4.1 ATMs SECURITY ISSUES

The security and vulnerability are opposite sides of the same coin, an Automated machine becomes vulnerable due to weakness of its security. Automated teller machine manufactures go on adding and strengthening security features of Automated teller machine so that customer can carry banking transactions hassle free and without any fear of siphoning of amount from their account and the same frauds works with similar speed to crack the innovated security feature so that they can have access over the Automated teller machine to exploit the accounts of bank customers.

Today banking system is changing and innovating for quick and safe transactions at minimum cost and the banking sector is in no way left behind from the other industries. Automated teller machine is one of such vital instrument for the banking sector to remain in competition, which provides facility to customer to carry their banking operations not only beyond the bank premises and banking hours but also to transact anywhere in the world that too in local currency, where the clients makes the transactions. Banks started Automated teller machine as self-service terminals to primarily withdraw money. Main objective of Automated teller machine was to supply higher service to the shoppers and lower the banks value. Automated teller machine elements cut back per unit transaction cost, supports innovation, produce new service
opportunities and increase flexibility and quality levels of product and services. At the same
time however, financial institutions and their Automated teller machine are becoming more
vulnerable to similar security-related attacks as known from the regular computing environment.
This can be particularly of concern in an exceedingly ever-changing context wherever Automated
teller machines were owned by monetary establishments and put in their premises, in the main
on bank branch facilities, to a replacement reality wherever a lot of of and a lot of Automated
teller machines are a unit placed off-premises and Automated teller machine acquirer networks
area unit a lot of typically owned and controlled by freelance Automated teller machine operators.

Automated teller machine crime has become a worldwide issue that faces not solely customers,
however conjointly bank operators. Security measures at banks will play an essential, conducive
role in preventing attacks on customers. These measures are essential importance once
considering vulnerabilities and faith in civil proceedings and banks should meet bound standards
so as to make sure safe and secure banking surroundings for his or her customers.

Automated teller machine security problems and Automated teller machine fraud problems
typically follow some distinct patterns based mostly upon the situation of the Automated teller
machine security attacks or Automated teller machine fraud incidents. Automated teller machine
fraud problems within the most half involve MasterCard fraud and open-end credit fraud.

During the first to middle 1970’s, the primary recognizably trendy Automated teller machine
were put in within the United Kingdom of Great Britain and Northern Ireland and overseas.
The magnetic strip card was introduced at this point, and card standards were united through
the American Bankers’ Association that area unit still in effective these days.

Because of the issues encountered with ATM card forgers, banks tried to cipher the PIN on
the cardboard, or derive it from the account range, or offer another suggests that of checking
it, in an exceedingly means that they hoped wouldn’t be too obvious to criminals and hackers.
In fact, if one has got a Barclaycard or Barclay charge card that dates back a couple of decades, to detect that the primary and fourth digits of your PIN add up to an equivalent because the second and third, or that the primary and third add up to an equivalent because the second and fourth.

However this kind of security wasn’t abundant sensible against a bright forger, and this brings United States to the second contribution that Automated teller machine created to laptop science and thus fostered industrial development of cryptography, that is that the study of codes and ciphers.

Automated teller machine security attacks involving physical attacks against the Automated teller machine security enclosure area unit wide unfold. Automated teller machine explosive attacks is today very Europe, Australia and African countries. The study on the trends of attacks on Automated teller machine in various regions shall be taken separately.

Automated teller machine ram raid incidents conjointly occur globally however area unit most rife within the United States may be partially thanks to the biggest range of Automated teller machines deployed in soft-target locations like convenience stores.

Today’s Automated teller machines have become pretty vulnerable. Several of them use in operation systems like Microsoft Windows. Around majority of security incidents occur on Windows systems and use IP networks as their communication mechanism. This exposes the system to high security risks thanks to the abundant vulnerability in open systems of this sort, and that they are liable to malware infection.

There ought to be a necessity of some dominant system that ought to customize for monetary self-service systems, enabling a centralized check to be unbroken of that applications are a unit run on the system, that native or remote resources area unit accessed and that different
system area unit communicated with. By suggesting that of this sort of management package ensures a high security Automated teller machine surroundings isolating at supply any infection by viruses, Trojan horses, worms or different malware, whereas conjointly preventing any malicious package from being entered or run with access to sensitive Automated teller machines resources.

Every Automated teller machines during which this sort of package fitted has an Access management List (ACL) giving an associate degree complete definition of the processes, system resources (files and libraries) and permissible communications. The other part not showing on this list ought to be mechanically blocked.

Automated teller machines security provided by the banks to safeguard the Automated teller machine. The major security risks of Automated teller machines can be grouped broadly in four divisions:

I. Physical Security

II. Software/Package Security

III. Logical Security

IV. Communication Security

4.2 PHYSICAL SECURITY:

Automated teller machines is almost a direct currency dispenser terminal permitting the client to directly get the money, however a while thanks to lack of security in some way or the other, some unauthorized user or hackers or criminals take an opportunity to tamper the machine and steal the money by physical attacks on Automated teller machines and by tampering with the machine, cutting the safe, bombing, shoulder surfing, ram riding are the other common abuse of
Automated teller machines by the frauds. There are several criminal attacks on Automated
teller machines involving hold-up, removal of Automated teller machines from its premises by
force, or by assault to the Automated teller machines within the premises with safe-breaking
instrumentally or by explosives. In the majority of attempts of attacks, the criminal has gained
success of varying degree. To safeguard from this sort of frauds some security features are
being added/created for Automated teller machines from time to time but these security features
gets holed by the criminals.

LOCKS FOR ENTRY IN ATM KIOSKS

The first security feature a customer comes across before operating an Automated teller machine
is digital lock at the entrance of Automated teller machine housing or kiosks. The door allows
the customer to open the door only after inserting ATM card into designated slot. However
these doors do not require card to insert while leaving the Automated teller machine kiosks as
door can be opened by pulling inside. Though these features have been added to restrict
unauthorized person from entering the Automated teller machine kiosks, but importance in
imparting security to the machine is limited as an wanted guest can always enter through
Automated teller machine kiosks door in time gap of closing the door of a genuine ATM card
holder or may enter while a client is leaving the Automated teller machines after completing his
transactions. Normally there are more than one Automated teller machine installed in an
Automated teller machine kiosk and thereby numbers of both genuine and fake customer may
be found at any moment in Automated teller machine kiosks. Presence of large number person
inside kiosks enhances physical security threat to the Automated teller machines.
The door locks of Automated teller machine kiosks having one or more machine have been considered to allow only genuine ATM card holders entry into the kiosks, the digital locks cannot restrict the entry by use of fake/cloned ATM cards. These door digital locks are also misused some times by frauds by installing card reader device which can send the details of ATM cards inserted in it.

**EXTORTIONS INSIDE ATM KIOSKS.**

Wayside cheaters and gangster used to loot money from victims at deserted/isolated places by nabbing the passerby, with introduction of Automated teller machine, they did find small money or no money from the victims. Since they noticed that invariably all the victims had ATM cards
with them, they added the practice of forced withdrawal from the victims from ATM cards. Gangster either wait in Automated teller machine kiosks for the victim as if they are waiting to withdraw the money or nab a victim at deserted place and bring the victims to Automated teller machine kiosks and force the victim at knife point or gunpoint to use his ATM card and withdraw the money from the Automated teller machine using ATM card and his PIN number.

PHYSICAL SECURITY THREATS TO ATMs

Initially Automated teller machine were introduced by the banks and its transactions were limited to the same bank by connecting through computer system of the bank having account details of its customer and therefore it was not placed at much distant from the bank. But with sharing of transactions on Automated teller machine by host of bank apart from the bank to
whom Automated teller machine belongs has led to situation where Automated teller machines are being at any place which is convenient to its customer/clients. Installation of kiosks in Mall/shoping centre have become common apart from other places such busy market intersections, hospitals, railway stations, bus stands, air port and a host of other places where the bank thinks that Automated teller machine shall be able to fetch good business. The Automated teller machine installed within closed area of a bank or shops/mall are almost secure from the point that thieves or frauds cannot operate in crowded place and where otherwise also security arrangement exits on regular basis and therefore can be rated as highly secured Automated teller machines.

The Automated teller machines installed within the premises of bank or Shopping Mall can be categorized in the security zone next the Automated teller machines placed within banks/Shopping Mall, as it has be looked after the agencies entrusted for the security of the bank/shoping mall. The figure 4.3 is an illustration of an Automated teller machine placed by a bank within its premises but outside its banking area.

![Figure 4.3 ATM in bank premises](image-url)
The Automated teller machine installed in kiosks to cater the demand of clients by being placed on the spot highly frequented by the clients/users but isolated place are prone to its misuse by thieves for forced transactions. These Automated teller itself can be disengaged from its place of installations and carried way to convenient place for break opening of its money chest as illustrated below:

![Decamping of ATM](image)

**Figure 4.4 Decamping of ATM**

The concentrate of this approach is to stop physical attack on the Automated teller machines can be achieved in 2 ways that

a. By victimization dispenser mechanism that creates it troublesome to retrieve cash while not correct authority.

b. The second way is to use of dye markers and smoke canisters that stop the employment of the money within the machine by a thief.
HARDWARE SECURITY FOR MANUFACTURER:

There are a unit some standard area unit developed by totally different nations against that Automated teller machines will be factory-made with interference of physical attacks.

