2.1 REVIEW

This review of Auto teller machine seeks to analyze relevant research documentation and findings already available to improve this research and its competence to investigate the concern it seeks to fetch about. Different organizations have framed different definitions. Several researches have been carried out on banking regarding their corporate social responsibility globally and it is important to examine them in relation to this research topic. This will enhance effectiveness and stimulate an all inclusive analysis and discussions of critical issue in relation to the vulnerabilities or weaknesses in Automated teller machine and its security issues under consideration.

The content of this Chapter comprise the theoretical study of various issues related to the topic and review on the current scenario. Before starting the research in depth in same area we have reviewed more than 30 research papers, white papers, reports and other literature related to our topic to analyze the points in-depth of review which find its places in our review. These literature points supports in to sets of the frameworks and the empirical study which are evidence of this research. In this chapter firstly we have reviewed about the Automated teller machine processing and thereafter for different vulnerabilities and an analysis on attacks in current time and vulnerabilities is carried out. This step by step analysis is represented by describing the different ways in which Automated teller machine transactions becomes vulnerable or are attacked. The discussion then moves on to various types of weaknesses/vulnerabilities/attacks and threats which have been discovered by other researchers. After this we analyze different ways of securities and protections, which are provided and what are the current
status of defenses from these vulnerabilities, which have been developed to protect against these attacks categorizing them and analyzing how successful they are useful in protecting against the attacks. This review covers various types of vulnerabilities, which have been discovered till now and different security solutions having declared all current schemes for protecting Automated teller machine transactions are lacking in some ways, the key aspects of the problem have been identified. This is followed by a proposal for a more robust defense system which uses a small security concept to protect cash and consumer both at the time of abnormal situation of cash dispensing.

The Automated teller machine has now become inseparable part of our daily life and it has gained such an important place that it’s strange to think it was ever cutting-edge technology of life without this helpful machine easing our life; which began in the 1960s, with establishment of first cash-dispensing Automated teller machine by Barclays Bank at its in London branch beginning of revolutionary era in banking sector. With lapse of time Automated teller machine is more mere cash dispensers but has been developed into self supported system and aiding its users customers to carry out a range of banking activities, including deposits and mobile phone top-ups.

Given that the Automated teller machine is such a prominent feature in people’s lives, it’s important to understand its background, technical development and its capabilities. Here’s a quick introduction to the Automated teller machine and its global significance, Automated teller machine was first introduced as punched card-accepting Automated teller machine by Barclays in London branch in 1968 but this was not in fact the very first incarnation of the Automated teller machine as CitiBank, then known as First National City Bank, already introduced a version of the Automated teller machine known as the Bankograph in American branches in 1960. The Bankograph did not allow the customers to withdraw money but instead allowed them to pay bills without the assistance of bank staff or the machine was meant for receiving cash in form of paper notes as well as coins. Moreover, Barclays’ 1968 addition was cumbersome as cards were regularly swallowed by these early Automated teller machines which allowed the scope for research for multiple usable cards for convenience. Apart from United State of America and United Kingdom, works were going on to develop machine for
use by banks in North America and Western Europe and growth in research of Automated
teller machine was rapid. In 1969, the first machine to use magnetically encoded plastic was
installed by Chemical Bank at New York, although initial take-up was slow as the running
costs for these machines, known as Docutellers, outstripped the cost of hiring a human teller
and it led to modification and machine known as Total Teller was introduced in the early 1970s
with added features and Automated teller machine began spreading in banks across the two
continents. Today, Automated teller machine has gained popularity across the globe. Experts
estimate that developed countries like the USA, Canada, the UK and Japan have a high
concentration of Automated teller machine per capita, while steady economic growing countries
like India and China has seen fairly large growth in the number of bank machines in the last
decade. However, it’s not just the number of Automated teller machine that has increased
throughout the world but also its functions. Apart from withdrawing and depositing cash, modern
Automated teller machine also allows you to put credit on a mobile phone just by entering your
phone number of the keypad. What’s more, some machines will let you pay money into a
beneficiary’s account, while others will print mini bank statements of your last few transactions.
Though Automated teller machines are universal and easily accessible in wealthier countries,
they are relatively scarce in some regions - like the Middle East and Africa - means that the
industry still has the potential to grow[12]. As a result, Automated teller machine software and
its applications are in constant development, as companies investigate the benefits and drawbacks
of different platforms in varying environments. However, as software changes, so does the
concern for Automated teller machines’ security. Today’s biggest worry for Automated teller
machine industry professionals is to maintain the security of global systems beyond the traditional
advice to consumers to keep their PIN secret. The development of chip cards and Chip and
Pin technology has helped to combat Automated teller machine from fraud to certain degree
but there are still scope for advancements and improvements

In order to operate Automated teller machine successfully, a bank needs computer hardware
and software, internet service provider, adequate bandwidth, quality ICT employees, reliable
electric power supply to Automated teller machines. Automated teller machines have to be
placed at a point where it can be viewed widely and very convenient for users.
There are two types of Automated teller machine are card based and card less. A card based Automated teller machine has a card reader to read a card (token), display panel, Keypad, a printer for receipts, an area for deposits, a money dispenser and a processor. A card less automated teller machine has a biometric input device to receive biometric information of the user in place of card reader and rest all the devices except the card reader of an Automated teller card reader machine.

Here in figure given below an External device Architecture of Multi Function Automated teller machine shown with various parts description:

![Multi Function ATM](image)

**Figure 2.1 : ATMs’ external hardware structure**

The internal hardware structure has shown by internal components of an Automated teller machine can be easily identified[13].
Figure 2.2: ATMs’ internal physical hardware structure

To better understand the functioning of an Automated teller machine here we are explaining the functioning of each unit.

Automated teller machine mainly consist of eight units, these are:

**CARD READER:**

Card reader is a device to read encoded information from ATM Card to identify particular account number of the user. The encoded information are available in the magnetic stripe on the back of the ATM card. For passing the encoded information to Automated teller machine, the card has either to be swiped or to be pressed on the card reader. Automated teller machines’ card reader captures account information from ATM card and passes on to the host processor. In Automated teller machine of old designs the ATM cards are swallowed by the Automated teller machine.
KEYPAD –

Keypad used Automated teller machines have numerical input and is used for various inputs like PIN number and to amount of money etc. Keypad also has some functional keys apart from numeric key pad for carrying out different functions related to commands displayed on the display board. Once the Automated teller machine reads the information from ATM card, it verifies the authenticity of the card user by demanding to feed personal identification number (PIN) by the Key pad. The information passed by the user through the Key pad is matched by Automated teller machine with data available with ATM card and only after the information matches the Automated teller machine allows the ATM card use to proceed for further operations which he wants to perform like withdrawal, balance enquiry, etc.

DISPLAY SCREEN –

Automated teller machine displays different operations instructions which has to be carried out by the user on the display screen for the user and user has to fulfill the demand of Automated teller machine by supplying the data through the Keypad. Automated teller machine displays all transaction information provided by user on the Keypad including some for which may appear hidden as * being encoded in place of input formation put up by the ATM card.

RECEIPT PRINTER –

Automated teller machine have inbuilt device of printer which gives the print out of all the details of transactions made regarding your withdrawal like the date and time and the amount withdrawn and also the balance amount in the bank is also shown in the receipt. Thus a paper receipt of the current transaction is obtained by the user.

CASH DISPENSER –

This is the central system of the Automated teller machine from user receives the required money is obtained.

BIOMETRIC DEVICE –

Biometric device is a device to measure biometric parameters and attached with Automated teller machine, which works on biometric information than card reader. The device receives impressions of the users customer like finger print and other impression to identify the user.
STORAGE DEVICE –

It is used to temporarily store a database of customer information from the card and/or biometric information for matching the information on the steps to be followed in subsequent steps.

PROCESSOR –

Processor is configured to receive the input signals from the input device, receive biometric information from the biometric device, and access the database of customer information in response to the input signals to obtain data about the customer identified by the customer identifier, biometric information for the customer. The processor then compares the received information including biometric information available with bank, compares the two sets of information to verify whether two sets of information match to together or not, the passes the confirmation report to bank as well at display panel either confirming identify has been confirmed or further access has been denied. It is only after confirmation of matching of the two sets of information, Automated teller machine allows the users to proceed any further.

