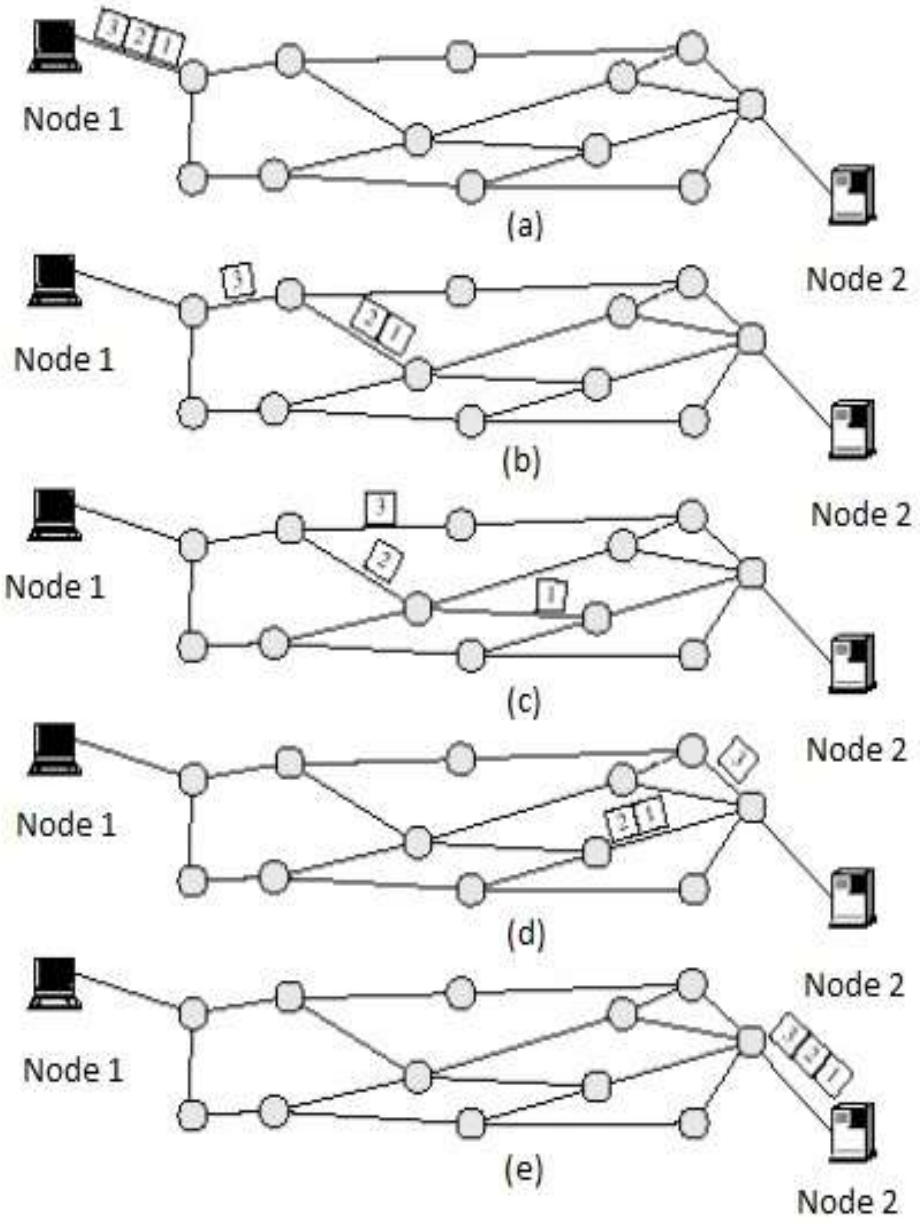

Fig. 3 (a) Packet Switching- Datagram Approach

There are two approaches of the packet switching- datagram and virtual circuit. Each packet is treated independently from all others in the datagram approach to the packet switching. Packets are referred to as datagrams in this technology. In this approach each and every one packets to be connected with the identical message however may go by dissimilar routes to arrive at their target [refer Fig 3 (a)].

In virtual circuit approach to packet switching the correlation is preserved between all packets correlated to a message as well as session. A single path is selected always between transmitter and receiver since the starting of the session. When the data is sent, all packets of the message or session travel one after another through that path in the transmission [refer Fig 3 (b)]. The Virtual circuit switching is a packet switching type technique wherein a path is established between the origin node and the target node through which all the message /session packets will be routed during a call. We call this a virtual circuit since to the user; this connection appears to be a dedicated physical circuit. However, the same route is being used by other communications as well. Before the data transfer starts, the source and destination identify a suitable route for the virtual circuit. All intermediate nodes between the two points put an entry of the routing in their routing table for the call. Additional parameters, such as the maximum packet size, are also exchanged between the source and the destination during call setup. The virtual circuit is cleared after the data transfer is completed.

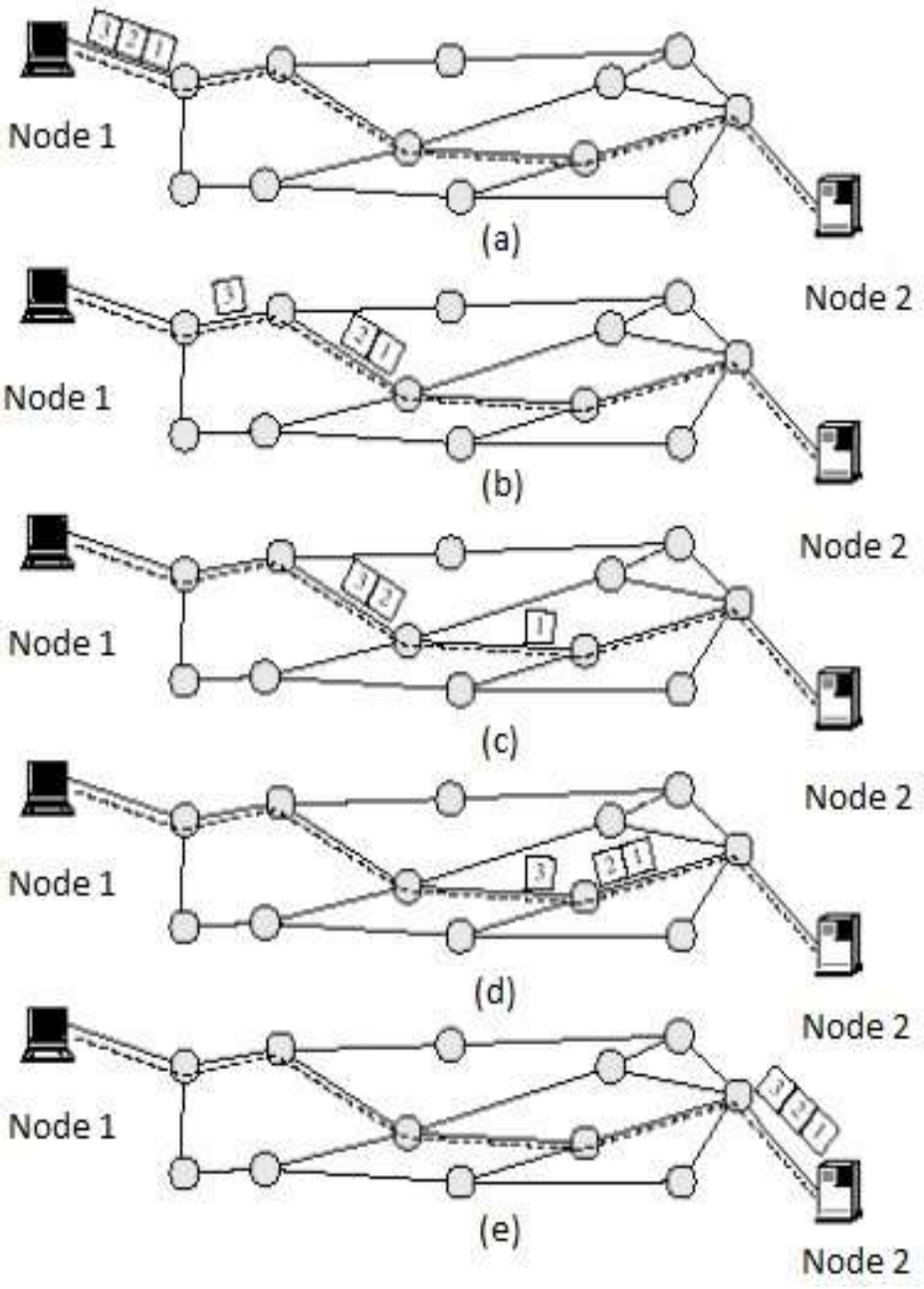

Fig 3 (b) Packet Switching- Virtual Circuit Approach

Virtual circuit packet switching is connection orientated type of switching. This is in contrast to datagram switching, which is a connection less packet switching methodology. Virtual circuit transmission is implemented in two formats:

a. Switched virtual circuit (SVC)

b. Permanent virtual circuit (PVC)

a. SVC:

In SVC, a virtual circuit is formed when it is required and establishes just for the specific time period of the particular exchange. As an example here consider that station X needs to transmit some packets to station Z. First, station X sends a request to the firm of connectivity with station Z. When the connectivity is established, continuously all the packets are sent one by one in the order of sequence. The connection is released after last packet received. And now that virtual circuit ceases to exist.

There is only a single path exists for the specific time period of transmission, even though the network could choose an alternating path in reaction to collapse or blockage. All the time that station X wants to talk with station Z, a new path is made. It may be the similar every time, or it may be some different in answering to unreliable network settings.

b. PVC:

In PVC, the same virtual circuit is formed between two users as discussed previously as continuing flow of data in proper sequence. It is devoted to a particular user and none else may utilize it. Because this is forever in place, it may be utilized without connection making and connection terminating. Whereas two SVC users can find the dissimilar route always when they request to establish a connection, two PVC users at all times find the similar route.