These standards are a unit as follows:

- American Underwriting Laboratories UL291 Level one and Level a pair of Standards,
- French RMET15 and RMET30 levels, CS, C1, C2 levels
- Nordic customary INSTA 612
- German RAL626/3 customary

Automated teller machines safes that go with these standards need totally different levels of resistance against hand tools, electrical tools, and thermal tools. The INSTA customary conjointly needs resistance against explosive attack.

UL291 CUSTOMARY FOR ATM SECURITY:

Most of the Automated teller machines have unit of 2 forms of safes or security cupboards for securing cash. One sort of Automated teller machines safe is that the Business Hours (BH) safe and also the different the twenty four Hours Level one safe. Each safes have to be compelled to meet the UL 291 security customary designed by Underwriters Laboratories, associate degree freelance product-safety testing company. This customary needs that the Automated teller machines manufacturer must supply a degree of protection against unauthorized removal of currency and also the removal or manipulation of dealing records[53]. In different words, Automated teller machines with either sort of safe should stand up to attacks from somebody attempting to rob cash or amendment the dealing records. Each sort of Automated teller machines safes must be able standby in environmental and endurance needs.
ATMs SECURITIES

(i) BUSINESS HOURS ATM MACHINE

An Automated teller machines with a Business Hours safe is meant to store money solely throughout business hours under the watchful eye of an accountable owner, manager, or worker. The money hold on during this sort of safe ought to be removed at the shot of the business day. The metal of the Business Hours Automated teller machines should stand up to a physical attack from a stealer armed with wires, lines, chisels, pry bars, or wrenches for a minimum of 5 minutes. This provides enough time for the shop owner, manager, or worker to make a decision and call the police. Business-hour Automated teller machines must meet the UL 291 standards and Automated teller machines should typically weigh around one hundred twenty five metric weight unit.

(ii) TWENTY FOUR HOURS LEVELS ATM MACHINE

Automated teller machines with Level one have one safe unit designed to be used twenty four hours every day and should weigh around 250 metric weight units and may hold money unattended. The steel of the one safe should withstand physical pressure of fifty thousand psi. This sort of Automated teller machines are meant to face up to higher degree of attack, victimization fishing, trapping, and forcing techniques, on the currency instrumentality from the client access panel for least half-hour. Attacks on different parts of the safe, victimization picks and moveable electrical tools like drills and grinders will be resisted by this sort of safe for up to fifteen minutes. All of our Automated teller machines models have the Automated teller machines safe is separated from the client access panel space, that is an additional security feature that creates Automated teller machines fraud and theft that far more troublesome and difficult.
(B) ENVIRONMENTAL NEEDS

All Automated teller machines have to be compelled to stand up to eighty-five percent humidity for twenty-four hours. This ensures that each one of Automated teller machine maintains records and also the quality of the currency within the automatic teller machine. Several existing Automated teller machines incorporate a security to meet the guidelines as laid down by the American Underwriters Laboratories UL291 customary Level one. This needs that associate degree Automated teller machines safe resists attack by common hand tools solely. The quality conjointly needs that the safe be made of 1» steel plate to the body and door or of a cloth giving equivalent protection to 1» steel plate. Underwriters Laboratories have accepted that ½» high tensile plate which can accord with this demand and variety of Automated teller machines safes is factory-made of such material. However UL291 Level one customary does not provide full protection against force attack like wedging of the door or associate degree attack on the door or body victimization angle grinders and no protection against explosive or attack by element cutting instrumentality.

(C) MECHANICAL/COMBINATIONAL LOCKS FOR PHYSICAL SECURITY:

To protect the Automated teller machines from physical attacks, mechanical or combination locks are a unit used wherever in their area unit 2 sets of mechanical locks and Automated teller machines opens only if each the lock opened properly with 2 separate keys i.e. there is a mixture of 2 locks control to open the money container with this sort of lock. It stops the Automated teller machines from in house worker attacks if any banking official will perform a fraud it stop the system.

(D) TIME/TIME DELAY LOCK:

Lock providing time protection associate degree/or time delay facilities can enhance the protection of an Automated teller machines safe by providing a deterrent to hold-up.
(E) CLOSED CIRCUIT TV (CCTV):

Strategically sited cameras will offer continuing police investigation (locally or from an overseas observation Centre) of the approaches to the Automated teller machines. They conjointly offer a helpful visual deterrent. Recorder employed in conjunction with the cameras will record events endlessly or once activated by movement detectors. All national legislation regarding the employment of CCTV ought to be discovered.

(F) ATM CLADDING

Reinforcement panels will be fitted to hide the door associate degrees one or a lot of body sites of an Automated teller machines safe to extend resistance to physical attack. The panels conjointly defend the present protection system which might be increased by upgraded blot work, strap work and hinge protection.

(G) LINE UPS

To prevent customers from shoulder surfboarding banks create barricades before the Automated teller machines to outline the road up positions for users and restricting the side view of person standing behind the actual user of the Automated teller machine. This shall prevent shoulder surfboarding to a greater extent. Below is that the image shows the road up distance users to safeguard the user input data.

Figure 4.5 line ups for physical security
In new generations of Automated teller machines, to combat and minimize the Automated teller machines from physical attacks like cutting, fire, tempering etc. sensor are fitted. New series of Automated teller machines are equipped with heat detector, vibrating detector and tampering detector, which are designed to defend the Automated teller machines from external attacks and forestall the Automated teller machines from being taken to outside Automated teller machines premises.

**HEAT SENSOR**

New Automated teller machines unit are assembled with a heat detector, if an associate degree offender attempt to create a hearth to achieve the money from ATM and lift the fireplace is cabin than heat detector activate and ring an alarm for that and start hearth fighting system on.

**VIBRATION SENSOR**

Similar to heat detector, vibration sensor area unit currently conjointly fixed either within the Automated teller machine or premises housing Automated teller machine. Vibration alarm activates once somebody attempt to cut causing vibration in the Automated teller machine and its premises for taking appropriate actions to defend the Automated teller machine from cutting and forestall the Automated teller machine from any sort of tampering with the machine.

The vibration detectors are used in the Automated teller machine, which contains sophisticated signal process analyzer (EVD –Explosion Vibration Detector and mechanical device unleash mechanism housed among a sturdy steel enclosure. This mix offers are refined to attack detection of associate degrees by controlled access to the protected unit by an authorized user.
The above figure 4.6 shows the ATM and its companion magnet hasp, the latter is fitted to the forefront of the door. Once the door is closed the magnet is hidden below the lid of the Automated teller machine and door standing will be monitored. To permit access to the safe, a low-tension DC offer is applied to the Automated teller machine – indicated by an inexperienced junction rectifier. The licensed user presses the discharge switch and also the lid of the ATM will be opened (limited travel) thereby releasing the magnet and permitting the safe door to be opened. Additionally to twin anti-tamper protection (single output), the ATM offers variety of further outputs:

**VIBRATION.** Attack by means of grinding, hammering, drilling, or thermal cutting device can trigger the VIB output.

**IMPACT.** Explosives, a series of consistent strikes or makes an attempt at ram-raider can activate the IMP output instantly.
TILT. Any decide to move the protected instrumentality can activate the lean output. Additionally, high-energy attacks like ATM ram-raid also will trigger this output.

DOOR. A voltage-free contact that reports the state of the safe door.

SLIDE. A voltage-free contact indicating if the Automated teller machine cowl is opened/closed.

The principle to operate vibration alarm system of the Automated teller machine is signal processing and analysis of the assorted on-board sensors then to require acceptable action within the event of a legitimate attack. Additionally, this unit features a range of dedicated inputs that support remote sensors that enhance and extend the world of coverage.

**VIBRATION SENSOR**

Alarm system based on vibration sensor is based on sensing increase in vibration level which might would have occurred due equipments deployed for forced removal of the Automated teller machine or attempt to damage the safe of the Automated teller machine to loot the cash kept in Automated teller machine. Any attempt to harm the Automated teller machine physically by any mechanical means shall generate vibration much above the normal level of noise in Automated teller machine kiosks and it this increase in level of vibration which is needed to be sensed for raising the alarm and activating the alarm at police control room and the bank office.

A vibration sensor called Shear mode accelerometer designs feature on sensing crystals attached between a centre post and a seismic mass. A compression ring or studs are applied as pre-load force to the element assembly to insure a rigid structure and linear behaviour. Under acceleration, the mass causes a shear stress to be applied to the sensing crystals. This stress results in a proportional electrical output by the piezoelectric material. The output is collected by electrodes and transmitted by lightweight lead wires to either the built-in signal conditioning circuitry of ICP sensors, or directly to the electrical connector for charge mode types.
The sensing crystals are isolated from the base and housing. Shear mode accelerometers rejects thermal transient and base-bending effects to a larger extent.

The shear geometry allows itself to lend to small size to promote high frequency in the response while minimizing mass loading effects on the test structure. With combination of ideal characteristics, shear mode accelerometers normally offer optimum performance to meet the requirement.

**SELECTION OF AN ACCELEROMETER :**

Selection of the best accelerometer for specific predictive maintenance application is difficult, even for the most seasoned of engineers/technicians. Typically, the process the best suited accelerometer can be chosen by examining or filtered down to a series of qualifying questions related to actual requirement for a particular purpose, in this case to have scope to defend the Automated teller machine from burglar who is attempting to cut the Automated teller machine from its installation for breaking upon its chest to decamp with money stashed inside i.e.
accelerometer needs to be activated when the sound level increases in an Automated teller machine from its normal working level to noise of cutting the metal plates by metal cutter or electric cutter or gas cutters as noise level of these cutting device is much higher than the normal level for generalized Automated teller machine operation for conducting financial transactions.