WORKING PROCESS:

An Automated teller machine is a real-time front terminal of automatic teller services with the support of a central bank server and a centralized account database.
Once card reader reads the information from the magnetic strip, using the bank’s routing number, the Automated teller machine connects the user to the main host computer of the bank opening the further communication channel. Once connected, the Automated teller machine allows the user to perform various operations of banking. For example, whether the user wants to withdraw money or user requests for an amount to be send to the any other bank account or beneficiary, Automated teller machine also checks whether requisite amount is available in the users account. If the amount demanded is within permissible limit for withdrawing, the withdrawal is approved. Amount from users bank count is deducted or debited and Automated teller machine releases the amount by dispensing terminal. In case amount requested is more that permissible limit for the day or amount available in users account, Automated teller machine denies withdrawal. Data transfers takes place in encrypted form for safe and secure data transmission in a network data communication. To secure transmission it is essential to keep information like PIN number, password etc. totally of confidential and users are advised not to share these information with anybody including the bank officials.

**DISPENSING MONEY**

Once the Automated teller machine receives approval after processor allows the transactions to go through, Automated teller machine dispenses the specified amount of money through Dispenser slot of the machine. The money is held in a sealed container with a spring-loaded bottom to maintain pressure. Rubber wheels in contact with the top currency notes (bills) roll, causing the currency notes (bills) to be dispensed into holding area until correct amount is reached. Once the correct amount is counted out, the currency notes (bills) exit via the external slot to the user. The Automated teller machine then ejects the card in type of Automated teller machine where card are to be inserted, thereafter Automated teller machine prints the receipt and returns to standby mode.

Automated teller machine services are an important segment of all economics activity of individuals and have an important part of financial operations. An Automated teller machine is a self service system to satisfy users banking and financial operations. Automated teller machine is an electronic computerized telecommunication device for use by customers to operate their account from premises within or outside the bank and without any binding to perform banking transactions within banking hours only i.e. it is available to uses 24 hours a day on all day of week i.e. 24X7.
Information technology advancement is growing very quickly and has taken a lead especially in service sector to reduce the man power required as well direct interaction between Customer and the bank and Automated teller machine technological advanced equipment making a link between banks and its clients without direct manpower. This is a posture on service quality and customer satisfaction. The introduction of Automated teller machine was aimed at services of bank more efficient as well as accurate.

With growth bank sector and demand for increasing fast and accurate financial transactions, Automated teller machine has gained important role that too without human interaction. Since the Automated teller machine process the direct requirement of currency withdrawal and accepts deposits the security measures of Automated teller machine be considered in terms of its security of Automated teller machine and from different type of attacks or unauthorized transactions which can take place at Automated teller machine. With growing technology attempts have made to make the transactions hassle free, easy as well as secure, however there were number of challenges that have been encountered by the pioneers of this technology such as the security which led to developments meant to improve the confidence of the customers in this technology. Hackers or attackers keep an eye to gain the money from Automated teller machine from various fraud methods. There are so many weaknesses or vulnerabilities are identified by various researchers in Automated teller machine and time to time various security of Automated teller machine have been strengthened and research and development in the security of features of Automated teller machine is as never ending process. Hackers/unauthorized users are also busy in finding out ways and means to tackle the added security features of Automated teller machine for making fast money. In this chapter we have tried to mention the review on these weaknesses/ vulnerabilities which are found in Automated teller Machine till now and what the securities are to be developed or suggested by various researchers.

2.2 BACKGROUND OF THE STUDY:

The Automated teller machine was first introduced in the 1960s and as per report there were over 1.5 million Automated TMs installed worldwide by 2005. The Automated teller machine has enhanced the convenience of customers to enable him to access his cash requirement at his wish at any moment subject to availability of fund with him.
According to a World Bank report, published in 2010, the Automated teller machine per 100,000 adults in World was 44 in 2009 whereas the Automated teller machine availability per 100,000 adults in India was merely 3.55.

**Figure 2.4: ATMs’ growth in world**

**INDIAN PERSPECTIVE OF ATM GROWTH:**

Automated teller machine growth in India was very low compared to other emerging markets but it has gained momentum now and the number of automated teller machines is increasing by nearly 25 percent every year, mentioned in the Reserve Bank’s Report. As per news published by Times of the NPCI an umbrella organization promoted as by the Reserve Bank and banks for retail payments has put the total number of ATMs in India at 1,04,500 the end of October 2013. It is heartening to note that 59% of ATM belong to State Bank of India group; a group of banks in the public sector having very much presence in rural India. As per trend available and information provided by the banks, with rising popularity of the machine, number of Automated teller machine is increasing day by day and expected to cross two hundred thousand mark within next 4 years. However bulk of Automated teller machine are in metropolis and urban city.

“Although there has been a steady year-on-year 25 percent growth in the number of Automated teller machines in the country, their penetration as measured by the number of Automated teller machines per million population is still very low when compared to other emerging markets,”
RBI Governor D Subbarao said in his keynote address at the IDRBT Banking Technology Awards Function. In proportional terms, India has one of the lowest numbers of Automated teller machines and POS (Point of Sales) terminals – 63 Automated teller machines and 497 POS per million populations\[15\][16].

### 2.3 Efficiency of ATM:

As in India the number of Automated teller machine user’s are very low, so for our analysis we consider the analysis published in Europian Journal of Scientific Research 2011 by Umar Faruq and Ahmed Yusuf of Bayero University Kano-Nigeria. We consider the figures and values of their survey to analyze the findings of various vulnerabilities and requirement to enhance the security of Automated teller machine. In this paper they mentioned that in Nigeria 77% users are using Automated teller machine, while 17% do not use the Machine and 6% are neutral. Out of this 77% of people that uses the machine, 62% are comfortable with the usage while 24% are not comfortable and 14% neutral. 31% of users believed that Automated teller machine is reliable while 43% said the network is not reliable. 26% of users said that Auto Teller machine security is reliable while 43% believed that Automated teller machine security is not reliable.

Considering these fact and findings we analyze that bank are providing various functions with securities in Automated teller machine but still there are some vulnerabilities and still more security is required towards the secure and reliable transactions in Automated teller machine. Our study is now based on these findings on various vulnerabilities and different security issues on Automated teller machine.

Financial institutions have implemented many strategies to upgrade the security at their Automated teller machine and reduce scope for fraud. These include choosing a safe location for installing the Automated teller machines, installation of surveillance video cameras, remote monitoring, anti-card skimming solutions, and increasing consumer awareness by informing them of various methods of safeguarding their personal information while transacting at the Automated teller machine or on the Internet.
2.4 REVIEW ON VULNERABILITIES:

A report has been published on Computer Attack and Cyber terrorism: “Vulnerabilities and Policy Issues for Congress” in April 2005. This report provides background information for three types of attacks against computers (cyber attack, physical attack, and electromagnetic attack), and discusses related vulnerabilities for each type of attack. In this report, three Methods for Computer attack have been defined. A computer attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data. Different attack methods target different vulnerabilities and involve different types of weapons or peripherals, and several of may be within the possession/current capabilities of many of the terrorist groups. Three different methods of attack are based on the effects of the weapons used. However, as technology evolves, distinctions between these methods may begin to blur.

A physical attack involves conventional weapons directed against a computer facility or its transmission lines;

An electronic attack (EA) involves the use the power of electromagnetic energy as a weapon, more commonly as an electromagnetic pulse (EMP) to overload computer circuitry, but also in a less violent form, to insert a stream of malicious digital code directly into an enemy microwave radio transmission; and

A computer network attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness of its software, alter the system configuration, or in the computer security practices of an organization or computer user. Other forms of CAN are enabled when an attacker uses stolen information to enter restricted computer systems[17].

Considering the above report we found that Automated teller machine vulnerabilities are also categorized on three areas and in each area there are various vulnerabilities found in the Automated teller machine system which makes the banking transaction unreliable or insecure and allows the fraudulence to be carried through a Automated teller machine. Vulnerabilities are categorized in bellow given three areas:
Physical vulnerabilities

Communicational or network vulnerabilities

Software or logical vulnerabilities

2.5 MAJOR AREAS OF STUDY:

Auto Teller Machine is extended facility of direct banking financial transactions and the customers are getting accustomed to Automated teller machine increasingly day to day with new technologies and so is the growth rate of fraud and unauthorized access of accounts is growing fast. In this sequence Automated teller machine frauds are in the list of high rate of frauds or unauthorized transactions with Automated teller machine. Crime at Automated teller machines’ have become issue of importance worldwide that faces not only customers, but also to banks and other bank operators.