Generally Packet switching is used in ATM communication with Bank server. Examples for the packet switching are X.25, frame relay and IP (Internet Protocol). We will discuss all of these in brief on next pages.

2.5.1.3 X.25

The X.25 is the inception technology in this field. The X.25 shows how make a connection established by a packet mode workstation to a packet network for the data exchange. Virtual circuit is used to approach packet switching and asynchronous TDM to multiplex packets. At the network layer of X.25 the virtual circuits has formed; the simple means of that is a physical connection recognized between two nodes can bear moderately a few virtual circuits at the network layer with each circuit meticulous for carrying either data or control information, a concept called in-band signaling. Each virtual circuit in

X.25 must be acknowledged for use by the packets. The virtual circuit identifier in X.25 is known as the logical channel number (LCN).

X.25 is a standard set of protocols that contains the three types of protocols for the first three layers of OSI Model. The OSI model has been defined by the International Standards Organization (ISO). The following three X.25 Protocols generally work for the three layers are:

- X.25 RS232 : For Physical layer
- X.25 LAPB : For Data Link Layer
- X.25 PLP: For Network Layer

In OSI layer terms, user and protocol information is encapsulated within the Packets to be passed down to Layer-2. Layer-2 encapsulates the packet contents inside an information frame and passes the result down to Layer-1 for transmission on the link. The resultant bit stream is transferred between the DTE and DCE through a standard physical interface like RS-232 which is a X.25 Protocol. It performs the same functions of communicating between different host users (DTE) and network nodes (DCE) as in Network Layer but there it happens at Packet Level and in Data Link Layer it happens at Frame level.

X.25 PLP implementation has been designed to be primarily concerned with network routing functions pertaining to end-user entities of public and private Packet networks. X.25 PLP provides a standard Layer 3 networking interface between the Subscriber or Logical DTE and the network entry point called either the Data Switching Exchange (DSE) or Logical DCE.

The protocol allows end users of the network to:

- Communicate with remote DTE devices and remote end users "attached" to DTE devices,
- Temporarily or permanently own a part of network capacity of determined quality and type
- Recover from severe or mild errors at the network level
- Flow control information on a VC –Virtual Circuit.

In the beginning, X.25 was designed more than 25 years ago to bear voice over analog telephone lines (dial-up networks). Typical applications of X.25 today include automatic teller machine networks and credit card verification networks. X.25 also supports a variety of mainframe terminal/server applications.

2.5.1.4 Frame Relay

But as high speed required a new technology born called Frame relay. It belongs to virtual circuit technique that gives low level i.e. physical layer as well as data link layer service in reply to the demanding of higher data rate on lower price, bursty data, and less overhead because of enhanced transmission media. It has a number of benefits over comparable wide area networks like X.25 and T-line. The operation of X.25 is generally performed at higher speed @44.376 Mbps. It is capable to be used like backbone network since it operates at physical layer and datalink layer. It handles frame size of 9000 bytes at the instant. It is less expensive in comparison to other traditional WANs. Originally Frame Relay was developed to make use of across Integrated Services Digital Network (ISDN) interfaces. At present, it is used for a diversity of other network interfaces. In this chapter the main focuses to know about specifications and different applications of Frame Relay regarding the context of WAN services. Packet-switched technology is used in Frame Relay; and Packet-switched networks facilitate ending stations to dynamically distribute the network medium and the obtainable bandwidth. The following two techniques are used in packet-switching methodology:

- Variable-length packets and,
- Statistical multiplexing

Variable-length packets are used to get more efficiency and flexibility for transferring the data. These packets are switched among the different segments in the network whenever the target node is reached. In a packet-switched network the statistical multiplexing techniques manage the network access. Frame Relay often is described as a efficient edition of X.25, contributing fewer of the strong capabilities of X.25 like windowing and retransmission of last data. Frame Relay is rigorously a Layer 2 protocol suite, whereas X.25 provides services at Layer 3 (the network layer) as well. This enables Frame Relay to propose higher performance and greater transmission efficiency as compared to X.25, and makes Frame Relay suitable for current WAN applications, like LAN

interconnection. Devices attached to a Frame Relay WAN fall into the following two general categories:

- Data terminal equipment (DTE)
- Data circuit-terminating equipment (DCE)

Generally DTEs are considered to be terminating equipment for a particular network and typically are situated on the premises of a customer. In reality, they may be owned by the customer. Examples of DTE devices are terminals, personal computers, routers, and bridges.

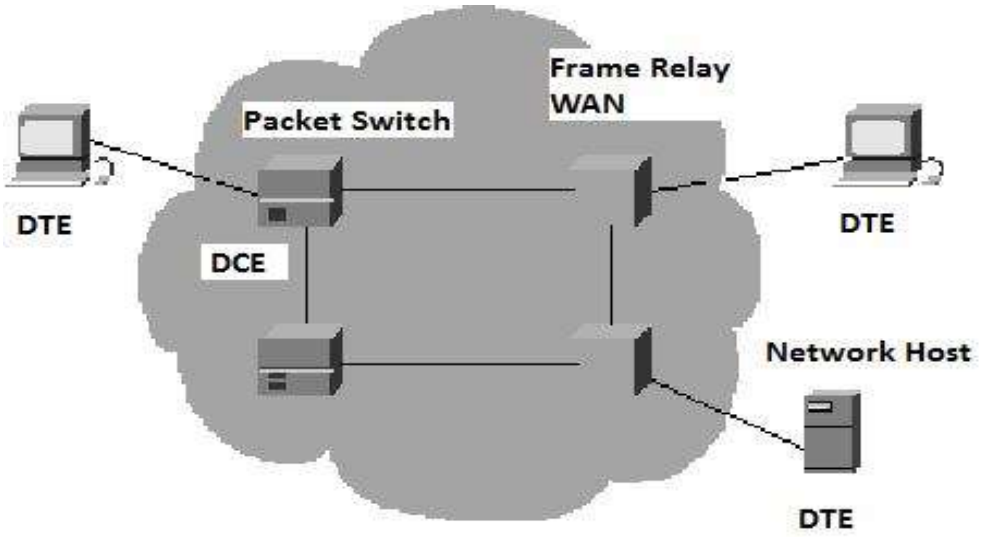

Fig. 4 Frame Relay Network

DCEs are carrier-owned internetworking devices. Main reason behind to use DCE equipment is to offer proper clock and switching services in the existing network. These are the devices which really send data by using of the WAN and mostly of those packet switches. The two categories of devices have a specific relationship between them and Fig 4 describes it. The DTE device and a DCE device connected through both the layers- physical and datalink and consist of both a physical layer component and a link layer component. The physical component defines the mechanical, electrical, functional, and procedural specifications for the connection between the devices. Standard RS-232 is suggested and recommended to interface with physical layer as most common specification. The establishment of connection between the DTE

devices are getting through the protocol which is datalink layer component for example a router, and the DCE device, for example a switch.

The main benefits of this technology is to offers extra flexibile and added well-organized use of bandwidth. Nowadays popular LANs, like Ethernet and Token Ring, are good examples of networks which has used packet-switching. It has several disadvantages also. Note that it allows variable length size of frames due to this it may form delays that is differ for each and every user.

Flags	Address	Data	FCS	Flags
(8)	(16)	(Variable)	(16)	(8)

Fig 5. Frame relay frame

The following descriptions summarize the basic Frame Relay frame fields illustrated in Fig 5:

- **Flags**—delimit the beginning and end of the frame. The value of this field is always the same and is represented either as the hexadecimal number 7E or as the binary number 01111110.
- **Address**—Contains the following information:
    I. **DLCI**—The 10-bit DLCI is the essence of the Frame Relay header. This value represents the virtual connection between the DTE device and the switch. Each virtual connection that is multiplexed onto the physical channel will be represented by a unique DLCI. The DLCI values have local significance only, which means that they are unique only to the physical channel on which they reside. Therefore, devices at opposite ends of a connection can use different DLCI values to refer to the same virtual connection.
    II. **Extended Address (EA)**—The EA is used to indicate whether the byte in which the EA value is 1 is the last addressing field. If the value is 1, then the current byte is determined to be the last DLCI octet. Although current Frame Relay implementations all use a two-octet DLCI, this capability

does allow longer DLCIs to be used in the future. The eighth bit of each byte of the Address field is used to indicate the EA.

III. **C/R**—The C/R is the bit that follows the most significant DLCI byte in the Address field. The C/R bit is not currently defined.

IV. **Congestion Control**— The congestion control consists of the 3 bits that control the Frame Relay congestion-notification mechanisms. These are the FECN, BECN, and DE bits, which are the last 3 bits in the Address field.

- **Data**— It contains encapsulated upper-layer data. Each frame in this variable-length field includes a user data or payload field that will vary in length up to 16,000 octets. This field serves to transport the higher-layer protocol packet (PDU) through a Frame Relay network.
- **Frame Check Sequence**— It ensures the integrity of transmitted data. This value is computed by the source device and verified by the receiver to ensure integrity of transmission.