This might seem obvious at first in selecting accelerometer is the step to actual vibration present in an Automated teller machine by measuring and also measuring the level of vibration while dislodging an Automated teller machine from its pedestals i.e. determining the goals. Vibration can be monitored with accelerometers that provide raw vibration data or transmitters that provide the calculated overall root mean square (RMS) vibration. Analysts find raw vibration readings to be useful because they contain all the information in the vibration signal. The true peak amplitudes and vibration frequencies may be available. The overall RMS or peak values are useful in control systems such as PLC, DCS, SCADA and PI because of their continuous 4-20mA signal and some applications use both. By determining signal variety is required for the application significantly narrows the search of equipment required. Vibration has to be measured in terms of acceleration, velocity or displacement. Some industrial sensors measure variation in temperature along with vibration. Finally, some applications, such as vertical pumps, are best monitored in more than one vibration axis in which case does the application require single, biaxial or triaxial measurement. There are two main differences between low-cost and precision accelerometers. First, precision units typically receive a full calibration, that is, the sensitivity response is plotted with respect to the usable frequency range. Low cost accelerometers receive a single-point calibration and the sensitivity is shown only at a single frequency. Second, precision accelerometers have tighter tolerances on some specifications such as sensitivity and frequency range.

For example, a precision accelerometer might have a nominal sensitivity of 100mV/g ± 5% (95 to 105mV/g) (see Figure 1) while a low-cost accelerometer might have a sensitivity of
100mV/g ± 10% (90 to 110mV/g). Customers with data acquisition systems will often normalise the inputs with respect to the calibrated sensitivity. This allows a group of low cost sensors to provide accurate, repeatable data. Regarding frequency, a precision accelerometer typically has frequency ranges in which the maximum deviation is 5% while low-cost sensors frequency might offer a 3dB frequency band. Even so, a low cost sensor might offer excellent frequency response.

The maximum amplitude or range of the vibration being measured determines the sensor range that can be used. Typical accelerometer sensitivities are 100mV/g for a standard application (50g range) and 500mV/g for a low-frequency or low-amplitude application (10g range). General industrial applications with 4-20mA transmitters commonly use a range of 0-25mm/s or 0-50mm/s. Physical structures and dynamic systems respond differently to varying excitation frequencies. A vibration sensor is no different. Piezoelectric materials, by nature, act as high pass filters and as a result, even the best piezoelectric sensor will have a low-frequency limit near 0.2Hz. A ranges in which the maximum deviation is 5% while low-cost sensors might offer a 3dB frequency band. Even so, a low cost sensor might offer excellent frequency response.

The maximum amplitude or range of the vibration being measured determines the sensor range that can be used. Typical accelerometer sensitivities are 100mV/g for a standard application (50g range) and 500mV/g for a low-frequency or low-amplitude application (10g range). General industrial applications with 4-20mA transmitters commonly use a range of 0-25mm/s or 0-50mm/s. Physical structures and dynamic systems respond differently to varying excitation frequencies. A vibration sensor is no different. Piezoelectric materials, by nature, act as high pass filters and as a result, even the best piezoelectric sensor will have a low-frequency limit near 0.2Hz. A sensor that acts as a dynamic system with one degree of freedom exhibits natural frequencies. The signal is greatly amplified at the natural frequency, leading to significant change in sensitivity and possible saturation. Most industrial accelerometers have single or
double-pole RC filters to combat saturation excitation at the resonant frequency. Thus it is critical to select a sensor with a usable frequency range that includes every frequency of interest. Applications with extremely high temperatures can pose a threat to the electronics built into accelerometers and 4-20mA transmitters. Charge-mode accelerometers are available for use in very high temperature applications. These have no built-in electronics, but instead have remote charge amplifiers. Charge-mode accelerometers with integral hard line cable are available for applications hotter than 260°C, such as gas turbine vibration monitoring.

Industrial accelerometers with integral polyurethane cable can be completely immersed in liquid for permanent installation. For high-pressure applications, it is a good idea to test the sensors at pressure for one hour. An integral cable is also normally required if the application is sprayed rather than being completely immersed, such as cutting fluid on machine tools. Industrial accelerometers can be constructed with corrosion and chemical resistant stainless steel bodies. Consider using PTFE cable with corrosion resistant boot connectors if the application is in an environment with harmful chemicals. Consulting a chemical compatibility chart is strongly recommended for any suspect chemicals. Integral armour-jacketed cables offer excellent protection for cables that might come into contact with debris such as cutting chips or worker’s tools. Ultimately, the sensor will need to be installed on equipment in convenient position. However, sensor geometry has little effect on its performance, but factors such as the space available and positioning that ensures that a maintenance engineer can gain safe access, do need to be taken into account. Accelerometers and 4-20mA transmitters are both available with CSA and ATEX approvals for use in hazardous areas. Compare the type of approval needed with the sensor’s published approvals to ensure it meets requirements.

**SENSOR TECHNOLOGY FOR SENSING VIBRATION:**

It is also worth to consider to specify a shear or compression technology sensor before choosing one for specific purpose. This question could command an article all of its own but in essence,
the argument boils down to the proven reliability, accuracy and repeatable performance delivered by shear designs against the earlier compression technique that can be sensitive to base bending and thermal transient effects causing measurement errors. The answers to these questions can greatly narrow searches for the best solution in a specific application. Keep in mind, some combination of answers might be mutually exclusive, i.e. a solution meeting every criterion does not exist. For example, a particular model might not carry the proper ATEX certification for use in hazardous area applications and some additional feature for specialized applications needs to be considered.

HEAT AND SMOKE SENSOR:

The damage to the Automated teller machine can be caused by cutting the machine to remove the machine from the housing or forced opening of the safe. In both the case if mechanical instruments are used, they are bound to generate vibrations of high level sufficient for the alarm system to activate. Other method which can be used for removing the Automated teller machine or forced opening of the safe can be by gas cutter or electrode cutters. The cutting tool may not be able generate high level of vibration but certainly increase the heat level of the kiosks and raise the smoke level above permissible limits. Hence Heat/smoke sensor shall be needed to deployed in combination with vibration sensor. International Code Council (ICC) has set combined codes into a single set of model building and fire codes. The ICC International Building Code and International Fire Code were first published in 2000 and were adopted by some states.

SMOKE SENSORS:

There are two basic types of smoke detectors are used today:

Ionization

Photoelectric.
The sensing chambers of these detectors use different principles of operation to sense the visible or invisible particles of combustion given off in developing fires. The purpose of this guide is to provide information concerning the proper application of smoke detectors used in conjunction with fire alarm systems. The guide outlines basic principles that should be considered in the application of early warning fire and smoke detection devices. It presents operating characteristics of detectors and environmental factors, which may aid, delay, or prevent their operation. The use of early warning fire and smoke detection systems results in significant reduction in fire deaths. The sooner a fire is detected, the better the outcome for saving lives. This document provides guidance for the proper operation of fire detection systems for those who apply, install, and maintain them. This document presents information for fire protection, mechanical, and electrical engineers; fire service personnel, fire alarm designers; and installers. A key element in the effectiveness of smoke detection systems is the latest version of NFPA 72 for installation and testing of systems. Installation must comply with all code requirements and directions from Authorities Having Jurisdiction (AHJs). AHJ directives always take precedence over other codes and exercise final authority over installations and maintenance procedures. Correct installation and maintenance of smoke detectors prevents unwanted nuisance alarms. Occupants can become desensitized when repeated nuisance alarms occur. In worst case scenarios, technicians could disconnect alarms from the system to avoid the unnecessary disruption. Either situation negates a detector’s potential life saving benefit, making the proper operation of an early

TESTING LABORATORIES:

Testing laboratories test smoke detectors, control panels, and other components of fire alarm systems to verify conformance with NFPA requirements and their own standards. Equipment that passes their tests is identified by a label and/or listing
IONIZATION SMOKE DETECTOR OPERATION:

A typical ionization chamber consists of two electrically charged plates and a radioactive source (typically Americium 241) for ionizing the air between the plates. The radioactive source emits particles that collide with the air molecules and dislodge their electrons. As the molecules lose electrons, they become positively charged ions. As other molecules gain electrons, they become negatively charged ions. Equal numbers of positive and negative ions are created. The positively charged ions are attracted to the negatively charged electrical plate, while the negatively charged ions are attracted to the positively charged plate. This creates a small ionization current that can be measured by electronic circuitry connected to the plates (“normal” condition in the detector).

Particles of combustion are much larger than the ionized air molecules. As particles of combustion enter an ionization chamber, ionized air molecules collide and combine with them. Some particles become positively charged and some become negatively charged. As these relatively large particles continue to combine with many other ions, they become recombination centers, and the total number of ionized particles in the chamber is reduced.

WORKING OF SMOKE DETECTORS:

This reduction in the ionized particles results in a decrease in the chamber current that is sensed by electronic circuitry monitoring the chamber. When the current is reduced by a predetermined amount, a threshold is crossed and an “alarm” condition is established. Changes in humidity and atmospheric pressure affect the chamber current and create an effect similar to the effect of particles of combustion entering the sensing chamber. To compensate for the possible effects of humidity and pressure changes, the dual ionization chamber was developed and has become commonplace in the smoke detector market.
A dual-chamber detector utilizes two ionization chambers; one is a sensing chamber, which is open to the outside air. The sensing chamber is affected by particulate matter, humidity, and atmospheric pressure. The other is a reference chamber, which is partially closed to outside air and is affected only by humidity and atmospheric pressure, because its tiny openings block the entry of larger particulate matter including particles of combustion. Electronic circuitry monitors both chambers and compares their outputs. If the humidity or the atmospheric pressure changes, the outputs of both chambers are affected equally and cancel each other. When combustion particles enter the sensing chamber, its current decreases while the current of the reference chamber remains unchanged. The resulting current imbalance is detected by the electronic circuitry. There are a number of conditions that can affect dual-chamber ionization sensors such as dust, excessive humidity (condensation), significant air currents, and tiny insects. All of these can be misread as particles of combustion by the electronic circuitry monitoring the sensors.