Diebold Inco (2002), indicated that fraud at the Automated teller machine although more difficult than at a POS, has recently become more widespread. Recent occurrences of Automated teller machine fraud range from techniques such as shoulder surfing and card skimming to highly advanced techniques involving software tampering and hardware modifications to divert, or trap the dispensed currency[18].

Automated teller machine fraud issues in the most part involve token based fraud i.e. ATM card based frauds. The Automated teller machine analysis shows that significant number of token/card based transaction were used genuinely in one specific location prior to detection of subsequent fraudulent transactions. Automated Teller machines may be the mechanism used to convert compromised or cloned credit cards and debit cards into hard cash, so long as the card fraud included falling of the personal identification number (PIN) in unauthorized hands[19][20].

Automated teller machine skimming is type of physical vulnerability is now common in most parts of the world that have a mature network of Automated teller machines’, self-service terminals and point of sale (POS) terminals that accept magnetic stripe based credit cards and debit cards. Most bank Automated teller machine security issues and Automated teller machine fraud issues involving Automated teller machine skimming are the result of criminals attaching a
skimmer to the Automated teller machine card reader slot. Europe has historically been one of the most targeted geographical territories for Automated teller machine skimming attacks, although the world-wide spread of such Automated teller machine skimming fraud has been, and continues to be significant. As per the report published in BACKGROUND PAPER: PLASTIC CARD FRAUD By Hanna Mohammad, in May 2011 Skimming is a form of magnetic stripe counterfeiting in which criminals are able to copy magnetic stripe track information (including Card Verification Value - CVV) from a valid card[21]. Information may then be encoded on a counterfeit or stolen card and used fraudulently. According to APCA, almost $35 million was skimmed from Australian-issued credit, debit and charge cards both in Australia and overseas in the financial year from 1 July 2009 to 30 June 2010. This is a reduction from the previous financial year where an estimated $45 million was skimmed between July 2008 and June 2009. The reduction is thought to be due to financial institutions responding to a series of skimming attacks on Automated teller machines and EFTPOS terminals during 2009, as well as the progressive rollout of chip technology, which has seen a reduction in skimming fraud on Australian-issued credit cards[22].

<table>
<thead>
<tr>
<th>Period</th>
<th>2007-08</th>
<th>2008-09</th>
<th>2009-10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Locations</td>
<td>Numbers</td>
<td>Value (AS $)</td>
</tr>
<tr>
<td>IN Australia</td>
<td>Numbers</td>
<td>32572</td>
<td>18786287</td>
</tr>
<tr>
<td>Total</td>
<td>68,493</td>
<td>42,969,977</td>
<td>72,690</td>
</tr>
</tbody>
</table>

Table 2.1: Fraudulent transactions rate using ATM cards

Source: APCA Annual Review 2010
Automated teller machine deposit fraud which includes both cash deposit fraud and cheque fraud (check fraud) at automated teller machines is one type of Automated teller machine fraud that is particularly common in the US where many banks have a culture of crediting and allowing drawings against the deposit prior to manual reconciliation and verification.

Automated teller machine hacking should really only be used to describe attacks against the internals of the Automated teller machines software a type of software or logical vulnerability or network vulnerability, the Automated teller machines systems security but is commonly used to describe attacks against card processors and other components of the transaction processing network. The US have experienced a number of high profile ‘automated teller machine hack’ attacks against well known credit card and debit card processors. Some of the systems security breaches have included compromise of the PIN in addition to the card data, with subsequent fraudulent spend using cloned credit cards and cloned debit cards at Automated teller machines.

In terms of logical or software attacks Computer hackers opportunistically scan the Internet to find and infect computer systems that are mis-configured, or lack current software security patches. Compromised computers can become part of a “bot network” or “bot herd” (a “bot” is a remotely controlled, or semi-autonomous computer program that can infect computers), sometimes comprised of hundreds or thousands of compromised computers that can all controlled remotely by a single hacker. This “bot herd” hacker may instruct the computers through an encrypted communications channel to spy on the owner of each infected computer, and quietly transmit copies of any sensitive data that is found, or he may direct the “herd” to collectively attack as a swarm against other targeted computers[23].

In the paper of Financial Fraud Action Group UK (2010). Fraud the Facts 2010, the Definitive Overview of Payment industry and Fraud and Measures to Prevent it, Financial Fraud Action Group UK mention in his paper the type of software vulnerability defined is the Malware (including key loggers and spyware) are the type of software vulnerabilities that as one of the key cyber threats to the financial industry. Spyware is installed on a victim’s computer or false Automated teller machine and with the use of malware criminal record what keys are pressed such as online banking passwords or personal identification number (PIN)[24].
Another type of threat is Phishing refers to online scams that frequently use unsolicited messages purporting to originate from legitimate organizations, particularly financial services. Victims are deceived into disclosing their financial and/or personal identity information to commit or facilitate other crimes (e.g. fraud, identity theft and theft of sensitive information)[25] .

Another Automated teller machine fraud issue is ATM card theft which includes credit card trapping and debit card trapping at Automated teller machines for making duplicate cards or cloned cards. Originating in South America this type of Automated teller machine fraud has spread worldwide. Although somewhat replaced in terms of volume by Automated teller machine skimming incidents, a re-emergence of card trapping has been noticed in regions such as Europe where EMV Chip and PIN cards have increased in circulation[26].

Automated teller machine funds transfer to fraud is prevalent in Asia. This Automated teller machine scam involves criminals tricking of victims using the Automated teller machine to siphon off money into the criminals account.

Automated teller machine security attacks involving physical attacks against the Automated teller machine security enclosure are widely spread. Automated teller machine explosive attacks although originating and not uncommon in Europe are more prevalent in Australia and South Africa.

Automated teller machine ram raid incidents also occur globally but are most prevalent in the US, perhaps partly due to the large number of Automated teller machines deployed in soft-target locations such as convenience stores[27].

Automated teller machine security incidents involving a high degree of precision to gain access to the Automated teller machine security enclosure occur globally. The UK and Canada have experienced many such precision Automated teller machines security attacks in recent years.

Identifying vulnerabilities in the Automated teller machine system is an indispensable skill for the auditors of today. The sheer number of the Automated teller machine crimes and their wide variety make it very difficult for any person to grasp the essence of the subject. In CA journal October 2012 an article has been published by CAT.S. Subramanian has said, “After analyzing thirteen hundred cases, has classified the vulnerabilities into four groups viz., Customer and the
Bank being cheated, Machine failure, Security failure and Accidents. This article illustratively covers the point of ‘the Customers and the Bank being cheated’. Further, this article is an attempt to equip the auditors that would help them in detecting the loopholes that lay hidden in the Automated teller machine system. The Automated teller machine system has totally revolutionaries the banking services by reducing the hassles a customer had to endure in transacting with the banks, but the occurrence of an unprecedented number of Automated teller machine crimes has given it quite an amount of notoriety. It has placed a huge burden on the banks in the shape of extra security management. It has also cast on the auditor the additional responsibility of identifying and reporting on inadequate security in the Automated teller machine systems. It will be difficult for an auditor to understand the vulnerabilities of the Automated teller machine system without obtaining a good insight into the weaknesses of in functioning of the Automated teller machine system and the wide variety of vulnerabilities arising there from[28]. Once understood, it will give him an ability to identify risks and strengthen his audit procedures.

The analysis given below is based on the results of a detailed study of about thirteen hundred cases reported in news papers and articles from all over the world and in the internet. Most of the aspects of Automated teller machine frauds have been included, even though some of them may not be directly relevant from an audit point of view. Some of the cases might look imagined or exaggerated versions, but each method described here is based on actual facts. If a person attempts to study the vulnerabilities of the Automated teller machine, he would find himself drowned in cases of frauds so large in number and so wide in spectrum that he would not make any head or tail out of it. In order to obtain a proper grasp on the subject, classification under the following groups will help, viz., the risk of losses arising on account of:

1. The bank being cheated.
2. The customer being cheated.
3. The faults in the machines
4. The faults in software and procedures
5. Inadequacy or failure of security arrangements
Unforeseen circumstances and accidents

In this Part we discussed in details the point the bank or the customer being cheated.