2.5.1.5 Asynchronous Transfer Mode (*ATM*)

ATM is the cell relay protocol and can be assumed of like the highway of the information superhighway. If there is consideration a concept of cell networking then most of the problems related to packet networking has solved easily. A cell has fixed size and it is consider like a small data unit. A cell has taken as the fundamental unit of data transfer in a cell network. Entire data are loaded into similar cells which may be sent with whole predictable and standard manner. If there is arrival of packets of dissimilar sizes from another network at the cell network, it must be split into many small data units of equivalent length and loaded into cells. Now the cells are multiplexed with other cells and routed through the cell network. Since each and every cell has equal size so that the problem allied at multiplexing of various size of packets are ignored. It called asynchronous transfer mode (*ATM*) because asynchronous TDM is used. TDM uses slots which has fixed size. From an input channel that has a cell may fill up a slot of *ATM* multiplexers; the slot is not filled if none of the channel has a cell to send.

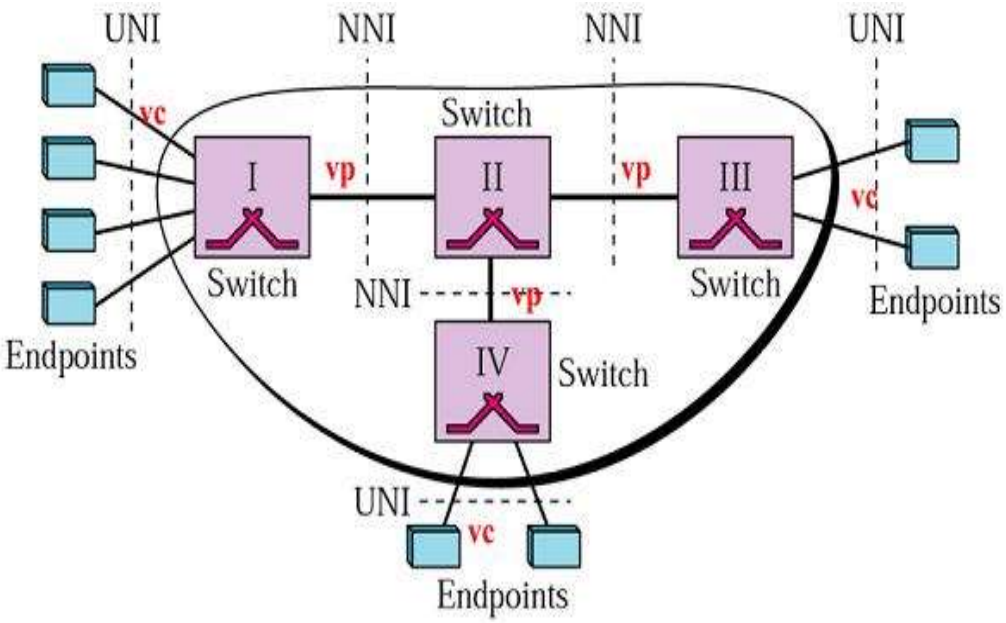

Fig 6. *ATM* Architecture

Following are the main characteristics of *ATM* network:

- The *ATM* service models include constant bit rate (CBR) service, variable bitrate (VBR) service, available bit rate (ABR) service, and unspecified bit rate (UBR) service.
- *ATM* uses packet switching in which packet has fixed-length of 53 bytes. In *ATM*, these packets are called **cells.** Each cell has five bytes of header and 48 bytes of payload. The fixed-length cells and simple headers have facilitated high speed switching.
- *ATM* uses virtual circuits. In *ATM*, virtual circuits are called virtual channels. The *ATM* header includes a field for the virtual channel number, which is called the virtual channel identifier (VCI) in *ATM*.
- *ATM* does not provide resending of data on a link-by-link base. If there is an error in an *ATM* cell header, simply a switch finds it and attempts to correct the error by using error correcting codes. If it fails to correct the error, it removes the cell instead of to request a resend data from the previous switch.

There is a brief discussion about *ATM* reference model.

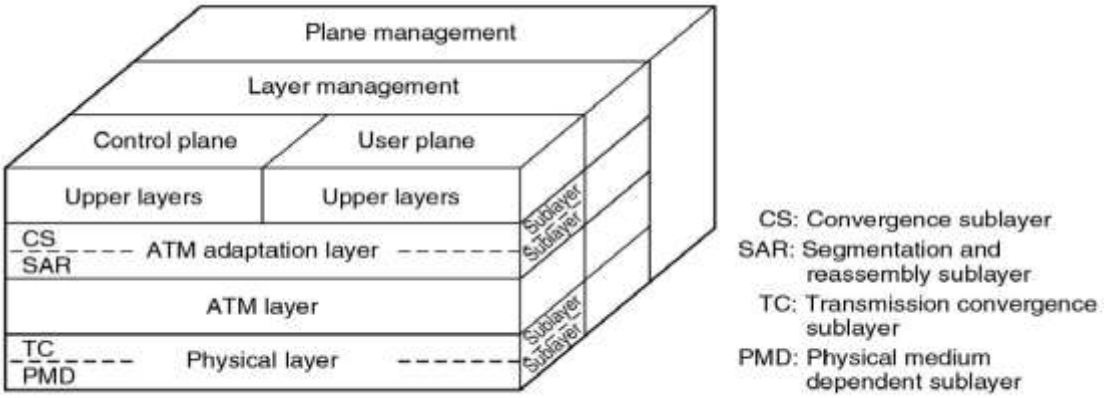

Fig 7. ATM Reference Model

The reference model of *ATM* builds up with three planes which cover entire layers:

- Control – all signaling request may be produces and manages here.
- User – data transfer manages here.
- Management – contains 2 parts: First is Layer management : manages layer specific functions and second is Plane management : manages and coordinates functions related to the whole system

The *ATM* physical layer deals with voltages, bit timings, and framing on the physical medium. The *ATM* layer is the heart of its standards. It denotes the formation of the *ATM* cell. The *ATM* adaptation has two sub-layers:

- **Convergence Sub-layer (CS)**

It decides the Class of service (CoS) for the receiving data traffic. And it gives a specific AAL service at an AAL network service access point (NSAP).

- **Segmentation and Reassembly Sub-layer (SAR)**

Segments higher – level user data into 48 – byte cells plus necessary overhead at the sending node and reassembles cells at the receiving node.

2.5.1.6 SONET/ SDH

The fiber-optic cable which has high bandwidth is most appropriate for nowadays maximum data rate technologies and for moving a big numbers of low rate techniques instantly. To achieve it the significance of fiber optics grows in conjunction with the progress of techniques requiring higher data rate or wide bandwidth for the transmission. Development of fundamentally similar and compatible standards called Synchronous Optical Network (SONET) at ANSI in The United States and Synchronous Digital Hierarchy (SDH) at ITU-T in European Union simultaneously. Among the concerns, there are three interests- First, SONET/ SDH is a synchronous network. A single clock is used to handle the timing of transmission and equipment across the whole network. Second, SONET/ SDH consist of recommendations for the suitable standardization of fiber optics transmission system apparatus sold by different manufacturers. Third, the SONET/ SDH physical specifications and frame design include mechanisms that allow it to bear signals from incompatible tributary systems particularly asynchronous services like DS-0 and DS-1.

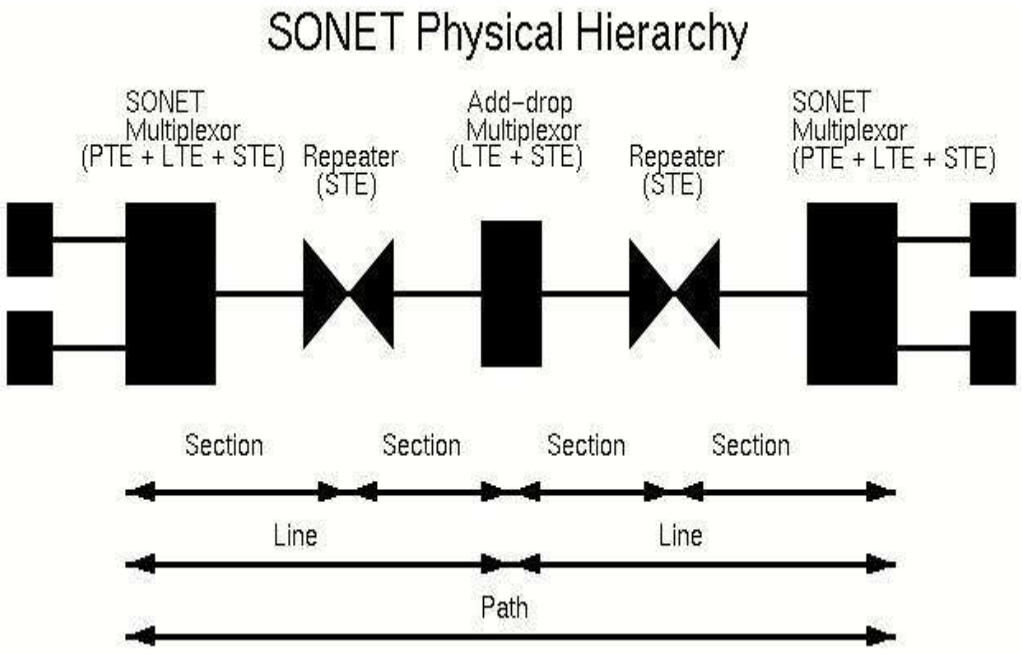

Fig 8. SONET System

Fig 8 shows the devices used in a SONET transmission system and some possible ways of arranging and linking those devices. SONET devices are:

Multiplexer/ Demultiplexer- either multiplexes signals from multiple sources into a Synchronous transport signal (STS) or demultiplexes an STS into different destination signals.

Repeater- an STS repeater takes a received optical signal and regenerates it. This device functions at the datalink layer.

Add-drop multiplexer- It is capable to attach signals receiving from various sources into a specified route or eliminate a most wanted signal from a route and retransmit it without demultiplexing the complete signal. It uses header information like pointers and addresses rather than bit positions.