PHOTOELECTRIC SMOKE DETECTOR OPERATION:

Smoke produced by a fire affects the intensity of a light beam passing through air. The smoke can block or obscure the beam. It can also cause the light to scatter due to reflection off the smoke particles. Photoelectric smoke detectors are designed to sense smoke by utilizing these effects of smoke on light.

PHOTOELECTRIC LIGHT SCATTERING SMOKE DETECTOR

Most photoelectric smoke detectors are of the spot type and operate on the light scattering principle. A light-emitting diode (LED) is beamed into an area not normally “seen” by a photosensitive element, generally a photodiode. When smoke particles enter the light path, light strikes the particles and is reflected onto the photosensitive device causing the detector to respond.
PHOTOELECTRIC LIGHT OBSCURATION SMOKE DETECTOR

Another type of photoelectric detector, the light obscuration detector, employs a light source and a photosensitive receiving device, such as a photodiode. When smoke particles partially block the light beam, the reduction in light reaching the photosensitive device alters its output. The change in output is sensed by the detector’s circuitry, and when the threshold is crossed, an alarm is initiated. Obscuration type detectors are usually of the projected beam type where the light source spans the area to be protected.

SMOKE DETECTOR DESIGN CONSIDERATIONS

Although smoke detectors are based on simple concepts, certain design considerations need to be observed. They should produce an alarm signal when smoke is detected, but should minimize the impact of an unwanted signal which can arise from a variety of causes. In an ionization detector, dust and dirt can accumulate on the radioactive source and cause it to become more sensitive. In a photoelectric detector, light from the light source may be reflected off the walls of the sensing chamber and be seen by the photosensitive device when no smoke is present. Insects, dirt, drywall dust, and other forms of contamination can accumulate in the sensing chamber and reflect light from the light source onto the photosensitive device.

Electrical transients and some kinds of radiated energy can affect the circuitry of both ionization and photoelectric smoke detectors and be interpreted by the electronic circuitry to be smoke, resulting in nuisance alarms. The allowable sensitivity ranges for both types of detectors are established by Underwriters Laboratories, Inc. (UL). Detector performance is verified in fire tests. All smoke detectors are required to respond to the same test fires regardless of their principle of operation.
SELECTIO

N OF DETECTORS:

The characteristics of an ionization detector make it more suitable for detection of fast flaming fires that are characterized by combustion particles in the 0.01 to 0.4 micron size range. Photoelectric smoke detectors are better suited to detect slow smoldering fires that are characterized by particulates in the 0.4 to 10.0 micron range. Each type of detector can detect both types of fires, but their respective response times will vary, depending on the type of fire. It is often difficult to predict what size particulate matter will be produced by a developing fire because the protected buildings normally contain a variety of combustibles. The fact that different ignition sources can have different effects on a given combustible further complicates the selection. A lit cigarette, for example, will usually produce a slow smoldering fire if it is dropped on a sofa or bed. However, if the cigarette happens to fall upon a newspaper on top of a sofa or bed, the resulting fire may be better characterized by flames rather than by smoldering smoke. The innumerable combustion profiles possible with various fire loads and possible ignition sources make it difficult to select the type of detector best suited for a particular application.

SMOKE DETECTOR’S LIMITATIONS:

Smoke detectors offer the earliest possible warning of fire. They have saved thousands of lives. Special application rules can compensate for the limitations of smoke detectors. Smoke detectors may not provide early warning of a fire developing on another level of a building. Detectors should be located on every level of a building. Detectors may not sense a fire developing on the other side of a closed door. In areas where doors are usually closed, detectors should be located on both sides of the door.

As already indicated, detectors have sensing limitations. Ionization detectors are better at detecting fast, flaming fires than slow, smoldering fires. Photoelectric smoke detectors sense smoldering fires better than flaming fires. Because fires develop in different ways and are often unpredictable in their growth, neither type of detector is always best. A given detector may not
always provide significant advance warning of fires when fire protection practices are inadequate, nor when fires are caused by violent explosions, escaping gas, improper storage of flammable liquids such as cleaning solvents, etc.

**TYPICAL SYSTEM LAYOUT**

**WIRING SUPERVISION**

The initiating circuits that connect smoke detectors to a control panel should be supervised to detect and annunciate a fault (trouble) condition that could interfere with the proper operation of the circuit. Smoke detectors are generally categorized as either 2-wire or 4-wire detectors. Two-wire detectors derive their power from their connection to the fire alarm control panel alarm initiating device circuit. Since they are dependent on the initiating circuit, these 2-wire detectors must be tested and listed for compatibility with the associated control panel, to ensure proper operation.

Four-wire detectors are powered from a separate pair of wires, and, like the 2-wire detector, apply an electrical short across the associated alarm initiating device circuit to transmit an alarm. Because they do not derive power from the alarm initiating device circuit, electrical compatibility is predicated upon the operating parameters of the power supply to which the detectors are connected, and not the initiating circuit. Supervision of the power to 4-wire detectors is mandated through the use of an end-of line power supervision relay. When power is on, the relay contacts of the end-of-line relay are closed and connected in series with the end-of-line resistor beyond the last initiating device. Loss of power at any point in the power supply circuit will cause the relay to de-energize and a trouble con-
CLASS A CIRCUITS:

Class A circuits also differentiate between short circuits across the loop and open faults on the loop. Supervision is accomplished by monitoring the level of current passing through the installation wiring and the end-of-line resistor, which in a Class A circuit is an integral part of the fire alarm control panel. Class A wiring must return to and be terminated in the control panel. This technique requires that a minimum of four conductors terminate at the panel. It also requires the fire alarm control panel to monitor Class A circuits. The additional circuitry necessary for Class A supervision enables the control panel to “condition” the initiating circuit to monitor the initiating circuit from both ends when in a trouble mode due to an open fault on the loop. This “conditioning” ensures that all devices are capable of responding and reporting an alarm despite a single open circuit or non-simultaneous single ground.

Wireless Circuit:

Wireless detectors and their internal transmitters use one or more internal batteries as the source for their operating power and are UL listed. Supervision of the internal battery power source is incorporated within the smoke detector circuitry. If the battery power source depletes to the threshold specified by UL, the smoke detector will sound a local alert and initiate a trouble signal once per hour for a minimum of seven days or until the battery or batteries are replaced.

The wireless initiating devices are supervised for tamper and/or removal by initiating a distinct trouble signal. Each wireless device also initiates a test transmission every hour to verify the communication circuit. Any device failing to communicate is identified on the control panel no less than every four hours.
Figure 4.8 Class B Circuit

Class B circuits differentiate between short circuits across the loop (alarm) and open faults on the loop (trouble). Supervision of this circuit is accomplished by passing a low current through the installation wiring and an end-of-line resistor. The fire alarm control panel monitors the increases or decreases in the supervisory current and sends an alarm or trouble condition, respectively. A single open in a Class B circuit disables all devices electrically beyond the open

**GENERAL ZONING GUIDELINES:**

The faster the source of an alarm can be pinpointed, the faster action can be taken. Although formal rules for zoning are not given in fire protection codes, an exception is the rule for wireless devices stating that each smoke detector must be individually identified. It is always advisable to zone any system that contains more than a small number Fire Safety Functions. Often smoke detectors are utilized to control ancillary equipment. Care should be taken to ensure that detectors utilized in such a manner are approved for their intended purpose. A few of the typical applications are as follows:
to control the flow of smoke in air handling and air conditioning systems,

to release doors to contain smoke in a fire situation,

to release locks to allow exit in a fire situation,

to capture and recall elevators in a fire situation,

to activate a suppression system.

Spacing and placement requirements for detectors used in releasing service may be different from detectors used in conventional open area applications. 4-wire detectors are recommended in these situations because the control panel and detectors used will affect the power requirements. More than one detector relay on a circuit may not receive enough power from the 2-wire circuit to operate during an alarm.

NFPA publishes standards for the proper application, installation, and maintenance of automatic smoke detectors. The principal codes and standards, which should be reviewed before specifying or installing automatic smoke detectors. The purpose of this guide is to provide information concerning the proper application of smoke detectors used in conjunction with fire alarm systems. The guide outlines basic principles that should be considered in the application of early warning fire and smoke detection devices. It presents operating characteristics of detectors and environmental factors, which may aid, delay, or prevent their operation. The use of early warning fire and smoke detection systems results in significant reduction in fire deaths. The sooner a fire is detected, the better the outcome for saving lives. This document provides guidance for the proper operation of fire detection systems for those who apply, install, and maintain them. Correct installation and maintenance of smoke detectors prevents unwanted nuisance alarms. Occupants can become desensitized when repeated nuisance alarms occur. In worst case scenarios, technicians could disconnect alarms from the system to avoid the unnecessary disruption. Either situation negates a detector’s potential life saving benefit, making the proper operation of an early warning fire and smoke detection system indispensable. This
document presents information for fire protection, mechanical, and electrical engineers; fire service personnel, fire alarm designers; and installers. A key element in the effectiveness of smoke detection systems is the latest version of NFPA 72 for installation and testing of systems. Installation must comply with all code requirements and directions from Authorities Having Jurisdiction (AHJs). AHJ directives always take precedence over other codes and exercise final authority over installations and maintenance procedures. Testing laboratories test smoke detectors, control panels, and other components of fire alarm systems to verify conformance with NFPA requirements and their own standards. Equipment that passes their tests is identified by a label and/or listing.

