OPEN ACCESS Freely available online

Journal of Research and Development

Research Article

Global Identification of Smart Card Technologies-Safe and Secure: A Research

Thangavel V*

Department of Philosophy, St. Francis Institute of Management and Research, Mumbai, India

ABSTRACT

Smart card technology is currently popular for global identification. The use of smart cards continues to increase in various fields along with the rapid development of technology. Data security stored on a smart card needs to be a focus of attention to avoid misuse of data by unauthorized parties. It is not enough for the security mechanism to be carried out only during the communication process of sending data, but the mechanism for securing data on the smart card also needs to be done. In this study, a data security technique using dynamic keys is proposed by changing the key and access conditions on the smart card according to predetermined rules. This technique ensures that the keys used to access each smart card are different so that the risk of data duplication and modification threats can be minimized. In addition, this mechanism is a low-cost security privacy protection. The test results show that the data security technique using dynamic keys ensures read and write access to the smart card can only be done if the keys used match the rules. This paper presents an overview of the history, commercialization, technology, standards and current and future applications of smart cards. Section 1 is an overview of smart cards, including their current global use in identification, verification and authorization applications through their ability to support transaction processing, information management and multiple applications on a single card. This section also includes a summary of the invention and early development and application of smart cards. The second section describes a typical smart card based transaction, tracing it from the initial contact between a card and the card reader through the transaction to termination of the transaction. The third section describes the physical characteristics of the smart card and its associated contact and contactless interfaces, Integrated Circuit (IC) chip and processor capacity. Section 4 summarizes the international standards associated with smart cards, including those related to interoperability among contact and contactless cards, and their respective reading devices. In section 5, the focus is a high-level discussion of associated access technologies, including a more detailed look at magnetic stripe and barcode technologies and standards. This section includes a very brief mention of the impact of RISC-based technologies and Sun's Java™ Virtual Machine®. Section 6 discusses smart card security relating to the card's ability to authorize and facilitate electronic, logical and physical access to controlled applications and physical locations. Also discussed is physical security, which relates to cardholders, environment and cards tampering and data security, which is related to smart cards ability to support cryptography and cross validation of data stored on the cards across multiple databases for purposes of identification verification. Section 7 concludes this paper with a look at the future of smart card related developments, including those related to both technology and applications. Technology related developments include the support of more than a single operating system on the processor chip and peripheral card technologies. Application related developments include those related to identification, information storage and transaction processing.

Correspondence to: Thangavel V, Department of Philosophy, St. Francis Institute of Management and Research, Mumbai, India; E-mail: v.thangavel@rocketmail.com

Received: 16-Nov-2023, Manuscript No. JRD-23-28042; **Editor assigned:** 20-Nov-2023, PreQC No. JRD-23-28042 (PQ); **Reviewed:** 05-Dec-2023, QC No. JRD-23-28042; **Revised:** 08-Jan-2025, Manuscript No. JRD-23-28042 (R); **Published:** 16-Jan-2025, DOI: 10.35248/2311-3278.25.13.283

Citation: Thangavel V (2025) Global Identification of Smart Card Technologies-Safe and Secure: A Research. J Res Dev. 13:283.

Keywords: Smart card; ATM card fraud; Card trapping; Card skimming; Card jamming; Card phishing; Card steeling; Program cracking; Card steeling; Banking; Debit card fraud; Credit card fraud; ATM card theft; Cash withdrawal fraud; Exchange fraud; Bank related fraud; Synthetic account fraud; Loos of money fraud; General fraud; Other fraud; Technology; International standard integrated circuit chip; Contact and contactless cards; Dual interface card; Memory base smart card; Microprocessor base smart card; Hybrid smart card; Electronic cards; Medi claim card; Insurance card; Provident fund card; Driving smart card; Multiple database identifier; Chip technology; Biometric base chip; Buto identifier; Card transaction; Online banking; Online money transfers

INTRODUCTION

E-banking has the potential to transform the banking business as it significantly reduces transaction and delivery costs. This paper discusses some of the problems developing countries, which have a low penetration of information and telecommunications technology, face in realizing the advantages of e-banking initiatives. Major concerns such as the digital gap between the rich and the poor, the different operating environments for public and private sector banks, problems of security and authentication, management and regulation; and inadequate financing of Small and Medium-sized Enterprises (SMEs) are highlighted [1].

E-Banking: In simple words, e-banking implies the provision of banking products and services through electronic delivery channels. Electronic banking has been around for quite some time in the form of Automatic Counter Machines (ATMs) and telephone transactions. In more recent times, it has been transformed by the internet-a new delivery channel that has facilitated banking transactions for both customers and banks. For customers, the internet offers faster access, is more convenient and available around the clock regardless of the customer's location.

History of smart card

Roland Moreno was a French inventor, engineer, humorist and author who was the inventor of the smart card. Moreno's smart card or la carte a puce in French, was little known internationally. However, he became a national hero in France and was awarded the Legion d'Honneur in 2009.

Smart cards appeared on the horizon when two German inventors, Jurgen Dettlaff and Helmut Group, patented the idea of having plastic cards hold microchips in 1968. The Japanese patented another version of the smart card in 1970 and former French journalist Roland Moreno filed for a patent on the IC card, later dubbed the "smart card," in 1974. Moreno received a first (that is, priority) patent in France in 1975 and a U.S. Patent in 1978.