2.5.2 Network

ATMs specifically connect with their host or ATM Controller directly through either

- Wireless network,
- ADSL or directly via a leased line
- Dial-up modem over a telephone line,

For ATMs point to multipoint design of wireless channel is provided to access multiple user terminals connect to a base station. Wireless point to multipoint channels are used both for fixed and for mobile access. The communication carrier uses a high power antenna to ensure direct line of sight between antenna installed on the roofs of ATM booth through sattelite. By wireless connectivity ATMs are more preferable at remote areas of the country. Government may provide moving ATMs to the people where they need it like traditional fairs, and small villages. Wireless ATMs are very useful in hilly areas, small islands where infrastructure development is very typical. In disaster management these type of ATMs installation give relief to the public immediately. Here we may use sattelite communication for this purpose. Satellite communications are used for organizing high speed, long distance microwave channels. Basically it is a self contained communication system with the ability to receive signals from a earth station and to transmit those signals back to another earth station with using transponders. Transponder is an integrated transmitter and receiver of radio signals. The main component of a sattelite includes the communications system that consists of the antennas and transponders, the power system, and the propulsion system. The power system

consists of the solar panels that supply electrical power, and propulsion system consists of the rocket which helps to propel the satellite. To get necessary power to locate itself in right orbit a satellite has a propulsion system and it helps to make occasionally corrections to its position. A satellite has thrusters those are helpeful to fire occasionally to do adjustments in its position. Like that existsting mobile network will help to send SMS of DynaPass to the user of ATM cum Debit card. Whenever a user swipe his/ her card in ATM bank server will send DynaPass as SMS to the user on his mobile number which is registered with bank. Here I discuss only about GSM technology which is mostly used worldwide. The same things may achieve from CDMA also by different techniques. GSM system includes three sub-systems, the radio sub-system (RSS), the network sub-system (NSS), and the operation sub-system (OSS). Here is main concern about only Radio subsystem for me and other two are beyond of my work. The radio subsystem includes entire radio particular entities like the mobile system (MS), and the base sub-system (BSS). A GSM network includes many BSSs and a base station controller (BSC) managed each BSS. The BSS performs all functions necessary to maintain radio connection to an MS, coding/ decoding of voice and rate adaption to/ from the wireless network part. In addition to a BSC, the BSS includes only a few base tranceiver stations (BTSs). A BTS includes entire radio equipment like antennas, signal processors, amplifiers required for radio transmission. A BTS can design a radio cell or using sector antennas, only a few cells and is connected to MS and to the BSC via different interfaces. A GSM cell can operate between approx. 100 m and 35 kms depending on the environment such as buildings, open area, hills etc. The BSC fundamentally manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. The BSC multiplexes the radio channels onto the fixed network connections. The MS has all user equipments and softwares required for communication with a GSM network. An MS includes user independent hardware and software and of the SIM (subscriber identity module) that stores all user specific data which is relevant to GSM. The most preference given to Leased lines as those need a very less time to make a connection and generally any Public Service Telephone Network (PSTN) provides this facility. Actually there is a need for fast communication between ATM and Bank server since minimum time required to do a transaction for a user. Since leased lines are so expensive that’s why banks estimate the traffic first to install ATMs. Machines on which a less traffic will usually depends on a dial-up modem over a PSTN line instead of using a leased line,

because a leased line comparatively more expensive to operate over a PSTN dial up line. Ethernet is currently the most common LAN standard. The term ethernet usually means a varient of the technology; variants include Fast Ethernet, Gigabit Ethernet, and 10G Ethernet. Ethernet is a network standard for data transmission at the rate of 10 Mpbs. This was standardized by the IEEE 802.3 workgroup, and since then, it has become an international standard. Nowadays 10G Ethernet used whis has speed of 10,000 Mpbs.

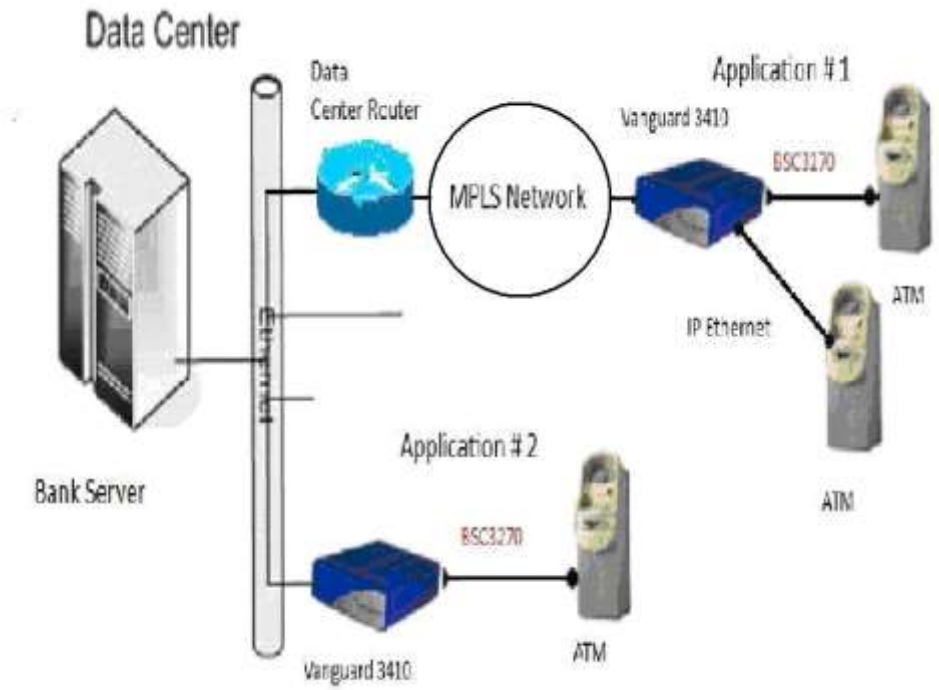

Fig. 8. An ATM machine Network model (NCR Corp)

The multiprotocol label switching (MPLS) technology combines the virtual circuit technique with the TCP/ IP stack functionality. It is another innovation in the field of integrating IP with virtual circuit technology. MPLS takes an intermediate position between the IP layer and the layers of frame relay, or ethernet, thus integrating them into the unified, more efficient structure.

MPLS Network: MPLS (Multiprotocol Label Switching) is a system in high-performance telecommunication networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels recognize virtual paths between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols. MPLS supports a range of access technologies, including T1/ E1, ATM, Frame Relay, and DSL.

MPLS is a highly scalable, protocol agnostic, data-carrying mechanism. Data packets are assigned labels in an MPLS network. The decision to forward the packets is exclusively made on the contents of this label, without the requirement to observe the packet itself. It allows the user to make end-to-end circuits for a transport medium by any protocol; type no matters. Most important advantage is to abolish dependency on a specific OSI model datalink layer technique, like Asynchronous transfer Mode (ATM), Frame relay, Synchronous Optical Networking (SONET) or Ethernet, and abolish the requirement for multiple layer-2 networks to persuade various kinds of traffic. MPLS belongs to the family of packet switched networks. The MPLS operation is generally performed amid Datalink layer i.e. Layer-2 and Network layer i.e. Layer-3, that's why this is habitually referred to like a layer 2.5 protocol. It was initially designed to offer a unified data-carrying service for circuit based clients as well as packet switching clients which provide a datagram service model. It can be used to carry many different kinds of traffic like IP packets, ATM, SONET, and Ethernet frames.

MPLS works by prefixing packets with an MPLS header, containing one or more labels. It is called a label stake and each label stake has four fields- a) A 20-bit label value, b) a 3-bit traffic class field for QoS (Quality of Service) priority, c) a 1-bit bottom of stake flag. If it is set, it signifies that the current label is the last in the stake, d) an 8-bit TTL (time to live) field.

These MPLS-based packets are switched after a label lookup/switch instead of a lookup into the IP table. As referred above, when MPLS was conceived, label lookup and label switching were faster than a routing table. The Label Distribution Protocol (LDP) is responsible to allocate labels amid LERs (Label Edge Routers) and LSR (Label Switch Routers). In the MPLS network, LSR is regular exchange label and it ensures the information regarding reachability through the standard procedures in order to make a full image of the network to use the forward packets. Whereas the network operator has formed the Label switched paths (LSPs) for various purposes, like to build network based IP virtual private networks or to route traffic along specified paths through the network. It is obvious that LSPs are just similar to permanent virtual circuits (PVCs) in ATM or Frame relay networks.

CHAPTER 3

SURVEY REPORT

We have done a survey on different ATM of various banks to check the existing protocol and working of existing machines. It is basically based on two points - A. Facility or services like cash withdraw, balance inquiry, card to card payment, and other services provided by ATM & B. How user's privacy is secure when he does the operations on ATM? According to a well known ATM manufacturer Die bold these have 4 threats- Fake ATM, Shoulder surfing, Skimming Devices and Fake keypad overlay attack. We have considered 5 banks- State Bank of India, Punjab National Bank, IDBI Bank, ICICI Bank and City Bank.