The manufacturers of the smoke detectors being used may be contacted for any published information pertaining to their products

(I) TERRIBLE SYSTEM:

The security provided by the Automated teller machine safe is of the foremost importance, the protection of associate degree Automated teller machine is improved by interloper Alarm and Hold-Up device. The system should be put in accordance with relevant standards and codes of flow and be maintained under contract. Associate degree interloper alarm associate degrees Hold-Up System will solely offer a deterrent to associate degree attack on the associate degree Automated teller machine system and assist in conjuration a response by an acceptable authority. The deterrent worth of the associate degree device protective a high stealing risk against competent and determined criminals is a smaller amount than for a coffee stealing risk. The speed and potency of the particular response to the activation is thus of nice importance. It follows that the upper the strength of the Automated Teller Machine safe the bigger the worth of the device as a result of a robust safe lengthens the time out there for response. The Automated teller machine possess hooked up to that observers ready to detect strategies of attack doubtless to be used against a secure by criminals like drilling, ripping, percussion, explosives and every
one sorts of cutting. The detectors ought to be of a kind declared by the manufacturer to be appropriate to be used with an Automated teller machine. The detectors ought to be put in consistent with any recommendations or directions provided with them however altogether cases:

(a) One to be hooked up to every door to the ATM safe, one to be hooked up to the ATM safe elsewhere than on the door (s).

(b) Every door to the Automated teller machine safe ought to be fitted, in positions inaccessible from outside the Automated teller machine, with a method designed to convey associate degree alarm condition once the door, the lock or bolt(s) of the door don’t seem to be within the secure position. Associate degree alarm condition ought to be once the door(s) of the Automated teller machine safe is/are not closed and secured.

(c) Throughout associate degree amount that the premises containing an Automated teller machine area unit unattended, the traditional approaches to the Automated teller machine ought to be protected additionally by movement detector(s) of the specification giving the simplest out there sensitivity, dependability and resistance to interference (e.g. Masking). it’s essential that the system style takes account of the chance of false alarms, e.g.: from the activity of cleaners etc.

(J) HOLD-UP TRIGGERING DEVICES:

(a) One or a lot of hold-up triggering device(s) ought to be fitted within and/or near the Automated teller machine to be used throughout loading/maintenance procedures. The device(s) ought to be placed for simple use and minimum risk to workers.

(b) Instead or to boot, wire-free hold-up triggering alarm(s) ought to be carried by the person(s) supervision loading/maintenance procedures. In most cases these area units to be more popular to mount devices.
(c) Hold-up triggering devices may be engineered into the management and signifying instrumentality and/or

(d) Hold-up triggering device(s) shouldn’t be placed in a section to that the general public have access and since this may create to false alarms.

(K) SUPPLEMENTARY MANAGEMENT INSTRUMENTS.

CONTROL AND INDICATING INSTRUMENTS

(a) The management and indicating instrumentality to the device protecting the Automated teller machine ought to be cited among the world protected by the system and not accessible to the general public. Wherever doable a method of making a hold-up alarm condition ought to be incorporated within the management and indicating instrumentality.

(b) Care is {required} that the protection to the Automated teller machine is active once required, i.e.: that it’s not unset due, for instance, to its being enclosed in zones protective different areas. Ideally all of the protection provided to the Automated teller machine ought to get on one zone of the system and also the hold-up triggering devices on another.

(c) Automated teller machine alarm signals ought to wherever doable be distinguished at the Remote observation Centre from those of different components of the installation and conjointly distinguish between hold-up and intrusion.

WARNING DEVICES

(a) All native warning devices ought to be instant. Wherever a delay is needed, this to be for the minimum amount acceptable to the acceptable authority.
(b) Hearable warning devices, like bells or sirens, shouldn’t operate upon the activation of anti hold-up devices.

USE OF LIFE SCIENCE IN ATM SECURITY:

Though not in India, Biometric Authentication have been successfully used within the banking system within the context of Automated teller machines. A life science system may be: “Biometrics details of a client (account holder) to be validated or demonstrate victimization physical, activity attribute or their characteristics. These characteristics should be verified automatically”. The identification has the advantage of checking the user’s personal attribute or characteristics. These characteristics will be physical ones like fingerprints, face, iris or activity like voice, written signature, keyboard sound etc. This results in a doable split within the typically referred to as what we tend to area unit i.e. physical life science and what we tend to do i.e. activity life science. Activity characteristics are a unit less stable than physical characteristics.

OPERATING ON BIOMETRIC SYSTEMS:

To demonstrate the user in biometric systems, Automated teller machine ATM usage typically, works on two-factor authentication requiring one thing you have got i.e. associate degree ATM card and one thing you recognize i.e. a PIN code or a countersign otherwise you are a unit i.e. life science it should be Fingerprinted, Face, Iris etc.. The identification has the advantage of checking the user’s personal characteristics. These characteristics will be physical ones like fingerprints, face, iris or activity ones like voice, written signature, keyboard sound etc.

To use an associate degree Automated teller machine presently, demands having a card that must be excusable by PIN as a second issue authentication. There have been some experimental testing situations in reference to machine machines at the tip of the twentieth century. In recent years the banking organizations everywhere the planet have enforced new “Chip card and PIN authentication schemes” in machine machines so as to cut back card fraud prices. Identification is used to verify a person’s identity by activity digitally bound human characteristics and compare those measurements with people who are holding on in an exceedingly example for that very same person. Templates will be hold on at the biometric device, the institution’s
information, a user’s positive identification, or a sure Third Party service provider’s information.

There are two major classes of biometric techniques: physiological (fingerprint verification, iris analysis, hand geometry-vein patterns, ear recognition, odor detection, DNA pattern analysis and sweat pore analysis), and activity (handwritten signature verification, keystroke analysis and speech analysis).

Recently, Biometric Automated teller machine unit have been introduced to be used beside ATM card. This can be positively impacted on the number of frauds if absolutely enforced. Most development has created identification wherever palm vein is employed as a method of authentication. When, in situ of cards, some biometric options like iris, membrane scans or face area unit captured and more authentication is completed by palm or fingerprint, then Automated teller machine transactions can’t be done except by the authentic owner of the account.

We can divide the identification in 2 totally different areas:

1. Physical
2. Behavioral

<table>
<thead>
<tr>
<th>Physical</th>
<th>Behavioral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>Handwriting Signature</td>
</tr>
<tr>
<td>Retina/ Iris</td>
<td>Handgrip dynamics</td>
</tr>
<tr>
<td>Face recognition</td>
<td>Voice dynamics</td>
</tr>
<tr>
<td>Voice</td>
<td>Lips dynamics</td>
</tr>
<tr>
<td>DNA</td>
<td>Gait</td>
</tr>
<tr>
<td>Ear</td>
<td>Shape</td>
</tr>
</tbody>
</table>

Table: 4.1 types of biometric identification
In the above table 4.1 few biometric recognition patterns are shown.

**FINGERPRINT RECOGNITION**

Fingerprint recognition relies on the imaging of the fingertips. The structure of a fingerprint ridge and valleys is recorded as a picture or digital example (a simplified information, minutiae-based most of the time) to be more compared with different pictures or examples for authentication or verification, see figure 1 picture of fingertips are captured with specific fingerprint sensors.

![Fingerprint Image](image)

**Figure : 4.9 Fingerprint Ridge and Valley**

Among all the biometric techniques, fingerprint-based identification is a lot of known technique that has been with success used in Automated teller machine user authentication. A fingerprint could be a set of skin lines, domestically parallel, named ridges and empty area between 2 consecutive ridges named valleys. The 3 international shapes of this pattern, divided in arches, loops and whorls, area unit the primary level of knowledge we tend to might examine to classify fingerprints. The common worth of ridge to ridge frequency is about regarding 0.5 a
mm and also the average worth of the vale to ridge height is of regarding 0.1 mm. By convention, the fingerprint image is displayed because the trace the inked finger would go away on a paper, or, in different words, because the latent print of the finger. After all this 1st level data is useless to proceed with fingerprint verification.

![Fingerprint Image](image1)

**Fig 4.10 Trivia Specific Point**

The figure above shows he Fingerprint’s trivia specific point of a person indicating wherever a ridge is ending or bifurcating.

![Fingerprint Diagram](image2)

**Figure 4.11 Points Extracted From A Fingerprint**
The above figure shows points extracted from the fingerprint of a person, the pattern of extraction are enough and reliable fingerprint verification authentications in biometric method.

The second level of knowledge used is trivia. These are specific point of the Fingerprint wherever a ridge ends or bifurcates. Tens of such points are also to be extracted from a fingerprint for data to be enough to proceed with reliable fingerprint verification. This is one of the way of that authentication method can used to visualize the believability/authenticity of the user. Forensic sciences are conducting fingerprint identification for over 100 years for identification of criminals. Other, however not adequate, second level data area unit core(s) and delta(s) location, The pattern of ridges and valleys, with its trivia, core(s) and delta(s) area unit distinctive to every individual (different even for identical twins) and this pattern is thought to be stable throughout the time period[54].