A. THE BANK OR THE CUSTOMER BEING CHEATED

This heading falls into further five categories, viz., losses or damages caused by,

I. Outsiders (strangers),

II. Insiders (employees),

III. Technicians (engineers, service providers) and,

IV. Bank customers.

I. OUTSIDERS (Strangers)

The card and the PIN are essential for breaking into an account. It is surprising how human ingenuity has been used to find diverse methods for achieving this end.

(a) SHOULDER SURFING

‘Shoulder Surfing’ is the oldest method of collecting the PIN. The crook in guise of next customer stands behind the customer, looks over his shoulder, watches key being stroked by user and memorizes the PIN.

(b) SKIMMING

When a person collects the PIN as well as the card details without the knowledge of the customer it is known as ‘Skimming’. The customer notices nothing abnormal in the Automated teller machine, as his card goes through the card slot the crook receives the details of users’ card. This is achieved by pushing a ‘Skimmer’ (an electronic device in the shape of oblong black disk which is held in place by spring levers) into the Automated teller machine slot in a manner the that user has to swipe the card to skimmer before card reaches to Automated teller machine card reader slot. Since card has to pass through the skimmer’s slot first before reaching the Automated teller machine, the skimmer reads the data on the magnetic stripe on the card.
and transmits them to a device to crooks standing nearby or waiting in a parked car. Some skimmers are affixed with tapes just below the card slot. In another model, the body of the skimmer appears just like the original card insertion unit and thrust into the card slot. Imagine, skimmers have also been found inside the Automated teller machines. Retailers of small sized Automated teller machines turn into crooks and they fix skimmers inside a few Automated teller machines and place them in Malls and Plazas. They are genuine Automated teller machine but they record and store card details as well pass words and PIN. These are recovered later and used to withdraw funds. In a very recent case police arrested Pascari of Limerick city in Ireland who crafted his own custom-made skimmer equipped Automated teller machines by ordering the spare parts directly from Automated teller machines manufacturers. An electronically sensitive, thin, plastic sheet pasted within the card slot can also obtain the card details and transmit them. A notice “Due to recent fraud attempts at this Automated Teller Machine, we require you to swipe your card in the card reader below before inserting your card. We apologies for the inconvenience” can be found pasted on the Automated teller machine. This swiping device is fraud card reader or a skimmer fixed by the criminal; while Automated teller machine needs either insertion of card or swiping of the card but not the both at the same time. The entrance door of an Automated teller machine enclosure has ‘card swipe’ device for unlocking the door. Hacker may replace Automated teller machine of the bank with similar looking device having skimmers and collect the card details. In places where several Automated teller machines are set up in a row, the suspect places “Do Not Use. Out of Order” boards before all the Automated teller machines except to one to which he has attached the skimmer. The customers are automatically forced to use the Automated teller machine with the skimmer. Miniature pinhole cameras can video graphs the finger movements on the keypad and transmit them wirelessly. These are of the size of rupee coin and blend with the color of the Automated teller machine. They are fixed just above the keypad. Sometimes, they are painted to appear like a logo and fixed on the broad frame of the Automated teller machine screen itself. Slightly bigger cameras that focus on the keypad are hidden in document folders where a sticker hides the camera from view. For the customer, the keypad looks normal. But it has been overlaid with a mould in the shape of the original key pad, made out of thick applicable plastic material of the same color and containing some special electronic circuits. When a person presses a key in the
mould, the Automated teller machine key also gets pressed. The mould records the position and transmits the key stroke details to another device. It is called ‘Duplicate PIN Pad Overlay’. The customer thinks it is a protective plastic covering. But it is a thin transparent, touch sensitive, plastic sheet stuck above the PIN pad. It detects every keystroke and transmits them electronically to another device. This is an advanced version of the PIN Pad Overlay.

(c) FASLE AUTOMATED TELLER MACHINE FRONTS

Gangs involved in large scale Automated teller machine fraud operations prepare duplicate front panels of the Automated teller machine and get them installed over the card insertion and print out units thus covering them up. No one can make out that it is not a part of Automated teller machine. The Automated teller machine works normally but at the same time while customer’s card has to pass through this panel and the skimmer installed within the front panel transmits the card details to a receiver.

(d) FAKE AUTOMATED TELLER MACHINES

It is a common practice the world over to allow private non banking parties to install Automated teller machines in Malls and Plazas. They can be misused to collect card details and the PIN. Parties install Automated teller machines in such public places with bank stickers, hotline numbers etc., pasted all over but without any real connection to any network. Initially cash is disbursed to few. Later on, it starts displaying a note of technical error or “No funds”. After a few days, they remove the machine; recover the details of cards and PINs and also to get more than what they had given from the installed skimmer!

(e) STEALING THE CARD

Snatching from the hand bag/wallet containing the Automated teller machine ATM card and breaking open letter boxes to steal bank’s letters carrying the card or PIN, are the common methods used. A decent looking gentleman helps an elderly person or an uneducated lady by withdrawing the cash from Automated teller machine and gives back the card. But he gives back a fake card. According to a recent report in Odisha, the police arrested Balaram Sahoo, who had amassed over Rupees ten million in two years with this method. Workers intercept the mails of their employers and steal the cards. Jail Wardens, hospital employees, helpers in
old age homes steal ATM cards of their wards. If a person, in a hurry, forgets to remove the card, the workers around notice it and make use of the active account for withdrawing cash. Some even change the PIN.

(f) SOCIAL ENGINEERING

When a person poses as very responsible and makes another person believe that he could be trusted, it is a case of ‘Social Engineering’. He convinces the card owner that he is safe enough to be trusted with his ATM card and PIN code. He might impersonate as a bank officer, bank employee or a member of the police. Here are some examples to illustrate.

POISING AS BANK OFFICE:

(a) He telephones the customer and says that the bank has cancelled his defective card because of security reasons. Card holder asks for the card but at the same time volunteers to get it collected. He says the old invalid PIN has also to be cancelled before issuing a new one and obtains the PIN. An accomplice collects the card.

(b) He represents himself as an employee of the bank of the card holder holds the ATM card, canvassing for a contest exclusively for ATM card holders with huge sums as prize money. He gives them the Performa of contest, which looks genuine. Performa of contest have some mandatory fields meaning thereby those information are must for Performa to be eligible for contest and should not be left empty and mandatory field asks for filling personal identification number(PIN) and or pass words. He then wants to verify the ATM card is genuine and swipes them in his portable Skimmer and obtains data encrypted on ATM Card.

(c) Skimmer poses as a bank security officer, he brings up a client and asks for his cooperation in nabbing a dishonest employee who is trying to steal funds from his account. To execute the trap he asks him to leave his card secretly under the door of the bank after closure of the bank. Next day, he informs him that the employee has been caught red handed and thanks him and tells him that his card is required as evidence and a fresh card would be issued to him. He then collects the PIN by saying that it is needed for cancellation of the old card.
(d) A lady’s card gets stuck in an Automated teller machine by some installed skimming device. She rings up the emergency phone number given in a bogus sticker pasted on the Automated teller machine. The man on the other side, who is an accomplice of crook, identifies himself as the bank employee and offers to issue a new one in its place of sticking ATM card. For that he needs her PIN and the lady gives it. The card is retrieved later by the crooks.

POSSING AS POLICE OFFICER

(a) First he steals wallets by breaking into lockers in Social Clubs, Sports Club etc. He then rings up the card holder, identifies himself as a police officer, informs him that his card and the wallet had been found with an arrested culprit. He says it will not be returned to him, but to the bank. He says that a small formality needs to be complied with, viz., the PIN has to be recorded in the files. He gives the phone number of the Police Station (his friend’s) where he should lodge his PIN.

(b) Dressed as a senior police officer in uniform, with badges, gun etc, driving a big car with flash lights on, accosts elderly persons driving their car and, with his intimidating language checks their belongings, confiscates the Automated teller machine card and also obtains the PIN.