Attacks on ATM machines

I. **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.

Fig 6. Micro Camera Embedded in Different Positions

II. **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.

Fig 7. Skimming Device Attached to ATM

III. **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.

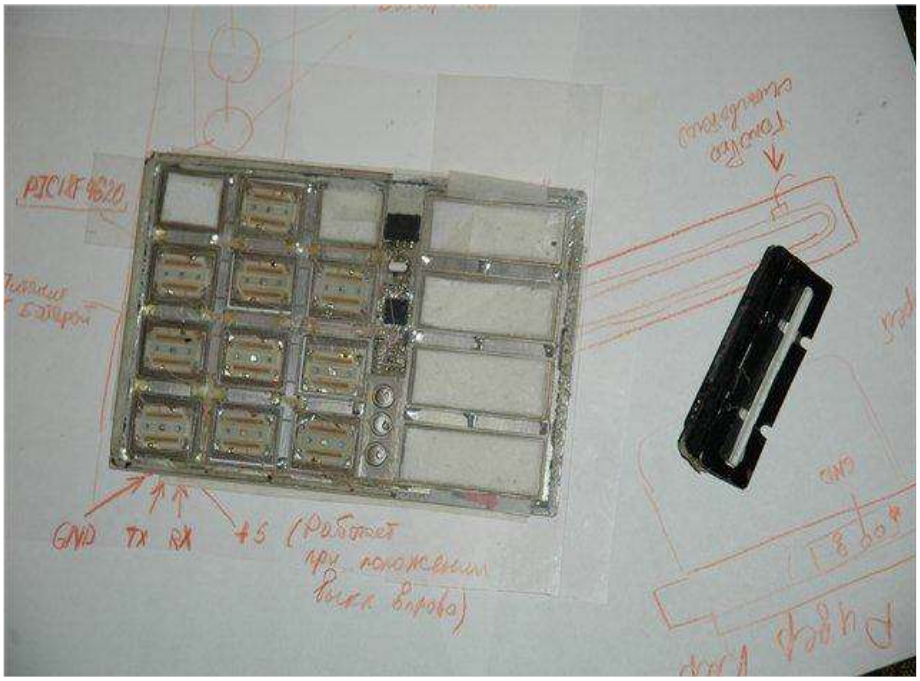

Fig 8. Fake Keypad

IV. 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.

Table-1

Facility	Bank Name				
	SBI	PNB	IDBI Bank	ICICI Bank	City Bank
A. Cash Withdrawal	Yes	Yes	Yes	Yes	Yes
B. Balance Inquiry	Yes	Yes	Yes	Yes	Yes
C. Mini statement	Yes	Yes	Yes	Yes	Yes
D. Cash Deposit	No	No	Optional	Optional	Optional
E. PIN Change	Yes	Yes	Yes	Yes	Yes

Table-2

Security Threats	Bank Name				
	SBI	PNB	IDBI Bank	ICICI Bank	City Bank
A. Fake ATM	Not possible	Not possible	Not possible	Not possible	Not possible
B. Shoulder Surfing	Possible	Possible	Possible	Possible	Possible
C. Skimming Devices	Possible	Possible	Possible	Possible	Possible
D. Fake Keypad Overlay Attack	Possible	Possible	Possible	Possible	Possible

SBI- State Bank of India

PNB- Punjab National Bank

CHAPTER 4

PROPOSED METHODOLOGY

Main object of the work is to conduct the reliability test of DynaPass and to propose two modified models of DynaPass, first of which will allow multiuser access of same account and the other will ensure user authentication. Here we try to enhance the security while using ATM. If there is an additional security of getting dynamic password or user authentication vide mobile phone for each and every transaction with account generated then it will give many fold times secure operation for an individual who has lost his/her ATM at any instance.

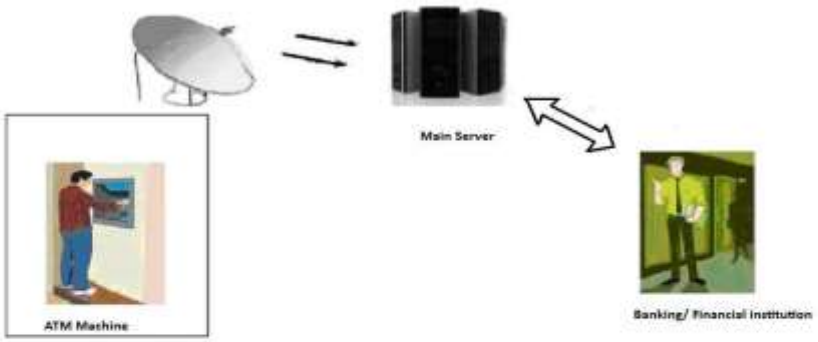

Fig. 9 (a). Normal Process of ATM transaction

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 or user authentication. So that in this proposed work I introduce the new authentication system which is highly secure and highly usable and based on multifactor authentication approach. It uses a sole approach to build a system to authenticate user and it is based on DynaPass (Dynamic Password) and SMS to enforce an additional security level over the conventional login in an ATM machine. The DynaPass is most sensitive data for any financial transaction through ATM, so DynaPass will be appeared in encrypted form on user's cell phone. The Financial institutions are liable for DynaPass creation and delivery

to the respective customers. The users access the ATM and enter the secure pin. The Control system authorizes the user and if that is an authentic user, then the access of system is given to the user, else the transaction is terminated.

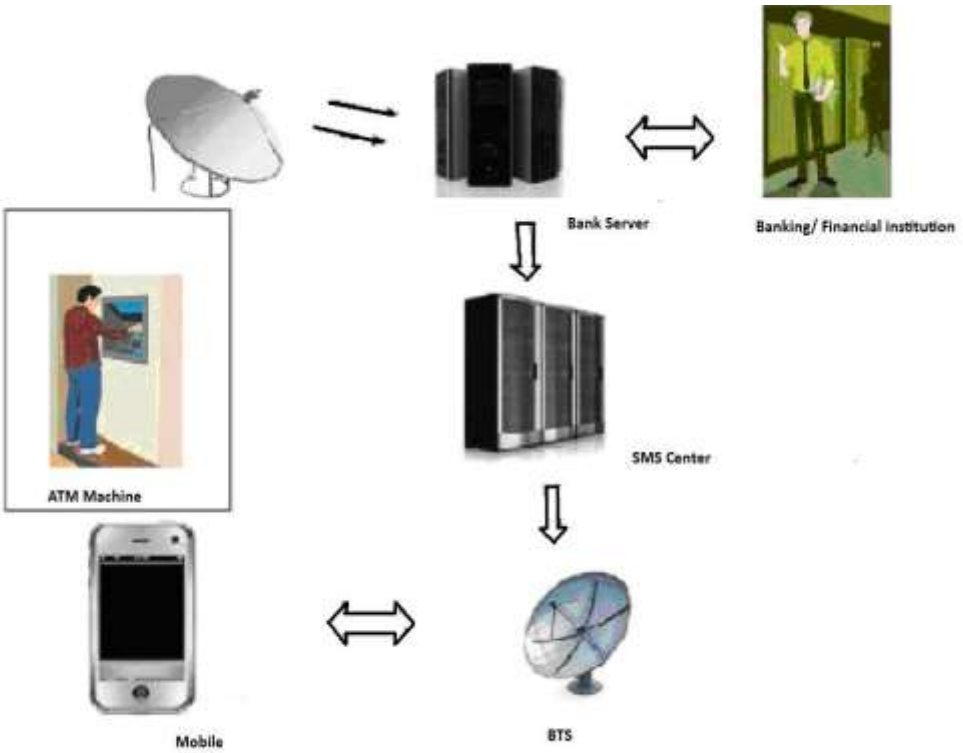

Fig. 9 (b). DynaPass Process of ATM transaction

For the next step the control systems processes 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.

The present method 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.

Step 3. If PIN matched then Go to Step 4.

Step 4. If not Go to Step 1

Step 5. And now ATM waits to enter the transactions request.

Step 6. User may use ATM now and transact.