The third level data are pores location on the ridges the employment of pore location is young, and coming back with the development of recent generation fingerprint sensors, ready to capture such details. As present, fingerprint recognition algorithms victimization system doesn’t seem to be mature enough to exchange minutiae-based ones.

**RETINA/IRIS RECOGNITION**

User authentication supported the attention splits in 2 families: 1- Iris recognition relies on the extraction of representative information from the outwardly visible colored ring round the pupil, whereas 2- membrane recognition relies on the analysis of the vessel pattern placed within the posterior portion of the attention.
The automatic technique of iris recognition, during this the iris could be a muscle among the attention that regulates the dimensions of the pupil, dominant the number of sunshine that enters the attention. The color relies on the number of endocrine pigment among the muscle. Iris imaging needs use of a top quality camera. Today’s industrial iris camera generally use close to infrared radiation to illuminate the iris while not inflicting hurt or discomfort to the client.

**FACE RECOGNITION:**

Face recognition relies on the imaging of the face. The structure of the face is recorded as an image or digital template a plenty, non-mature, simplified information formats for more comparison. Early face recognition algorithms used straightforward geometric models, however the popularity method is currently stirring into a science of refined mathematical representations and matching processes. Major advancements and initiatives within the past 10 years have propelled this technology into the spotlight.
The authentication method could be a comparison between a preregistered reference image, or example (representative information extracted from the raw image, engineered throughout associate degree registration step) and a new captured candidate image, or template. Looking at the correlation between these 2 samples, the formula can verify if the someone is accepted or rejected. This applied math method results in a False Acceptance Rate (FAR) i.e. the likelihood to simply accept a non-authorized user and a False Rejection Rate (FRR) i.e. the likelihood to reject a licensed user.

**VEIN PATTERN RECOGNITION**

The Vein Pattern technology works on characteristic the hypodermic (beneath the skin) vein patterns in associate degree individual’s hand. Once a user’s hand is placed on a scanner, a near-infrared lightweight maps the situation of the veins.
The red blood cells gift within the veins absorbs the rays and show up on the map as black lines, whereas the remaining hand structure shows up as white. When the vein example is extracted, it’s compared with an antecedently hold on patterns and a match is created.

Above mentioned biometric securities issues are helpful and acceptable for enhance the Automated teller machine security from dishonest attacks on system.

4.3 SOFTWARE SECURITY:

Software security in terms of Automated teller machine could be a major concern. There are 2 sets of software employed in Automated teller machine. One is that the package and another is that the program that works for different user operations on machine. In current generations of Automated teller machine the windows XP package is employed for many of the Automated teller machines. To use the windows XP in new Automated teller machines is its dependability and safety features that make the system safer and protected with package attacks. Windows XP permits the configuration of coarse security settings through the “Local Security User Rights” management what actions specific users and/or teams are permitted to perform on the system. These restrictions will create the package security a lot of robust in terms of an operation of associate degree Automated teller machine and create the system safer. Here is few operating operations and their actions are a unit mentioned bellow by that we are able to set the actions for specific tasks.
## SECURITY SETTING FOR USERS/GROUPS

<table>
<thead>
<tr>
<th>Working Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access this computer from the network</td>
<td>No one</td>
</tr>
<tr>
<td>Act as part of the operating system</td>
<td>No one</td>
</tr>
<tr>
<td>Add workstations to domain</td>
<td>No one</td>
</tr>
<tr>
<td>Adjust memory quotas for a process</td>
<td>Administrators</td>
</tr>
<tr>
<td>Change the system time</td>
<td>Administrators</td>
</tr>
<tr>
<td>Back up files and directories</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allow logon through Terminal Services</td>
<td>No one</td>
</tr>
<tr>
<td>Create a token object</td>
<td>No one</td>
</tr>
<tr>
<td>Debug programs</td>
<td>Administrators</td>
</tr>
<tr>
<td>Deny logon as a batch job</td>
<td>No one</td>
</tr>
<tr>
<td>Enable computer and user accounts to be trusted for delegation</td>
<td>No one</td>
</tr>
<tr>
<td>Load and unload device drivers</td>
<td>Administrators</td>
</tr>
<tr>
<td>Perform volume maintenance tasks</td>
<td>Administrators</td>
</tr>
<tr>
<td>Modify firmware environment values</td>
<td>Administrators</td>
</tr>
<tr>
<td>Manage auditing and security log</td>
<td>Administrators</td>
</tr>
</tbody>
</table>

Take ownership of files or other objects

*Table : 4.2 security settings for user’s and groups*
Windows XP permits the configuration of granular security settings through the “Local Security Policy”. The recommendations below ought to be analyzed and tested on non-production Automated teller machines to make sure compatibility with specific Automated teller machine package versions, applications and operational support needs. To boot, consult the Automated teller machine seller/manufacturers for a determination on specific settings listed below.

<table>
<thead>
<tr>
<th>Policy Recommended Security Setting</th>
<th>Status/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts:</td>
<td></td>
</tr>
<tr>
<td>Administrator account status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Limit local account use of blank</td>
<td>Enabled</td>
</tr>
<tr>
<td>passwords to console logon only</td>
<td></td>
</tr>
<tr>
<td>Rename administrator account</td>
<td>Rename</td>
</tr>
<tr>
<td>Audit:</td>
<td></td>
</tr>
<tr>
<td>Shut down system immediately if unable to log security audits</td>
<td>Disabled</td>
</tr>
<tr>
<td>Audit : Audit the access of global system Objects the use of Backup and Restore privilege</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Devices:</td>
<td></td>
</tr>
<tr>
<td>Allowed to format and eject removable media</td>
<td>Administrators</td>
</tr>
<tr>
<td>Allow unlock without having to log on</td>
<td>Not Defined</td>
</tr>
</tbody>
</table>
### Analysis of Security Issues of ATM

<table>
<thead>
<tr>
<th>Setting</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent users from installing printer</td>
<td>Enabled</td>
</tr>
<tr>
<td>Drivers</td>
<td></td>
</tr>
<tr>
<td>Unsigned driver installation behaviour</td>
<td>Warn but allow installation</td>
</tr>
<tr>
<td>Domain controller: Allow server operators to schedule tasks</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Digitally encrypt or sign secure channel data (always)</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Digitally sign secure channel data (when possible)</td>
<td></td>
</tr>
<tr>
<td>Disable machine account password changes</td>
<td>Enabled</td>
</tr>
<tr>
<td>Maximum machine account password age</td>
<td>Enabled</td>
</tr>
<tr>
<td>Require strong (Windows 2000 or later) session key</td>
<td>Disabled 7 days</td>
</tr>
<tr>
<td>Enabled Interactive logon: Do not display last user name</td>
<td>Enabled</td>
</tr>
<tr>
<td>Interactive logon:</td>
<td></td>
</tr>
<tr>
<td>Do not require CTRL+ALT+DEL</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
### Analysis of Security Issues of ATM

<table>
<thead>
<tr>
<th>Microsoft network client:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Digitally sign communications (always)</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Digitally sign communications (if server agrees)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Send unencrypted password to third-party SMB servers</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Microsoft network server:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount of idle time required before suspending session</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Digitally sign communications (always)</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Digitally sign communications (if client agrees)</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network access:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow anonymous SID/Name translation</td>
<td>Disabled</td>
</tr>
<tr>
<td>Do not allow anonymous enumeration of SAM accounts</td>
<td>Enabled</td>
</tr>
<tr>
<td>Do not allow anonymous enumeration of SAM accounts and shares</td>
<td>Disabled</td>
</tr>
<tr>
<td>Let Everyone permissions apply to anonymous users</td>
<td>Not defined</td>
</tr>
<tr>
<td>Remotely accessible registry paths</td>
<td>Not defined</td>
</tr>
<tr>
<td>Named Pipes that can be accessed anonymously</td>
<td>for local accounts</td>
</tr>
<tr>
<td>Sharing and security model</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Network security:</strong></td>
<td></td>
</tr>
<tr>
<td>Do not store LAN Manager hash value on next password change</td>
<td>Enabled</td>
</tr>
<tr>
<td>Force logoff when logon hours expire</td>
<td>Disabled</td>
</tr>
<tr>
<td>LAN Manager authentication level</td>
<td>Send NTLMv2 response</td>
</tr>
<tr>
<td>LDAP client signing requirements</td>
<td>only/refuse LM &amp; NTLM</td>
</tr>
<tr>
<td>Minimum session security for NTLM SSP based (including secure RPC) clients</td>
<td>Negotiate signing</td>
</tr>
<tr>
<td>Minimum session security for NTLM SSP based (including secure RPC) servers</td>
<td>Require NTLMv2 session security, require 128 bit encryption</td>
</tr>
<tr>
<td><strong>Recovery console:</strong></td>
<td></td>
</tr>
<tr>
<td>Allow automatic administrative logon</td>
<td>Disabled</td>
</tr>
<tr>
<td>Allow floppy copy and access to all drives and all folders</td>
<td>Disabled</td>
</tr>
<tr>
<td>Shutdown: Allow system to be shut down without having to log on</td>
<td>Disabled</td>
</tr>
<tr>
<td>Shutdown: Clear virtual memory page file</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>System cryptography:</strong></td>
<td></td>
</tr>
<tr>
<td>Use FIPS compliant algorithms for encryption, hashing, and signing</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Table 4.3** Policy Recommended Security Setting and their status
4.4. LOGICAL SECURITY:

Automated teller machines have begun to use industry-standard and multivendor hardware architectures (with USB connections for peripherals, local area network and IP communications), in operating systems and customary application layer dealing protocols, introducing substantial changes within the means Automated teller machines are deployed and put in. New reality wherever a lot of Automated teller machines are placed off-premises and Automated teller machines acquirer networks area unit a lot of typically owned and controlled by freelance Automated teller machines operators. There is such a large amount of fraud cases on ATMs has come into the notice during which criminal activities have junction rectifier to penetration of Automated teller machines networks and unauthorized distribution of money. Automated teller machines are getting a lot of and a lot of refined in terms of scale, utilized technology, funding, coming up with and execute. Automated teller machines fraud is high of mind for all monetary establishments and has created them involved regarding the integrity of their Automated teller machines’ package stack and their risks on monetary and name losses.