MISCELLANEOUS

The criminal, impersonating a senior officer of the super market, phones up a sales girl in the market and informs her that he wants to give her a huge cash incentive for her good work, but confidentially. He wants her ATM card number and PIN so that incentive could be deposited into her account without the knowledge of other employees. The girl gives them ATM card number and PIN.

(g) LEBANESE LOOPS

This was the first method used when the practice of ATM card number and PIN card capturing started. The culprit positions a thin rigid plastic strip having long wires in the sides (Lebanese Loop), deep inside the Automated teller machine slot, in which card has to be inserted. When a card is inserted, the ‘Loop ’prevents its movement and the machine stops. The culprit standing
behind him asks him to try entering the PIN twice or thrice, but nothing happens. He memorizes the PIN. After the card holder leaves, the culprit pulls out the strip with the help of the wires and the card comes out. A notice, “If for any reason your card is retained please enter your PIN number three times and then press cancel button.” is pasted on the Automated teller machine. The customer inserts the card and it is stuck. He enters the PIN three times but nothing happens. He leaves. The crook standing behind memorizes the PIN and retrieves the card. The secret is the opaque sheet of plastic placed inside to prevent the card reader unit reading the magnetic stripe.

(h) POST & COURIER

In Chennai, a customer received an SMS alert of Automated teller machine withdrawals by the ATM card even before the card was delivered to genuine account/ATM card holder. On investigation, it was found that four persons belonging to a courier company used to hand over the mails to a gang of criminals for a day, who fished out the card details and PIN and returned the mail intact. In US, a Californian postal carrier and a South Brunswick letter carrier were arrested on charges of theft of ATM cards. The interception of the bank letters by the employees in Post Offices and Couriers is a cause for serious concern.

(i) HACKING THE AUTOMATED TELLER MACHINE

In certain banks, dedicated lines are used to connect the Automated teller machine to the host computer along with a separate dial-up line to the host for the use of maintenance engineers. Stealing the confidential number for the dial up line the hacker intrudes into the Automated teller machine circuit and converts his friend’s card into a Security Card which enables him to do any fraud. According to the book “AUTOMATED TELLER MACHINE EXPOSED” published by Sailclose Publications 2003, a computer programmer in Taiwan stole 4 million dollars by making more than 7,000 cards by intercepting the communication line and obtaining data being processed by the Automated teller machine.

(j) JACKPOTTING

At the Black Hat Security Conference 2010 in Las Vegas, researcher Barnaby Jack demonstrated, on the stage, high-tech hacks against two genuine Automated teller machines.
In one, Jack reprogrammed the Automated teller machine remotely over a network; in another attack, he opened Automated teller machines’ front panel and plugged in a USB stick loaded with his own software. The large audience was shocked to see dozens of crisp bills flow out from both the Automated teller machines.

II. INSIDERS (Bank Employees)

Automated teller machine cash containers are protected by a set of confidential combinations. Only the restricted and trusted members of the staff of the bank or the service providers know them. When the Automated teller machine cash disappears mysteriously without any trace, it is rational to conclude that the combinations had been used with or without the connivance of the employees. It might have been leaked out on account of negligence or coercion. It is also possible that they were stolen. It is a cause for concern that, for the employees in the section dealing with Automated teller machine, ATM cards and PINs, opportunities exist for collecting PINs and card details. In many fraud cases, the bank employees were found to be the collaborators. Model Anupama Verma of Mumbai never uses her ATM card and had not even opened the PIN letter. Yet Rs 17.36 lakh was withdrawn from her account by using the ATM by as many as 170 times. Two employees of her bank were the culprits. Ralph Elmer of Battle Creek, Michigan never even knew that an ATM card was issued on his account but found that over $40,000 was withdrawals from their account for several years. There is a loophole in the dispatch section of the bank which sends the card and the PIN to customers. The employees were found to have changed the addresses on the envelope and diverted them to the address of a criminal. The deposit envelopes in the Automated teller machines’ deposit box were found to have been tampered with and cash removed by collectors. They were also responsible for stealing the amounts swallowed by withdrawals of account of non withdrawal. In a bank in Bahrain, an employee who handled the entire Automated teller machine operations single handed, swindled money and tried to cover up the fraud by juggling with the daily cash top-ups for the machine.

III. TECHNICIANS (ENGINEERS, SERVICE PROVIDERS)

Automated teller machine technicians and service providers like cash fillers etc., are given separate passwords for conducting the Automated teller machine operations. These passwords
are supposed to be activated only for the brief period of operation. There are instances where, due to negligence, the passwords were not deactivated, and it resulted in the disappearance of cash from Automated teller machine. In one case, an Automated teller machine repairman in New York who knew the keystrokes to change the denomination of the issue trays changed $20 tray into a $5 tray and made the bank issue $20 instead of $5.

IV. BANK CUSTOMERS

It is difficult to believe that customers are also indulging in fraudulent activities when they notice any weakness in the system. During the 9/11 disaster when the banks, for humane reasons, decided to open Automated teller machines without their normal controls, the customers stole $15 million within a few days. In the ‘Transaction Reversal’ method, the customer removes some notes in the middle of the stack when the machine delivers a stack of notes, and waits. The machine swallows the rest of the notes as unclaimed, but there would be no record of the shortage anywhere. In a recent Rupees 1 Crore fraud involving Federal Bank and other banks this method was used. The gang members used to demand a withdrawal of Rupees 10,000 from Automated teller machine of Federal Bank. Fraud collected only Rupees 9,900 and left the last hundred rupee note inside the Automated teller machine; the Automated teller machine retrieved the note and flashed a message that “transaction has failed” in the software system of the private bank whose ATM card was used for withdrawal. Their accounts never got debited. In Automated teller machines where checks are accepted as deposits, a huge number of frauds have been executed by depositing checks on accounts without balance and withdrawing cash against them.

MODIFYING THE AUTOMATED TELLER MACHINE

Chinese criminals used an unusual method. They cut the cash conveyor belt inside the Automated teller machine so that the undelivered cash falls within the machine. After the departure of the client, they removed the cash.

MISCELLANEOUS

In certain Automated teller machines, the customer has to swipe the card and then remove it. At the end, he has to hit a key to exit. If the key is not pressed, the machine waits for 60
seconds before closing. The Daily Telegraph Kolkata reported that one knew this secret and used to transact as soon as the customer left. Though he failed on most occasions, but he succeeded few times and had fetched a whopping sum of about Rs. 4 lakh.

PHISHING

Phishing technique is mostly used by hackers to obtain confidential details of bank password via email. But sometimes they collect ATM cards PINs too. The customer believes in a bogus email looking exactly like his banker’s asking for personal details, password PIN etc., He blindly complies with the request.

According to a paper published in IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.11, November 2011 By Rufai M. M., Adigun J. O. and Yekini N. A. Published various categories of Security Threats and Abuses in Automated teller machine. Threats can be seen as potential violations of security with expected or unexpected harmful results, and exist because of vulnerability in a system. If an unauthorized user invades into a system he/she can destroy information, operating systems, and programs. They can disclose information or they can cause disruptions or interruptions (damage systems, networks, organizations, institutions)[29]. Sources of threats can be classified as follows:

Physical, which include natural disasters (fire, storm, water damage) and environmental conditions (dust, moister, humidity).

Technical: This is synonymous to equipment or software failure e.g. A user apply for withdrawal in an Automated teller machine, the machine shows amount paid up but the cash is not delivered.

Human, which is the main source of communication breaches. It includes unauthorized users who wish to damage an Automated teller machine system, and authorized users who misuse the system either deliberately or accidentally. The human threats can be further categorized into internal and external. Internal human threats are disgruntled employees, hackers, former employees, system administrators, LAN and data base administrators. External human threats arise from commercial espionage, government-sanctioned espionage, vendors, manufacturers, kids looking for kicks, nosy reporters.
Theoretical, which includes the vulnerability of the algorithms, protocols, and mathematical tools used in the methods that they are implemented in the systems.