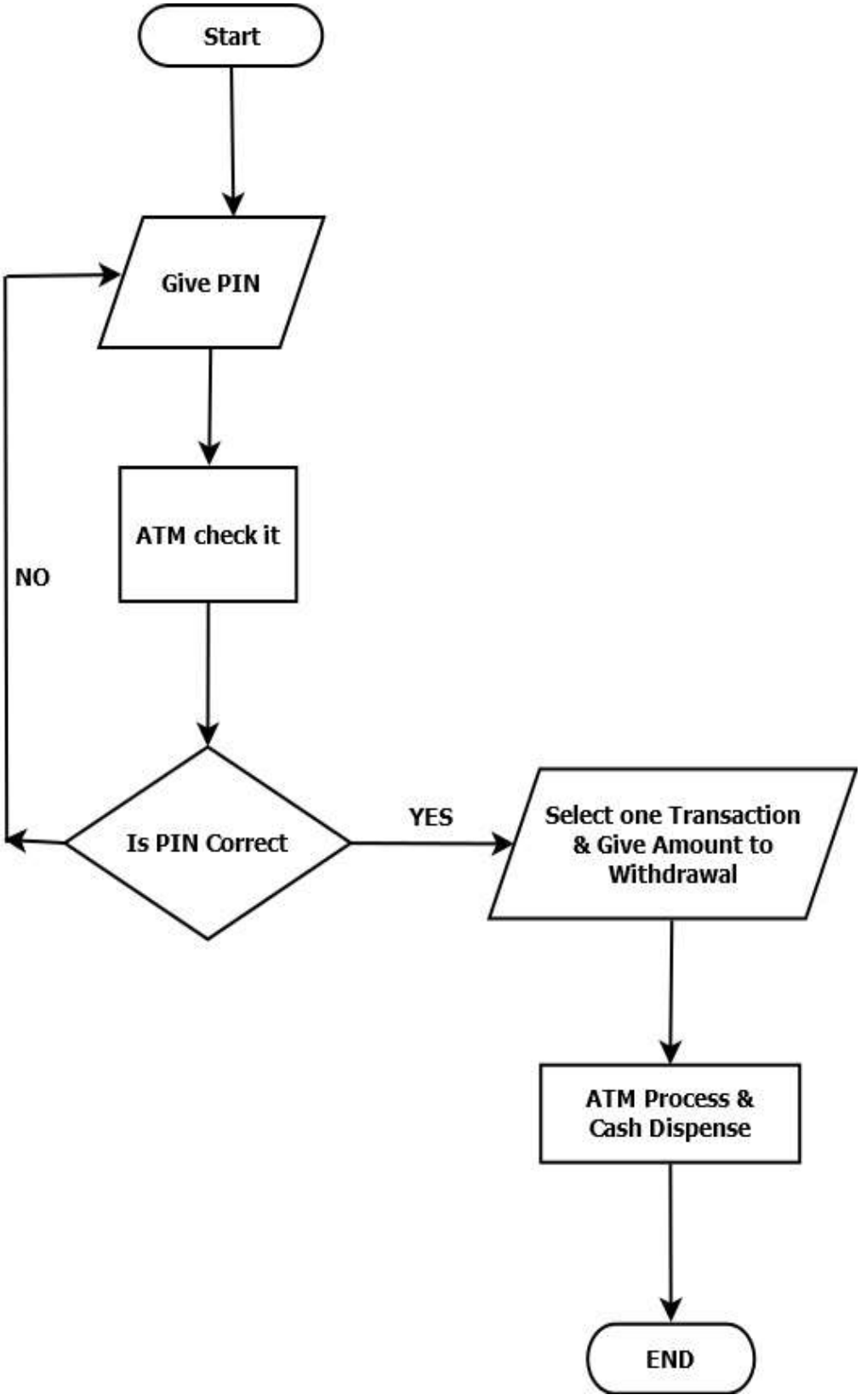

Fig 10. Flow chart for existing ATMs

The DynaPass method 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 Ubiquitous device.

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.

We here propose more secure third party authentication system, for the same it is required to register three or four persons including their mobile numbers through his debit card, who are part of the system. Only these registered people may do the financial transactions on behalf of the user.

Step 1. Bearer accesses user's account using Debit card through ATM machine with the help of PIN (the secret 4-digit number).

Step 2. ATM machine reads this card and after giving PIN 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.

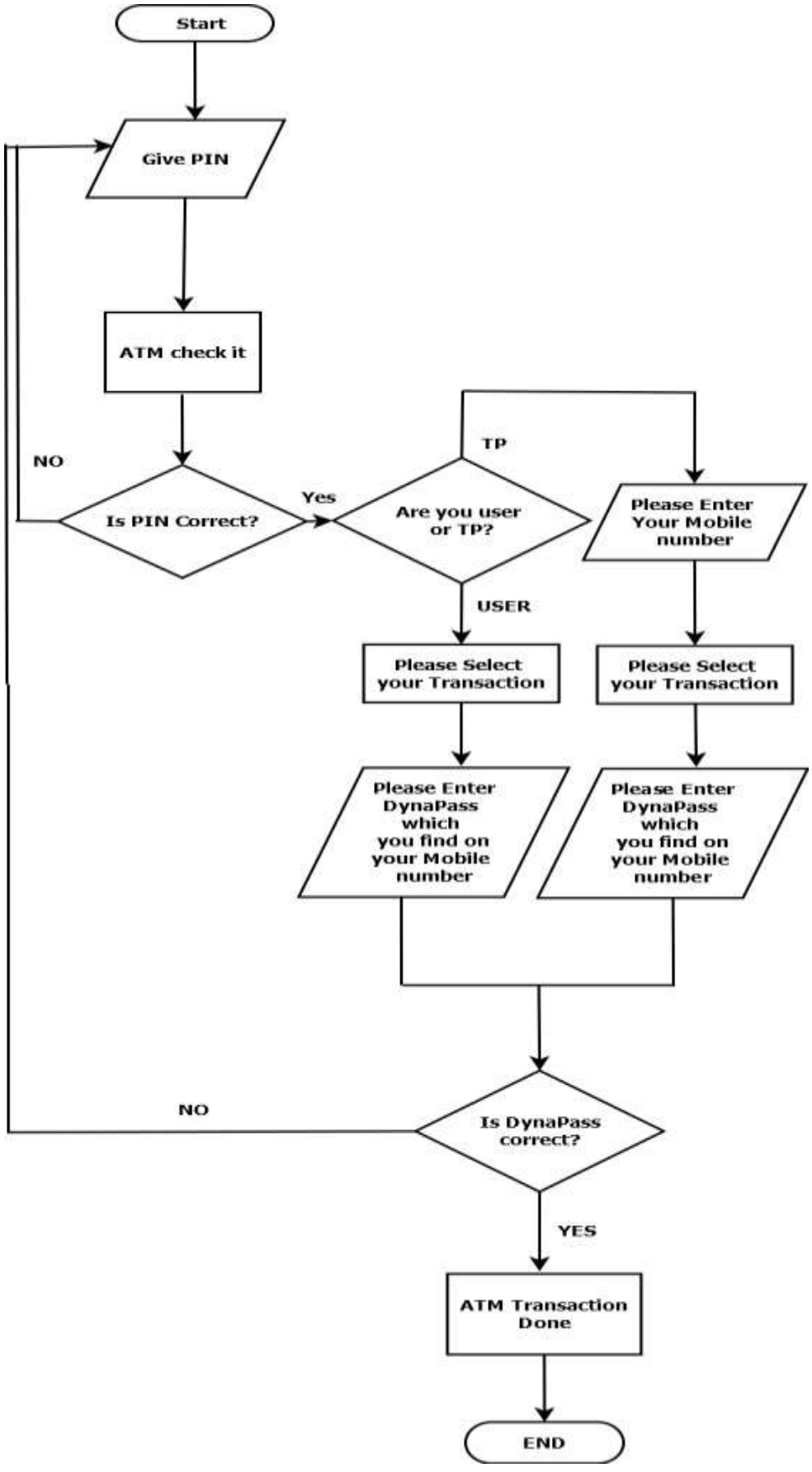

Fig 11. Flow chart for proposed ATMs

Another model proposed is of Biometric 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.

Step 9. ATM comes in initial ready state.

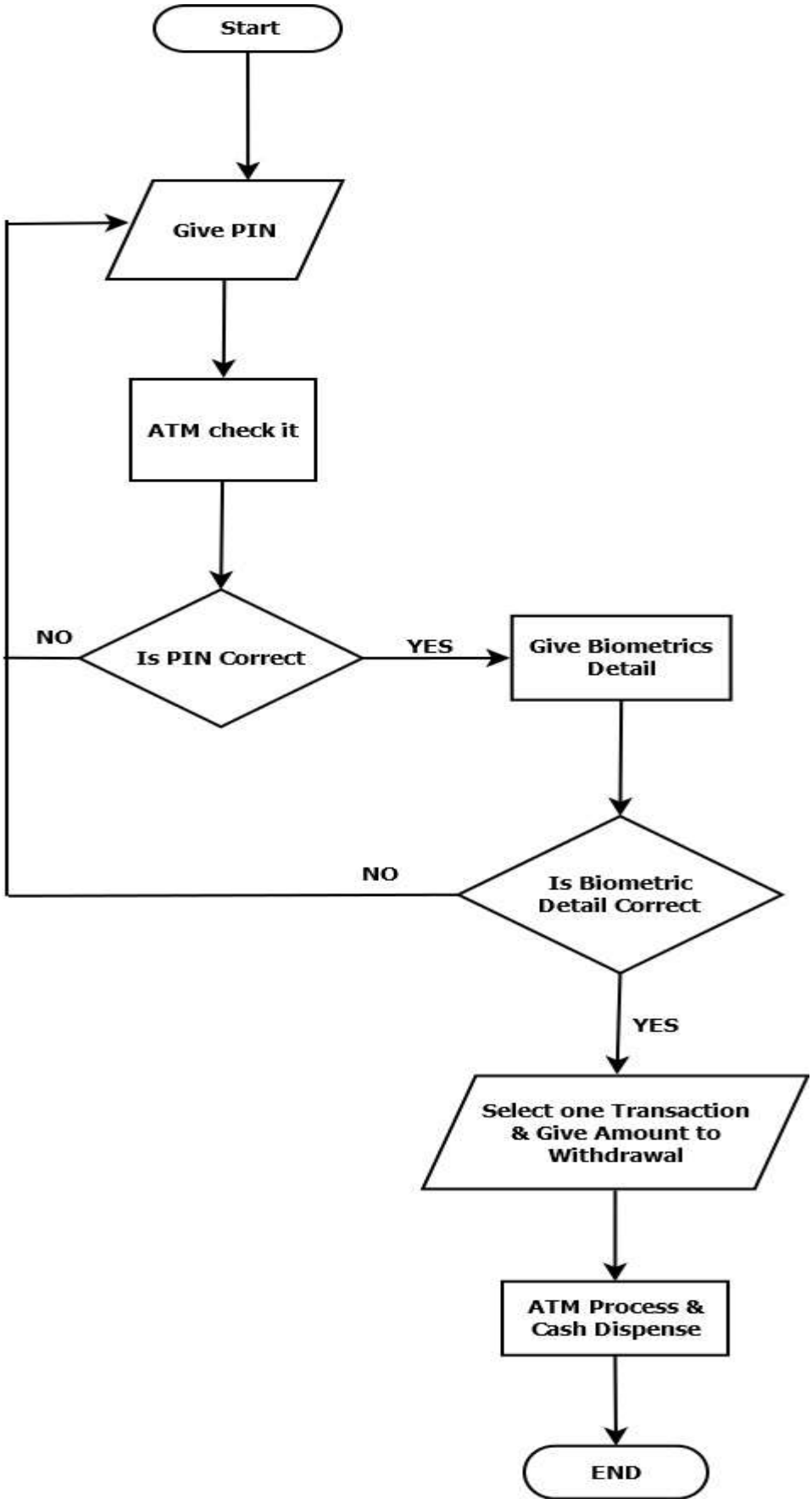

Fig 12. Flow chart for Biometric ATMs

As I worked on TiNA Pro, I have got the results and draw a screen shot as per following:

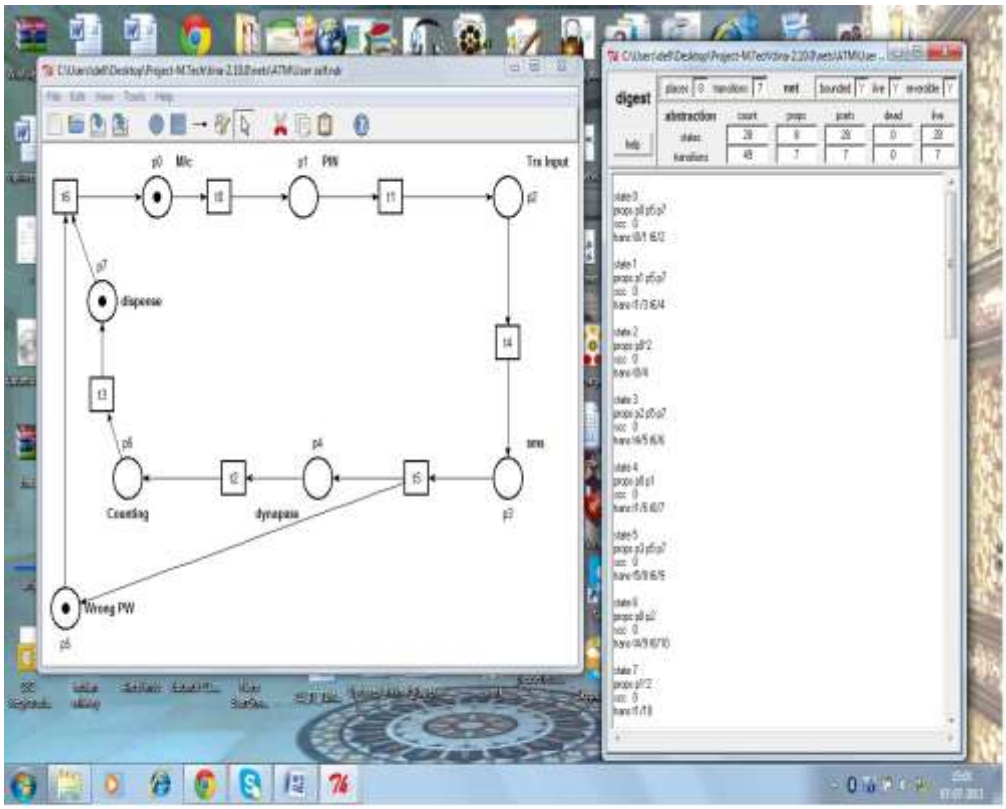

Fig 13. A Screen shot of Petrinet diagram in Tina Pro for Self

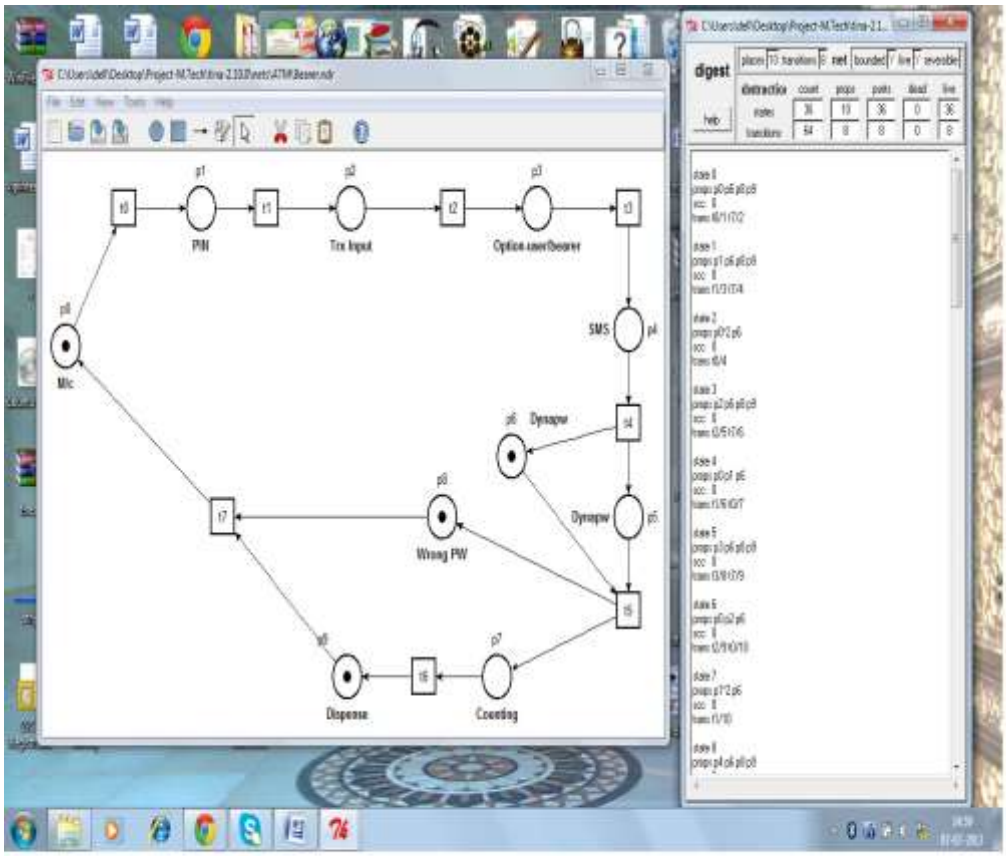

Fig 14. A Screen shot of Petrinet diagram in Tina Pro for TP

Chapter 5

RELIABILITY ANALYSIS

Since theft and forgery cases are very common in urban as well as rural areas in connection of using ATM machine called as ‘masquerading’. It is the case about to an ATM card stolen by anyone and he knows the static password anyhow, he can access the money through this stolen ATM card. There are 884 million subscribers (73% of population) in November 2011, up 154 million from November 2010 (**TRAI**, Jan 2012). 66 percent of mobile subscribers are urban dwellers [21]. It will grow day by day. These huge numbers of subscribers have getting the opportunity to use this mobile facility to join their banking system too. Many subscribers are using mobile banking right now but it is related to get SMS of the bank transactions.

A. Protocol validity- Here I use 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.

B. 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-3

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

Table-4

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.

CHAPTER 6

CONCLUSION & FUTURE WORK

6.1 Conclusion

In this dissertation work we have tried to analyze the performance of DyanPass a protocol designed for ATM transactions, which uses Mobile network and its data service for security.

A reliability analysis was performed on the DynaPass protocol using TinaPro a tool for protocol analysis. Also we analyzed the performance of the protocol on the basis of packet delivery, security and efficiency, and found the model is quite same.

But, over a period of time the mobile networks are becoming more and more vulnerable and the security is decreasing. To overcome the same we have proposed two more models of security namely:

1. Biometric Model
2. Bearer Model

Biometric model is a user authentication model which enhances the security of ATM transaction with human interface, while bearer model is more a validation model which allows transactions after dual validation.

These two models are slower than DynaPass but are secure. They have more number of transaction to be performed in a single transaction and have more algorithms involved in the model.

6.2. Future Work

In future the Biometric model and bearer model can be optimized in terms of time complexity so that the security can be enhanced. One may even attempt to design and develop a model combining both Biometric and bearer model so that more secure and single complete model can developed and deployed.

CHAPTER 7

TOOL USED

7.1 What is Tina Pro?

Tina (TIme petri Net Analyzer) is a toolbox for the analysis of Petri Nets and Time Petri Nets. At that time, the toolbox includes:

nd (NetDraw) : Time Petri net and Automata editor. It allows one to create a {Time} Petri nets, in textual or graphical form. It interfaced with the above tools.

tina : construction of reachability graphs. Depending upon the option retained, builds (references at the end of file):

The coverability graph of a Petri net created by the Karp and Miller technique. The markings reachability graph of a Petri net (untimed, or with timing information discarded).

struct : structural analysis of Petri nets. Computes generator sets for semi-flows or flows on places and/or transitions of a Petri net. Also determines the invariance and consistence properties.

7.2 About Petri Net

Petri nets are modeling tool based on graphic and mathematics which are suitable for many systems and they are also a capable tool for unfolding and studying information processing systems which are characterized such that concurrent, asynchronous, distributed, parallel, and/or stochastic. Analysis of communication protocols is one area, where Petri nets can be used to show necessary features of a system. Generalized Stochastic Petri nets and Extended Stochastic Petri nets, as tools relevant to normally distributed random variables extend modelling capacity in the area of communication protocols.

Here I refer several fundamental definitions, special kinds and behaviour of Petri nets known in literature to give a basis for Petri nets acronym. A Petri net is a meticulous type of directed graph. Initial state of Petri net is called the *initial marking*. Petri net diagram is

a bipartite directed, weighted graph including two types of nodes, called *place* and *transition*, and arcs connecting either place to transition or transition to place. A place that has an *outgoing arc* respectively *incoming arc* for a transition Ti is called *output place* respectively *input place* of transition Ti.