Logical security compulsory through developing secure payment systems moreover as in network and application penetration testing (certified moral hacking) and rhetorical analysis close compromises of cardholder information, has permitted to develop a selected and goal oriented approach to vulnerability assessment of Automated teller machines and associated logical security protection to known and unknown attacks. Exploiting combined vulnerabilities and also the developed malware program code in operation on the standardized process, in this sort of hacking, hacker is in a position to begin unauthorized money dispensing from the Automated teller machines by accessing the Automated teller machines at a self-selected time and date. The result with cash-out will be timely delayed or triggered by a predefined device. Logical security is taken into account on these sorts of risks given in Automated teller machines to reduce the attacks. Compromises of cardholder information, has allowed to develop a selected
and targeted approach to vulnerability assessment of Automated teller machines and associated network logical security protection to proverbial and unknown threats.

The following strategies will be employed in the attack:

- The offender will attempt to build amendment and/or delete information in/from databases or transmit queries to

- Information bases that come back a lot of data than the system would do once operating properly.

- Secure Socket Layer man-in-the-middle attacks: If an associate degree offender with success carries out associate degree SSL man-in-the-middle attack

- He will sniff information into the encoded tunnel, see, amendment and take a look at to falsify it, just in case such decoded login

- Data and sensitive data area unit transmitted among the tunnel.

- Session-hijacking attacks wherever the offender can attempt to takeover user-sessions and see, change, falsify or delete any user-data.

- Test on replay potentialities wherever it’s tested to check if the info from one shopper will be recyclable through

- Information disclosure: provocation of error messages to achieve version details of services. This provides some careful data regarding the server services and their configuration,

- At an equivalent time provides data regarding security vulnerabilities, consequently permitting targeted attacks.

- Tests of buffer or a heap overflow (POST) attacks whereby a DoS will be caused by movement down or phase change the server service. It’ll be doable to open a “root-
shell” and gain complete body access to the system, add further users or compromise the system in our own way (e.g. By putting in key loggers etc.).

Spoofing and fuzzing: generally applied in an exceedingly black-box approach to seek out vulnerabilities by manipulating protocols, files, etc. Apply brute force strategies or otherwise exploit weak cryptography

Based on previous analysis or no heritable documentation, the offender can verify and use vulnerabilities through analysis and investigation of interfaces and protocols.

In this sort of logical security problems an avid Whitebox approach applicable at the amount of Automated teller machines controls. Exploiting combined vulnerabilities and also the injection of deliberately developed program code (malware) in operation on the XFS standardized interface. They put in package includes the (hardened) package, the Automated teller machines application (end-user application moreover because the administration applications, for instance, application package downloading, package updates, observation of the Automated teller machines), the peripheral drivers and also the computer code (hardware intimate code). Usually, mechanisms are a unit in situ to observe an alteration of the package. As all of the peripheral are in restraint of the Automated teller machines, they’re all doubtless candidates for attacks. Vulnerability assessment and penetration testing area unit centered on the chances of manipulating the (arrow-lined) interfaces, with the aim to see if unauthorized access or different malicious activity may lead to unauthorized distribution of money. Typical penetration testing includes network and application layer testing moreover as controls and processes round the networks and applications. A typical API approach ought to be applicable for accessing associate degrees manipulating the assorted peripheral devices of an Automated teller machines. Access to interface commands ought to be restricted through the access management mechanisms of the Automated teller machines package. As totally different interpretations of the quality exist, typically, a middleware layer is employed to even out the variations between varied platforms.
This middleware layer is sometimes the results of a proprietary development by the Automated teller machines manufacturer, typically requested by Automated teller machines operators to possess specific practicality enclosed for his or her specific purpose and thus a lot of prone to attacks exploiting weaknesses during this management layer.

**APPROACH TO PENETRATION TESTING**

The following documents as a baseline in playing penetration testing:

- Documentation for Penetration tests, BSI (Standardization of information and data Security)
- Ethical Hacking and Countermeasures pointers, EC
- Several trade Best Practices

These documents are the inspiration for Penetration Testing Approach during which the subsequent phases and approaches are defined:
Referring to the amount of information provided on systems, architectures, networks, applications, in operating systems, procedures, access mechanisms, etc., initial analysis and actual testing will be performed on the premise of 3 totally different approaches mentioned within the image above:

Black-box approach, accurately simulating an actual “outsider” hacker with no or restricted previous information on any of the higher than things. Publicly out their data (view as an example queries on search engines, mailing lists, newsgroups, public databases and different web sources) is collected to seek out out regarding proverbial malware and exploits. Also, passive and active assessment of environmental data through e.g. packet-sniffing, port scans, OS and application process, service identification, desktop firewall evasion, IPS/IDS detection and network mapping is employed to seek out out regarding probabilistic existent vulnerabilities.

Greybox approach, with a narrowed down scope and with an avid target one threat situation with one entry purpose at bound suspected components of the ATM. This approach will be helpful just in case the ATM operator needs to receive a lot of careful investigations on a selected (e.g. Known) “insider” attack, while not already revealing all out there (and principally confidential) data. Reverse engineering (if not restricted by native laws) as a technique to know the applying logic will be a part of this.

Whitebox approach, accurately simulating an actual “insider” hacker assaultive with within information up to the amount of knowledge that bank branch workers, IT workers or Automated teller machines manufacturer technical workers have. A Whitebox approach assumes information of e.g. manufacturer’s product documentation, interface descriptions and protocol data, applications, programming languages, package development life cycle, privilege management, work mechanisms, data on security and committed to writing policies (e.g. Hardening guidelines) and patch management, manufacturer test- and debugging tools, supply codes, access to
manufacturer technical workers, etc. additionally and if not absolutely and firmly encrypted, a core Automated teller machines memory device will be investigated via rhetorical associate degreealysist (on a virtualized associate degree secure rhetorical copy of the initial information) to mimic the case of an offender possessing an Automated teller machines device when stealing with the aim to assess that confidential or essential data (e.g. The card data, client information, login credentials, etc.) is offered.

The increasing quantity of knowledge provided within the higher than 3 approaches is directly proportional to the likelihood of success in assaultive the Automated teller machines. All approaches aim to achieve careful information of transport and application layer protocols on each internal and external interfaces and just in case a vulnerability is detected and solely when the specific agreement of the Automated teller machines operator or effort bank client, specific program code (malware) will deliberately be developed that’s want to prove the vulnerability idea.

4.5. COMMUNICATIONAL SECURITY:

In the networking system information communicates in communicational lines. Normal information transmission will communicate in the traditional type of however confidential information might transmit within the kind of encrypted form o that no-one will hack the direction from communicational lines. The banking sector is one in all the vital sector wherever all sort of monetary data send through the communicational lines and it desires the high security of knowledge. Varied encryption algorithms are a unit want to defend the info among a network for electronic communication. Automated teller machines is additionally associate degree example wherever we’d like high security of knowledge in terms of knowledge communication from Automated teller machines to bank Server and contrariwise.
NETWORK COMMUNICATION LINE:

Communicational security in Indian banking industry, off-premise or remote Automated teller machines area unit dearly-won to control, primarily due to the value of the chartered telecommunication lines that banks have required to make sure the best level of security between the Automated teller machines associate degreed its server (or dealing processor – an external third-party element (hardware device) that links with bank databases and authorizes transactions). Chartered lines area unit generally terribly dearly-won, particularly relative to the value of employing a public network, which might be as very little as ten % of the monthly value of a chartered line. The appearance of wireless cellular networks has conjointly created it doable to avoid provisioning and putting in a wire line that is additionally dearly-won and long. The first drawback with employing a public network has been electronic communication security. As a result of all giant companies’ and monetary institutions’ company networks area unit connected to a public network (i.e., the Internet), and since kingdom has centered its criminal efforts on stealing individuality data, monetary data, money, and trade secrets, web property has created a replacement avenue to achieve embezzled access to direction. There is a unit such a large amount of efforts area unit created to keep up and improve information security around enterprise networks. As a result of Automated teller machines systems ought to be protected by a minimum of an equivalent level of security as different enterprise systems, chartered lines are wont to create the Automated teller machines system a vicinity of the company network.

In the same sequence connecting to associate degree Automated teller machines to a bank’s Automated teller machines server over the net compromises the enterprises’ security solutions, exposing Automated teller machines systems to attack. Banks, however, like all giant enterprises, area unit perpetually challenged to cut back in operation prices in each section of their businesses. The flexibility to cut back the first budget items of associate degree Automated teller machines
(the chartered line property charges) creates an awfully engaging come back on investment. Bank enthusiasm for past market solutions has been restricted due to the reduction in security and also the corresponding risk of a security breach that might harm the bank’s name and monetary stability. The ultimate issue concerned in changing from wired leased-line property to wireless cellular property is wireless carrier spec. Wireless carriers have typically catered to client markets and area unit involved solely regarding providing a reliable, low cost association to the net. Sadly, cellular communications will be too simply “eavesdropped,” captured, or jammed. In essence, this violates the Gramm-Leach-Bliley Act that states that monetary transactions should be firmly transmitted.