After reviewing the literature available on Automated teller machine vulnerabilities majorly we can categories various vulnerabilities in three major areas these are:

- Physical vulnerability
- Communicational Vulnerability
- Network Vulnerability

Types of Physical vulnerabilities:

- Card Skimming
- Fake Automated Teller Machine machines
- Card Trapping
- Distraction theft or ‘manual’ skimming
- Shoulder Surfing
- Leaving transaction ‘Live’
- Cash trapping
- Phishing
- PIN cash-out attacks
- Utilizing a Fake PIN pad overlay
- PIN Interception
- Ram Raid Attacks
- Theft of Automated Teller Machines
- Smash and Grab of Automated Teller Machines
Review of Literature

Safe cutting/Safe Breaking

Explosive Attacks

Types of communicational/logical vulnerabilities:

Viruses and malicious software

Less security over communication channel

Normal Encryption techniques which can be break easily

Logical/software vulnerability:

Use of computer software to steal sensitive cardholder’s information

Viruses

Malware

Types of Network Vulnerability:

Network attacks against AUTOMATED TELLER MACHINES

Weak data communication lines

2.6 REVIEW ON SECURITIES ISSUES:

Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities and causation in civil litigation and banks must meet certain standards in order to ensure a safe and secure banking environment for their customer. Customer trust is an essential component of banking services. Without trust, financial organizations and their clients may decide to forgo use of the Automated teller machine banking and revert back to traditional methods of doing banking operations. To counter this trend, the issues of Automated teller machine security at outside the bank premises and customer sites must be constantly reviewed and appropriate countermeasures devised. These security measures must be implemented so that they do not inhibit or dissuade the intended banking operation. In this part of the chapter we will discuss
some network and computer security issues related to Automated teller machine security and banking security outside the bank premises and will present some of the security concerns related to Automated teller machine.

Some security guidelines published in “INTERNATIONAL MINIMUM SECURITY GUIDELINES FOR THE AUTOMATED TELLER MACHINE INDUSTRY” by the Global AUTOMATED TELLER MACHINE SECURITY ALLIANCE in September 2004 in conjunction with GASA’s General Cyber Security manual and the white paper on a Continuous Cyber Security Process (CCSP) on operational security and operating system security as per their report Financial institutions and Automated teller machine manufacturers are replacing and upgrading aging Automatic teller machine fleets across the globe in order to satisfy regulatory and business imperatives. Regulatory requirements include the use of the Triple DES encryption algorithm, whilst business drivers include demands for increased functionality, enhanced customer experience and system integration to streamline management and monitoring. In order to satisfy these business and regulatory drivers, new platforms utilizing “mainstream” technologies are being introduced which is dramatically altering the vulnerability landscape associated with this traditionally proprietary system. The use of proprietary technologies afforded Automated teller machines a degree of defense against malware, “hacking” toolkits and utilities, denial of service attacks and other threats that have been used to exploit vulnerabilities in more prevalent operating systems and networks[30]. Most modern Automated teller machines are now running on operating systems and network communication protocols known by, and familiar to, the majority of computer users. As a result, they exist within the identical vulnerability landscape that the majority of computing systems and networks in use today experience, and are consequently exposed to many of the associated threats.

The recommendations presented in this report are essentially designed to provide a “common sense” approach to risk mitigation as a result of the rapidly changing threat model that the introduction to the Automated teller machine channel of the Windows XP and other common use operating systems, as well as the TCP/IP network protocol suite, has created. The default installation of modern operating systems includes many components, packages or clusters.
The selection of system components ultimately installed as part of an operational build can usually be made either during installation, post-installation, or both. However, as the majority of Automated teller machines are delivered with a standard operating system build, the only opportunity to remove unnecessary packages is at post-installation. Only the components necessary for the normal operation of the Automated teller machine should be installed. The decision to remove a particular package needs to be analyzed against the Automated teller machine vendor’s application requirements, and the acquirer’s management, monitoring and other operational considerations.

2.7 SECURITY FACILITIES IN THE PRESENT ATMs:

The designer of the present Automated teller machine has put in place a lot of security facilities. As good as these facilities are, it has not been able to totally solve the issue of Automated teller machine fraud. However, it is necessary we have a review of these existing security facilities. These facilities fall under different headings as follows:

PHYSICAL SECURITY

The essence of this approach is to prevent physical attack on the Automated teller machine. This is achieved in two ways:

1. Using dispenser mechanism that makes it difficult to retrieve money without proper authority.
2. Another approach is the use of dye markers and smoke canisters which prevent the theft of the money in the Automated teller machine.

TRANSACTIONAL SECRECY AND INTEGRITY

Fraud is prevented by ensuring that personal information is encrypted. Data in Automated teller machine transactions are usually encrypted with Data Encryption Standard, now the transaction processors are required the use of Triple DES.

CUSTOMER IDENTITY INTEGRITY

There have also been a number of incidents of fraud where criminals have attached fake keypads or card readers to existing machines. These have then been used to record customers’ PINs
and bank card information in order to gain unauthorized access to their accounts. Various Automated teller machine manufacturers have put in place countermeasures to protect the equipment they manufacture from these threats.

**DEVICE OPERATION INTEGRITY**

Automated teller machines that are exposed to the outside must be vandal and weather resistant. Openings on the customer-side of Automated teller machines are often covered by mechanical shutters to prevent tampering with the mechanisms when they are not in use. Alarm sensors are placed inside the Automated teller machine and in Automated teller machine servicing areas to alert their operators when doors have been opened by unauthorized personnel[31].

**2.8 ATM’S LOCKS FOR PHYSICAL SECURITY**

Automated teller machine lock is a security measure to protect the Automated teller machine from physical attacks for installed Automated teller machines where a Bank requires a Time Delay/Time Lock, the Bank’s security agency fit a lock in it accordance with the manufacturer’s requirements. It then be connected to an appropriate alarm system with monitoring via an ARC and a test made. For Automated teller machines supplied with locks which have external alarm monitoring capabilities, the lock connected to an appropriate ARC and a test made. If there is a requirement to monitor the status of a remotely monitored lock, it monitored from an appropriate ARC 24 hours daily. The ARC automatically generates an alarm signal if the telephone line fails or is cut. The ARC is able to monitor the functionality required by the Automated teller machine deployer e.g. lock open/closed, time access windows etc[32].

**DIFFERENT TYPES OF LOCKs**

The following lock types are recommended for all types of Automated teller machines:

- **Primary Safe Locking** The following locks are recommended:
  - A UL 437/Type 2, CEN Class B changeable key lock
  - A 3 wheel UL Group 2M/ CEN Class B Mechanical Combination Lock
  - A UL Type 1/ CEN Class B, 1 Time Code Electronic Combination Lock
In the event that this type of lock be used it is highly recommended that the following features should be taken into consideration:

1. Lock should support encryption technology for the codes
2. Unused lock codes should expire automatically
3. Seal code should start a security protection procedure in the event that the previous Automated teller machine closing has not been correctly affected
4. Lock should be able to provide Shared access between the Bank and the CIT company autonomously and simultaneously
5. That the owner of the lock can at any time be able cancel access to the Automated teller machine lock park without having to organize on site vendor meets

A UL Type 1/ CEN Class B Electronic Combination Lock If applicable, the electronic locks should be compatible with the monitoring/control system used by the Bank/Automated teller machine deployer [33].

Secondary Safe Locking (For dual control if required) Where a mechanical 3-wheel combination lock is already in use, for the purposes of dual control an additional changeable key lock may be installed as a secondary lock to the primary. (A key locking dial may not be acceptable, dependent upon the agreed insured value for loss). Many modern electronic combination locks have a dual control function that allows dual control without the necessity to fit a second lock.

One Time Combination Locks (For Use With Approved Third Parties if required) An approved third party is a commercial organization authorized to carry cash in transit, to conduct cash replenishments and/or to conduct first & second line maintenance of the Automated teller machine. When such parties are used, it is recommended that one-time combination locks, with clearly identifiable audit trails, be used. Such locks may be used as the Primary Safe lock.

**TIME DELAY/TIME LOCKS**

When required a programmable time delay lock may be fitted, allowing a pre-set delay whenever the lock is opened. This is usually 1-99 minutes in 1 minute increments Such a Lock, which
Review of Literature

may also be used as the Primary Safe Lock, may also be programmed as a Time Lock, whenever the Bank Branch/Automated teller machine Site is closed, and between replenishments.