Definition 7.1*: A Petri net N is a 4-tuple* (**P**, **T**, ***Pre, Post***) *such that:*

P *is a finite and non-empty set of places (represented by a vector with entries* P1, P2, P3…), **T** *is a finite non-empty set of transitions (represented as a vector with entries* T1, T2, T3…), ***Pre*** *is an input function, representing weighted arcs connecting places to transitions called precondition matrix of size* [|**P**|,|**T**|],

Post *is an output function, representing weighted arcs connecting transitions to places called post-condition matrix of size* [|**P**|,|**T**|],

The following symbols are used for input and output sets of a place P and a transition T (***F*** is the set of arcs):

- ✓ ●T = {P|(P,T) ϵ F} = the set of input places of T
- ✓ T● = {P|(T,P) ϵ F} = the set of output places of T
- ✓ ●P = {T|(T,P) ϵ F} = the set of input transitions of P
- ✓ P● = {T|(P,T) ϵ F} = the set of output transitions of P

This information can be extended to a subset. For example, let *S1* ϵ **P**, then ●S1 is the union of all ●P such that P ϵ *S1*.

In graphical representation (see Fig 6) places are generally depicted as circles, transitions are depicted as bars or boxes. The Arcs are labeled with their weights (positive integers), where a *w*-weighted arc can be taken as a set of *w* parallel arcs. Labels for 1-weighted arcs are usually omitted. A marking assigns a nonnegative integer to each place. If a marking assigns to place Pi a nonnegative integer *Mi*, we say that Pi is marked with *Mi* tokens. Pictorially, the marking of a place is usually represented by black dots (Fig 13 A) or by a number (Fig 13 B).

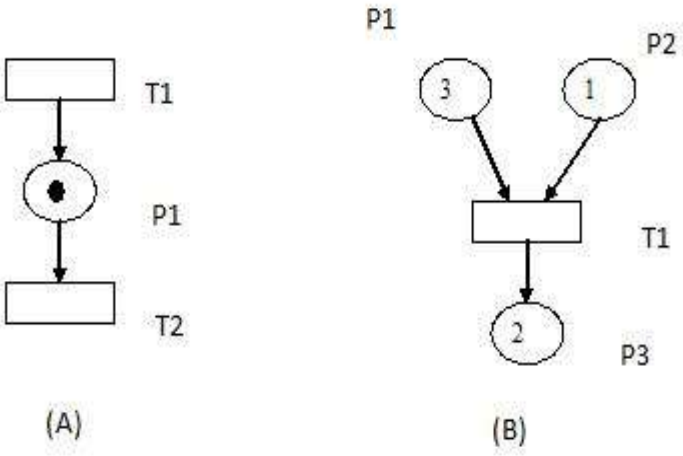

Fig 15. Petri nets

A transition without any input place is called a *source transition*, and transition without any output place is called a *sink transition*. Source transition is unconditionally enabled and firing of sink transition does not produce any tokens. A pair of a place P and a transition T is called a selfloop if P is both an input place and output place of T. A Petri net is said to be pure if it has no selfloops.

7.3 Ordinary Petri nets

A Petri Net is called Ordinary if all of its arcs re weighted by 1's. The dynamics of the Ordinary PN is described by moving tokens between places according to the *firing rules:*

- A transition T is enabled to "fire" if and only if each input place P of T is marked with at least one token.
- A firing of an enabled transition T removes token from each input place P of T, and adds token to each output place of T.
- No marking of the other places which are neither input or output of T remains unchanged.

7.4 Properties

There are two types of characteristics for studying Petri net model: characteristic, which depend on the early marking and those, which are independent of the early marking. The

first one type is known as marking dependent or behavioral properties, and the second one is known as marking independent or structural properties.

An example of structural properties is the strongly connect ness: Petri net N is strongly connected if there is a path from any place/transition to any place/transition.

A. Reachability

Reachability is a conceptual base to study and analyze the dynamic properties of any system. A marking *Mn* is called as *reachable* from marking *M0* if there exists a sequence of firings that transforms *M0* to *Mn*. The firing sequence is denoted by:

s = M0 T1 M1 T2 M2 ... Tn Mn

Or simply s = T1 T2.... Tn

B. Boundedness

A Petri net (N, M0) is called as k-bounded or simply bounded if the number of tokens in each of the place doesn't go beyond a finite number k for any marking $M \in R(N, M0)$. A Petri net (N, M0) is called to be safe if it is 1-bounded.

We say, that a Petri net N is logically restricted if it is restricted for any finite initial marking M0.

Definition 2.5: A Petri net is logically restricted if an m-vector y of positive integers such as $A \cdot y \leq 0$. A exists in the incidence matrix.

C. Liveness

The concept of liveness is precisely zero deadlocks in operating systems.

Definition 7.2: A Petri net (N, M0) is called live (or equivalently M0 is said to be live marking of N) if no matter what marking has been reached from M0, if it could trigger ultimately fire any transition of the net by processing through some further firing sequence.

This means, that a live Petri net guarantees zero deadlock operation, irrespective of what firing sequence is preferred. Liveness is an ideal characteristic for many systems, but for some systems it is very difficult to verify this strong property. Following relaxed condition, which defines several levels of liveness of transitions vas?

7.5 Analysis of Petrinet Models

The cover ability tree involves basically the details of all reachable markings of Petri nets coverable markings. This should be applicable to all classes of nets, however is limited to “small” nets due to the complexity of state-space explosion. For a bounded Petri net the cover ability tree is called reach ability tree because it contains all marking reachable from M0. From the initial marking M0 in a Petri net N, it possibly reaches to marking equaled to the number of enabled transitions. If new marking Mi is not dead marking of N, from each new marking Mi, again reach more markings. A tree representation of the markings, where marking Mi are nodes and the arcs represent transitions firings. Such representation will be infinitely large for unbounded PN.

CHAPTER 8

REFERENCES

1. S. Kanwal, N.A. Zafar, Formal model of automatic teller machine system using Z notation, International conference on Emerging technologies (ICET), Islamabad, 2007, pp. 131–136.
2. Kurita, S.; Komoriya, K.; Uda, R., "Privacy Protection on Transfer System of Automated Teller Machine from Brute Force Attack," *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on* , vol., no., pp.72,77, 26-29 March 2012
3. ATM of Banks: Fair Pricing and Enhanced Access - Draft Approach Paper, Reserve bank of India, Technical report, 2007.
4. Lasisi, H.; Ajisafe, A.A., "Development of stripe biometric based fingerprint authentications systems in Automated Teller Machines," *Advances in Computational Tools for Engineering Applications (ACTEA), 2012 2nd International Conference on* , vol., no., pp.172,175, 12-15 Dec. 2012
5. ATM crime: Overview of the European situation and golden rules on how to avoid it, European Network and Information Security Agency, Aug. 2009, Technical Report.
6. Nitin Munjal and Rajat Moona. “Secure and Cost Effective Transaction Model for Financial Services”. OPNTDS-09, 2009
7. James J. MCAndrews “Automated Teller Machine Network Pricing – A Review of the Literature” Review of Network Economics Vol.2, Issue 2 – June 2003
8. 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
9. 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
10. 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.

11. 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.

12. 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.

13. 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.

14. W. Adi, A. Mabrouk, A. Al-Qayedi, A. Zahro: (2004), Combined Web/Mobile Authentication for Secure Web Access Control, Wireless communications and Networking conference, IEEE Communications Society, pp. 677- 681. March 2004.

15. MasterCard Inc.: (1997), SET Secure Electronic Transaction Specification, Book 1: Business Description, MasterCard Inc., May 1997, http://www.win.tue.nl

16. A. Qadrei, S. Habib, Allocation of Heterogeneous Banks' Automated Teller Machines, First International Conference on Intensive Applications and Services, Valencia, 2009, pp. 16–21.

17. Tsutomu Matsumoto,Hiroyuki Matsumoto,Koji Yamada,Satoshi Hoshino," Impact of Artificial "Gummy Fingers" on Fingerprint Systems," Optical Security and Counterfeit Deterrence Techniques IV,Rudolf L. van Renesse, Editor,Proceedings of SPIE Vol.4677,pp.275-289,SPIE — The International Society for Optical Engineering,2002.

18. J. Hall, S. Kilbank, M. Barbeau, E. Kranakis: (2001), WPP: A Secure Payment Protocol for Supporting Credit- and Debit-Card Transactions over Wireless Networks, IEEE International Conference on Telecommunications (ICT), Bucharest, Romania, Volume 1, June 2001.

19. V. Pasupathinathan, J. Pieprzyk, H. Wang and J.Y. Cho: (2006), Formal Analysis of Card-based Payment Systems in Mobile devices, Fourth Australasian Information Security Workshop, Conferences in Research and Practice in Information Technology, Vol.54, pp. 213-220, January 2006.

20. Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Sugata Sanyal and Svein Knapskog: (2007) A Multifactor Security Protocol For Wireless Payment-Secure Web

Authentication using Mobile Devices, IADIS International Conference, Applied Computing 2007, Salamanca, Spain, pp. 160-167, February 2007

21. Mitzenmacher M., Upfal E.: (2005), Probability and Computing: Randomized Algorithms and Probabilistic Analysis, Cambridge University Press, New York, NY.,2005.

22. Soriano M. and Ponce D.: (2002), A Security and Usability Proposal for Mobile Electronic Commerce, IEEE Communication Magazines, Volume 40, Issue 8, pp. 62- 67, August 2002

23. Please refer it to get data for mobile users in India http://www.trai.gov.in/WriteReadData/trai/upload/PressReleases/859/Press_Release_Nov-11.pdf

24. William Stallings: (2003) Cryptography and Network Security Third edition, Pearson Education, 2003