Since the addition of security or re-architecture to denationalize their networks adds a layer of quality that raises instrumentality and support prices, carriers haven’t been willing to create those investments. Instead, they use routable, public addresses with scant segmentation, exposing their client and company customers to vulnerability scans and attacks that will compromise information or exploit compromised devices to attack different devices. Sadly, most carriers think about any new design that interferes with a straightforward “data-com pipe” business to be too specialized and outdoors their core business.

Due to the mixture of carrier individualistic security attitudes and also the vital come back on investment for victimization the general public web as a transport mechanism for Automated teller machines transactions, there exists a right away went for an extremely secure cellular design meant for monetary transactions and services. to the current finish, JBM physics has partnered with Communications and Security Compliance Technologies (CSCT) to deliver resolution an answer) that fulfills this want while not requiring the replacement of existing Automated teller machines within the field – a serious advantage over any solution presently being thought by the carriers themselves.
DATA ENCRYPTION TECHNIQUES:

Data encryption technique for secure electronic communication in banking and ATM transactions:

In Automated teller machine for secure electronic communication, varied encryption strategies are used. These are:

- DES
- AES
- 3DES
- RC4
- EPP

DES is the customary for electronic communication. DES (Data cryptography Standard) is the transformation (of data or information) to a type that is not possible to scan while not having acceptable knowledge or key. Information cryptography customary (DES) was developed to supply data security in network by an IBM team around 1974 and adopted as a world customary in 1977. Encryption customary (DES) could be a customary cryptological system with the sort and mode symmetry formula. Cryptological algorithms employed in DES – that is named the info cryptography formula (DEA) – is that the process of bits within the block of cipher (Cipher block). DES could be a block cipher victimization sixty four-bit blocks and victimization external key length of 64 bits moreover (same with a block size). In DES, the method encryption (plain text) victimization the interior key or sub-key in fifty six bits are generated from the associate degree external key.

The procedure is completed by formula DES is as follows:

Step 1: Plaintext block was permutated by initial permutation matrix (Initial permutation/IP)
Step 2: To dam the initial permutation proficiency level in these enciphering method (Encryption) to try and do sixteen rounds (Round). During this method used internal keys for various every rotation.

Step 3: The results of the enciphering method are permutated victimization reversal permutation matrix (the inverse initial permutation/IP-1)

DES within the blood profile mode is employed for all cryptography. The Automated teller machines computer keyboard or EFTPOS telephone set contains an intrinsically tamper-proof master kilometer proverbial solely to the machine and also the host laptop.

Each time the machine is started up (e.g. Every morning, associate degree typically a lot of frequencies) the host laptop sends to the Automated teller machines a replacement daily key kD encrypted victimization kilometer and an initial dealing key kT conjointly encrypted victimization kilometer.

The initial kT is employed for the primary dealing. For later transactions a replacement kT is calculated from kT:=kT⊕ last MAC sent by the Automated teller machines this can be referred to as ‘chaining’ the key kT; it’s done to create it not possible to record messages from associate degree ATM to its host machine then play them back at a later time. At the later time the key kT can have altered since it’s a operate of kD and every one the transactions that have occurred since the last initial kT was loaded.

A MAC (Message Authentication Code) used with associate degree Automated teller machines could be a 64-bit range that’s calculated from associate degree unencrypted message by running it through DES with key kD victimization blood profile mode. The ensuing 64-bit block is that the MAC. All transmissions area unit checked employing a MAC. In impact the dealing key kT is itself subject to blood profile cryptography.
FOR TRANSACTIONS ON ASSOCIATE DEGREE ATM:

1. The account range and name area unit scan from the card; the PIN is entered. Allow us to decision this the ‘message’.

2. From this ‘message’ a corresponding MAC is calculated then the ‘message’ is encrypted victimization kT. Next the encrypted ‘message’ and also the MAC area unit sent to the host laptop.

3. The host decrypts the encrypted ‘message’ victimisation kT to retrieve the ‘message’; the host then uses the ‘message’ to calculate a MAC, and checks that this can be adequate the MAC sent with the encrypted ‘message’. This authenticates the message as having return from the Automated teller machines. The host then checks the account details and PIN on its information, and if everything checks out properly it then replies with a ‘go ahead’ message encrypted with kT, and followed by its own MAC.

4. You enter the info for the dealing, and another ‘message’ is made by the ATM, together with the date, time, Automated teller machines number, a sequence range, and details of the dealing. this can be encrypted by the Automated teller machines victimization kT and sent (along with its MAC).

5. When authenticating the Mack as before, and when checking the account balance etc., the host sends as ‘OK to pay’ message together with the new balance etc., once more encrypted victimization kT and with its own MAC.

In ‘off-line’ mode the PIN is checked against a PIN hold on in encrypted type on the ATM card. Details of the dealing area unit recorded and later transmitted to the host. As no confirmation from the host of your identity is offered, the withdrawal limits area unit typically lowers with this mode. EFTPOS is comparable however includes some bourgeois data moreover. It is conjointly
counseled that a random range is enclosed at the beginning of every message, before the MAC is calculated and before cryptography is completed. This can be to more increase the protection.

**ADVANCED CRYPTOGRAPHY CUSTOMARY (AES):**

The National Institute of Standards and Technology (NIST) has created AES, that could be a new Federal science customary (FIPS) publication that describes associate degree cryptography technique. AES could be a privacy rework for IPSec and web Key Exchange (IKE) and has been developed to exchange the info cryptography customary (DES). AES is meant to be safer than DES: AES offers a bigger key size, whereas guaranteeing that the sole proverbial approach to rewrite a message is for associate degree interloper to do each doable key. AES features a variable key length—the formula will specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

AES ready to method six fold quicker compared with the triple DES for an equivalent process capability. However the employment of triple DES remains enough encountered thanks to the quickness of the COS giant enough to modify to the technology new. additionally, compared with AES, triple DES implementation is felt a lot of appropriate for application on the device hardware, like network system communications, VPN network devices or at associate degree Automated teller machines.

**3DES:**

DES was approved by the Yankee National Standards Institute (ANSI X3.92) in 1981 as non-public sector cryptography customary and is that the most generally deployed industrial cryptological formula within the world. This formula uses a 56-bit key length. Within the twenty years of its use, there have not been any findings indicative of recursive weakness. Despite the strength of the DES formula, advances in laptop speed and process power area unit approaching
the purpose wherever brute-force searches of its 56-bit key area will be accomplished among an inexpensive period of time. The Triple DES formula answers this drawback by specifying 3 rounds of DES operations, effectively increasing the key length to 168 bits. 3DES could be a revised variation of DES thanks to the requirement for higher levels of security. All the banks area unit victimization this cryptography customary for secure electronic communication in an exceedingly public network. 3DES could be a variant development of DES (Data cryptography Standard) – antecedently noted as “multiple DES” essentially thanks to the triple DES just continual use of DES; during this case repetition performed 3 times. Triple DES is usually called TDES or by the term stands 3DES. Security issues within the use triple DES, remains doable there assault with the employment of 232 Known-plaintexts, 2113 steps, 290 DES-determination, and 288 memory capability.

DES40 formula, out there internationally, could be a variant of DES during which the key key’s preprocessed to supply forty effective key bits. it’s designed to be used by customers outside the USA and North American country WHO need to use a DES-based cryptography formula. This feature provides industrial customers a selection within the formula they use, notwithstanding their geographic location.

**RSA RC4:**

It may be an extremely Secure, High Speed formula The RC4 formula, developed by RSA information Security opposition, has quickly become the de-facto international customary for high-speed encryption. Despite in progress makes an attempt by cryptological researchers to “crack” the RC4 formula, the sole possible technique of breaking its cryptography proverbial these days remains brute-force, systematic idea, that is usually unworkable. RC4 could be a stream cipher that operates at many times the speed of DES, creating it doable to cipher even giant bulk information transfers with stripped performance consequences.

RC4_56 and RC4_128 RC4 could be a variable key-length stream cipher. The Oracle Advanced Security choice unleash eight.1.5 for domestic use offers associate degree
implementation of RC4 with five 6 bit and 128 bit key lengths. This provides robust cryptography with no sacrifice in performance compared to different key lengths of an equivalent formula[55][56].

**ENCRYPTED PIN PAD (EPP):**

With traditional keypads, the PIN entered by the client is shipped in “raw” state via a cable to a separate printed circuit module containing cryptography integrated circuits. For many countries, this arrangement was satisfactory as a result of the cable logic gate card area unit placed among the secure chest space of the ATM. So as to decrease PIN stealing fraud, VISA associate degree MasterCard area unit currently requiring an encrypted PIN pad (EPP) in situ of the computer keyboard. The EPP could be a sealed module that now and domestically encrypts the PIN when entry. There are not any “raw” PIN numbers accessible to electronic hackers either by physically sound onto wires among the ATM or remotely sensing no particulate radiation emitted.

**ALARM SYSTEMS:**

In order to safe guard the Automated teller machines at remote locations as well as the user of Automated teller machine at such locations, we have discussed that there is need to install equipment capable of raising alarm at police station and the bank to which Automated teller machine for immediate interventions. Sounding of the alarm at the Automated teller machine is likely to increase danger level than mitigating the danger. There can three types of alarm, which can be fitted inside the Automated teller machine kiosks for the purpose and these are alarms working by sensing vibration, heat and smoke inside a teller machine housing. Details of each types of these alarm are here under.