**TIME DELAY OVERRIDE (TDO)**

In the event that a Multiple/Dual User Electronic Lock is fitted, it should be able to be programmed with a Time Delay Override Code (TDO) that can be used by the CIT or ISO to allow the user to bypass the time delay for obvious reasons. The TDO should be able to be programmed to either allow direct after hours entry or Dual entry (second code needing to be entered within 60 seconds of the first).

**2.9 ALARMS FOR ATMs**

**DURESS ALARM (HOLD UP ALARM)**

The electronic lock should also be able to generate a “Duress” alarm. It is advisable that this code be easy to remember and use and not require any additional keystroke to activate. The best is 1 code up 1 code down activation; meaning if the code was 123456# the user would substitute the last digit by either a number above or below that of the last digit [34][35].

**BPI (BOLT POSITION INDICATOR)**

Electronic locks should also be able to provide a dry signal indicating if the bolt is in the Retracted position (open) or the Extended (Closed) position. This signal can be used to monitor the condition of the lock remotely, prevent a cascade (multiple door openings at the same time) attack on a group of Automated teller machines or freeze the entry to the Automated teller machine room in the event that an Automated teller machine door is in the open condition. Alternatively there are many safe alarm systems in operation that monitor bolt position by other add-on means and these are acceptable and even compulsory alternatives in some countries.

**ALARM SYSTEM FOR AUTOMATED TELLER MACHINE**

Considering the alarming of the premises with addition of consideration should be given to alarming the Automated teller machine itself. This can be achieved by means of a stand-alone
alarm system with its own unique reference number (URN), or may be a separate area of the premises alarm system[36]. This will be jointly determined by the site host and deployed (who, in some circumstances, will be the same organization):

The system should be monitored by remote signaling to an ARC and should qualify for an appropriate local police response.

If it is a “confirmable” alarm system a dual signaling facility should be provided. The design should ensure that the system is armed at all times other than for maintenance, for servicing and cash replenishment.

It should give the earliest possible warning of attack on the Automated teller machine

Consideration should be given to including personal attack alarms for the use of CIT crews / replenishment staff in the event of an attack during cash replenishment.

A maintenance record should be kept for the alarm detection system and routine maintenance should be conducted. The minimum should be one planned maintenance visit each year (dependent upon the grade of system installed).

**ALARM EQUIPMENT**

The following alarm equipment is recommended for installation at each Automated teller machine location:

**Seismic Detector / Stress Detector:**

A seismic / stress detector should be fitted to the Automated teller machine safe body and safe door.

**MAGNETIC CONTACT:**

A dual read magnetic contact switch should be fitted to the door of the Automated teller machine Safe. A dual read magnetic contact should also be fitted on the door of the Automated teller machine Secure Service Room (if provided). This should be on a different circuit to the alarms fitted to the Automated teller machine safe.
VOLUMETRIC DETECTOR:

A volumetric detector should be placed on the wall of the Automated teller machine Secure Service Room. This should be able to detect any movement in the area surrounding the Automated teller machine. This should be on a different circuit to the alarms fitted to the Automated teller machine safe. If the Bank Branch has a cellar, which is under its direct control, a volumetric detector should be fitted to cover the area underneath the Automated teller machine anchoring. Personal Attack Alarms should be fitted in the Automated teller machine Secure Service Room as close as possible to the Automated teller machine. This is to provide protection to staff servicing or replenishing the Automated teller machine. If Automated teller machines’ are in a public area, then consideration should be given to installing a radio based Personal Attack Alarm, such that staff can be issued with portable devices.

ALARM CONTROL PANEL(S):

An alarm control panel (combination) should be fitted in the immediate vicinity of the Automated teller machine where necessary. If access control is used to secure the room, then an additional panel does not need to be fitted at the room door. Access Control Where possible, access to the rear of the Automated teller machine should be restricted and a door swipe or keypad system should be used to control the Automated teller machines’ Secure Service Room door.

HEAT SENSOR:

A heat/smoke sensor should be fitted inside the Automated teller machine. This should detect any form of oxy-acetyl.

VIBRATION SENSOR:

A vibration sensor should be fitted inside the Automated teller machine. This should detect any form of tempering with safe cutting and activate the alarm so that we can protect the tempering with Automated teller machine

AUTOMATED TELLER MACHINE SAFETY STANDARDS FOR PHYSICAL / HARDWARE SECURITY

There are number of existing standards against which Automated teller machine Safes can be evaluated. These standards comprise the following:
American Underwriting Laboratories UL291 Level 1 and Level 2 Standards,

French RMET15 and RMET30 levels, CS, C1, C2 levels

Nordic Standard INSTA 612

German RAL626/3 Standard

Automated teller machine safes which comply with these standards require different levels of resistance against hand tools, electric tools, and thermal tools. The INSTA Standard also requires resistance against explosive attack.

CEN produced and published a standard EN 1143-1 which includes the performance testing of Automated Teller Machine safes. Consequently Automated teller machine producers in Europe include a safe tested and certified to the appropriate part of EN 1143.

Many existing Automated Teller Machines incorporate a safe in accordance with the requirement of the American Underwriters Laboratories UL291 Standard Level 1. This requires that an Automated teller machine safe resists attack by common hand tools only. The standard also requires that the safe be constructed of 1» mild steel plate to body and door or of a material giving equivalent protection to 1» mild steel plate. Underwriters Laboratories have accepted that ½» high tensile steel plate will accord with this requirement and a number of Automated teller machine safes have been manufactured of such material. This UL291 Level 1 Standard provides little protection against force attack such as wedging of the door or an attack on the door or body using angle grinders and no protection against explosive or attack by oxygen cutting equipment. UL291 provides a lower burglary resistance than the lowest grade defined in EN 1143-1.

2.10 NETWORK OR COMMUNICATIONAL SECURITY

There are few communicational securities found in our literature study on Automated teller machine security. These are mentioned here in this section.

Automated teller machines are normally connects to Host systems via dedicated network segments that are not shared by general purpose servers and workstations. There are several
points along the communication path connecting the Automated teller machine with the host system that would permit the introduction of firewall enforcement points depending on the network topology. Access from within the general network to the Automated teller machine network should be controlled by the use of an enterprise “statefull” firewall. In situations where network architecture does not permit the use or introduction of a single (or several) firewall enforcement points on the internal network due to technical or business limitations, packet filters should be configured on the “next hop” perimeter router that provides TCP/IP connectivity to the Automated teller machine. Where Automated teller machines share network infrastructure (e.g. remote Automated teller machines on Branch networks), border router access control lists should be used to restrict access to the Automated teller machine from within the branch network if the traffic is passed through a suitable router. In environments where an Automated teller machine shares a VLAN with other branch traffic, the use of layer two (in TCP/IP terminology) controls, such as switch port security and static ARP mapping, should be employed to restrict intra-LAN access violations. Unused switch ports should be disabled until required for the addition of devices onto the network.

Network HUBS should not be used due to the ability to capture network traffic and the lack of security features they provide. Some Automated teller machines are being shipped with firewall capability either bundled with a 3rd party product, or as part of the actual operating system, and this should be enabled and configured irrespective of the extent of additional network enforcement points present or intended on the network.

2.11 INTRUSION DETECTION FOR COMMUNICATIONAL SECURITY

The Automated teller machine network access point into the central processing host systems should deploy one or more (depending on topology) network intrusion detection systems (NIDS). The NID(S) must be supported by appropriate management, monitoring and incident response policies and procedures.

MALWARE PROTECTION AGAINST COMMUNICATIONAL ATTACKS

If the Automated teller machine supports it, malware safeguard should be installed. Careful analysis of the product, signature file update management, engine update management, periodic scan invocation and status changes/alert notification needs to be undertaken.
Signature and Engine Updates should be applied to a control/test group as soon as possible after release by the software vendor. System stability should then be confirmed prior to the deployment of the update to the production systems.

Malware Scans Periodic system scans have the potential to cause degraded performance, and should be conducted when the Automated teller machine is out of service. The frequency of the scans should be determined based on Automated teller machine service level agreements, business requirements and additional security controls employed (e.g. firewalls, intrusion detection).

BIOMETRIC SECURITY:

An approach based on these publications that are pursued at the BSI is not to store the biometric template together with identity information gathered during enrolment itself, but a public data record as reference data. This data record allows both identification and verification of an individual if, and only if, the requestor proves his knowledge of the original template. Without proof no information can be derived from the public record and thus it cannot be used for fraudulent authorization. In particular, the data stored for identification or verification does not allow the recovery of the corresponding biometric data. This property minimizes the risk of unauthorized access to biometric data and can thus help to soothe common resentments against biometric authentication. This approach is conceptually very similar to password authentication systems that store only the hash values of the passwords from which it is computationally hard to draw conclusions about the original password. The hash value does not allow the recovery of the corresponding password without exhaustive search but still provides means to verify the correctness of the password presented during authentication. However, the transfer of this approach to biometric authentication is not straightforward because biometric measurements are inherently prone to errors, which are not tolerated by cryptographic hash functions. Therefore, the biometric authentication systems must be based on an error-tolerant authentication scheme. The error-correcting methods remove noise in the template. It is fundamentally impossible to avoid noise during biometric data acquisition, because “life means change”. For example, faces age and iris patterns are not perfectly invariant to a contraction of a pupil. More noise is introduced by changes in the environmental conditions, which is again an unavoidable
circumstance. Finally noise often finds its way into the sensor, during transmission or in the data processing process (“algorithmic noise”). The latter noise sources can be reduced or even removed by improved engineering.

Using the Biometric security systems we can improve the Auto teller machine security by attaching a physical property of a user to the system that allows the machine to access. A biometric characteristic is a general term used to describe a measurable physiological and/or behavioral characteristic that can be used for automated recognition. In this type of security we can use the user’s fingerprint to identify the authenticity of user, which is authenticated beside a stored template in the system. It add an additional feature to authenticate and are therefore a significant improvement in Automated teller machine security. The most common biometric security systems uses fingerprints, but these systems can also be uses other biometric attributes like fingerprint, face, iris, voice, signature, vein pattern, and hand geometry and facial recognition technology.

Biometric systems are commonly used to control access to physical assets like buildings, cash from Automated teller machine, laboratories, personal computer accounts, secure electronic documents, etc. Now a biometric systems has been used by Indian government to making AADHAR card for a unique identification to every individuals above 5 years of age and biometric information may used in various identifications.

Some of the biometric identification methods are as follows:

Fingerprint Identification – fingerprints structure is remain same during the whole life of a person and no two fingerprints are same.

Face Recognition – This is a new methods as it can be done without the person being aware that they are being scanned. This system analyzes specific features that everyone’s face has like the distance between the eyes, position of cheekbones, width of the nose etc.

Retina Scan – There is just no known way to replicate a retina and, as far as is known, the pattern of the blood vessels at the back of the eye is totally unique and never changes. The downside is that it takes about 15 seconds of careful concentration to do a good scan but this still remains a standard one in military and government installations.

Iris Scan – This is also very difficult to find the duplicate and stays the same for the whole life.
2.12 BIOMETRIC AUTHENTICATION IN THE CONTEXT OF ATMs:

While authentications of ATM card users on his bio-metric parameters still needs to be introduced in India, but it is use in some of the countries facing larger amounts of fraud through Automated teller machine. There were some experimental testing made scenarios in connection with Automated teller machines at the end of the 20th century (e.g. Dresdner Bank, Bank United of Texas). In recent years the banking organizations all over the world are desirous of implementing new “Chip card and PIN authentication schemes” in Automated teller machines in order to reduce ATM card fraud and costs of fraud. News have been published of security threats faced by about 40 Japanese banks, who have introduced biometric palm vein authentication technologies in about 19000 functional Automated teller machines. The vein is an externally invisible biometric feature and, therefore, difficult to copy. There are also projects in Brazil and in Austria related to introductions of biometric parameters for safe transactions at Automated teller machines. In Europe, the banking transaction of an automated teller machine is sent to the computer centre of the card issuing bank and there the customer authentication is performed centrally on main frame computers/servers. Therefore, in this case, it is essential that banks maintain biometric templates in a central database of its customers and it is recommended to keep such data protected and inaccessible from alteration or modification to prevent fraud. Especially, the method of protecting biometric templates by error-correcting and cryptographic methods could be practiced, as described in the following text.

The values of false acceptance rate by Automated teller machine in vein based biometric solutions, as published by banks are 0.00008% and 0.0001 %. Therefore, even for vein based biometrics has some problem and therefore is advisable to combine the biometric method with the traditional PIN method i.e card readers to enhance the security measures and to utilize it for further reducing vulnerability of Automated teller machine. This mechanism adopted shall ensure three stage security solution; ensuring users provide something they ‘own’ (the card), something they ‘know’ (the pin) and something they ‘are’ are themselves i.e. the personal biometric parameters before the transaction is processed’.

Major challenge for the future shall be to create upgraded international standards for personal identification schemes which shall also include biometric authentication technologies so as to
guarantee interoperability between different banking organizations of the country as well as other countries. Approach should to generalize of the existing standards of a bank to match with international banking standards combining with the biometric template protection approach.

The banking industry with use of ATM cards actually supports many different techniques’ of PIN generation methods and verifying procedures on different formats. The VISA PVV PIN Algorithm system supports a non-secret PIN Verification Value (PVV), where a generalization of the PIN procedure is done in the following the introductions of biometric technologies. The major aim for generalization is to permit the introduction of biometric technology with minimal changes in the actual standards and hardware implementations of Automated teller machine.

According to the scheme designed by Jules and Wattenberg, in a banking ATM card personalization centre there is a random codeword, i.e. \( c = G(s) \) for a randoms \( s \in GF(q)^k \), is bitwise added (XOR) to the biometric template \( f \) of the an ATM cardholder during enrolment which result in stored on the banking ATM card as \( y = c \oplus f \). Then the secret value of \( s \) is hashed with cryptographic hash function to obtain \( H(s) \). After generating a secret PIN for ATM cards, the hash value \( H(s) \) is used as new input parameter to produce a non-secret PIN verification value PVV in generalized way, and thereby combines conventional PIN procedures with biometric technologies for adding biometric values. The biometric data is introduced as one non-secret parameter on ATM card. The parameter “data_array-Reserved-2” and “data_array-Reserved-3” of the API “Clear PIN Generate Alternative” may be used for this purpose[37]. When a customer uses an Automated teller machine, he has to enter his secret PIN to the Automated teller machine and at the same time Automated teller machine extracts biometric feature of the customer generating a temporary biometric template. In the banking ATM card this biometric template \( f^* \), presented by the customer, is added to the value \( y \) stored in the banking ATM card of the customer. The result is \( f^* \oplus y = f^* \oplus c \oplus f \). Since system is working with an error correcting code, the corresponding decode function produces a value \( s^* \). If the hamming distance between \( f^* \) and \( f \) is almost \( t \), then \( s^* = s \), otherwise not. After hash has received value \( s^* \), \( H(s^*) \) is integrated into the banking transaction together with the encrypted PIN on Automated teller machine. The banking transactions are encrypted and sent to the bank central authorization centre. It is in the banking authorization centre that the transactions are decrypted[38].
The Automated teller machines encrypted PIN and the hash value $H(s^*)$ are extracted together with other parameters, the PVV, the account number, and are used as input parameters for the PIN verification procedure of the ATM card. A generalized PIN verification procedure generates a new PVV-value $PVV^*$, corresponding to the supplied PIN by the customer, for generating account information, hash value $H(s^*)$ and other parameters and compares it with the input-PVV available with central authorization center of the bank. If the $PVV^* = PVV$, the user is authenticated, the customers are allowed to move ahead for further communicating with Automated teller machine for carrying out further banking business. If the $PVV^* = PVV$ do not match i.e. authentication has failed, Automated teller machine allows the customer for retry but such attempt of retry is limited by a small value in order to prevent brute force attacks[39][40].

The retry for authentications of genuine customer may arise many times as the stored data of customer with bank might have taken by an angle which is different that the angle in which the customer might have producers before the biometric data receiver of the Automated teller machine. Since biometric data are subject to correct angles and postures of a human being, it is essential for the users to give biometric information with fully aware of posture and inclinations at the time these data are recorded for storing by bank and every time the customer uses the Automated teller machine biometric parameters to avoid rejections by the Automated teller machines.

Here we have mentioned few vulnerabilities types discovered by various researchers and their related security issues which will help us to identify new vulnerabilities and related security concerns and help us to frame new security solutions during this research.