The early smart card research was theoretical, since the technology to support this innovative thinking was not available until 1976. In 1977, Motorola semiconductor, in conjunction with Bull, the French computer company, produced the first smart card microchip. France was an early smart card proponent and its investment in smart card research in the 1970's reflected a national effort to modernize its technological infrastructure.

Because the technical infrastructure for the cards was limited and consumers and retailers were unwilling to adopt the expensive and unreliable technology, France's first test of smart cards in 1980 was unsuccessful. But this early failure did not deter France. Like other European countries, France needed to reduce telecommunications transaction costs and smart cards showed potential to achieve such a reduction, as most transactions could be processed offline. French companies explored other potential uses of the cards. Cartes Bancaires, the French banking association, attempted to use smart card technology to reduce fraud by individuals who scanned traditional magnetic striped cards and copied this data to counterfeit credit cards. Its investment proved profitable. Credit card fraud rates in France dropped tenfold once the cards were in service. French financial institutions replaced magnetic stripe cards with smart cards in 1992. This resulted in a 75% reduction in credit card fraud over a five year period.

Why it's called as smart card: With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader.

Working process of smart cards: Smart contact cards work by inserting it into a card reader and with the contact pad carrying a memory chip where information is being stored, the card readers can read whatever is written on the card and allow the user to perform any transaction he intends to do.

Implementation of smart cards used by banks

Smart cards, such as debit cards, are often used with a Personal Identification Number (PIN). Organizations also use them for security purposes, as MFA tokens and for authenticating Single-Log-On (SSO) users and enabling pass wordless authentic. Example: The most common examples of contact smart cards are credit cards, ATM cards and SIM cards.

Different type of interface technologies used in smart card

The two primary types of smart card operating systems are 1) Fixed file structure and 2) Dynamic application system. As with all smartcard types, the selection of a card operating system depends on the application that the card is intended for.

Smart cards have two different types of interfaces: Contact and contactless. Contact smart cards are inserted into a smart card

reader, making physical contact with the reader. However, contactless smart cards have an embedded antenna inside the card, enabling communication with the reader without physical contact. As of 2017, there are more than 38 million active RSBY smart cards in India.

Types of smart cards

A smart card can be categorized as either a memory card or a processing enabled card. Memory card is the simplest form of a smart card. Such a card provides limited capability to securely store personal information. According to a smart card manufacturer, the currently available memory for memory cards ranges from eight bytes to 2KB, while traditional magnetic stripe based cards can store approximately 220 bytes of information. The storage on a memory card is non-volatile memory. Such cards are sometimes referred to as "asynchronous cards," since they are used offline and their associated flow of data is essentially one-directional: Value on the card is moved to the reader and/or the vendor's computer system). These are simple prepaid cards, which transfer the electronic equivalent of cash to a vendor's digital cash register. Transactions can then be directed to traditional bank account. Europe's phone card was the predecessor of this type of smart card. More sophisticated cards are the processor enabled smart cards some refer to as "true" smart cards, which are based on semiconductor technology. These smart chip cards contain a chip with a few hundred bytes of RAM. However, a pilot program in Japan is testing a 1MB flash memory card currently. These cards may also have special circuitry to perform cryptographic operations such as RSA public key encryption, signatures and verification. RSA public key encryption is named after its developers, Ronald Rivest, Adi Shamir and Leonard Adelman. The data stored on a smart card can be protected by active data encryption schemes along with biometric identification (fingerprints, for example), which can be used to uniquely identify the authorized user. Unlike magnetic stripe based cards, which can be compromised for the purpose of criminal activity, such smart cards are difficult to duplicate. These cards are sometimes referred to as "synchronous cards," as he data flow is bi directional: Data is read from, as well as written to the card. In general, smart cards support the storage of information that can be "read-only," "added-only," "updated-only," or not accessible.

To support on board data processing and sophisticated applications, processor enabled smart cards carry significantly more memory than their magnetic stripe based card counterparts. Current processor enabled cards can hold a maximum of 64 KB of user data, with a current capacity of 1 MB flash memory. Nippon Telegraph and Telephone (NTT), Sharp and the French smart card maker Gemplus developed and are currently using a multiapplication smart card with 1MB flash memory and the Nomadic Information sharing Network Architecture (NiNa) for application download/upload post issuance in Yokosuka City, Japan. It is the first 1 MB flash memory card. Both Gemplus and Bull report that data contained on a processor enabled card can be stored reliably for a maximum of 10 years. This beefed-up memory capacity allows a processor enabled smart card to function as a multiapplication card, combining functions of:

Credit card: Essentially an electronically extended credit for making purchases.

Debit card: Allows users access to cash, typically at a bank or ATM, through the use of a Personal Identification Number (PIN).

Stored value card: An initial step toward a cashless society. A fixed amount of value is electronically placed on the card. By using a reader, retailers can deduct the appropriate value from the card. In the case of a disposable card-a department store gift card, for example, the card is thrown away when the value has been reduced to zero. With a loadable version of a stored value card, additional value can be placed on the card with a reloading device, perhaps through an ATM kiosk.

Information management card: Contains personal information not necessarily related to consumer purchasing, such as health and emergency contact information.

Loyalty card: Accumulates points or credits toward some type of vendor reward (discount, products and services). Such a card allows for rewards to be taken at the point of sale. Some processors enabled multiapplication cards can now support electronic downloading of new applications. These newer cards, called "white cards" by some, are more expensive than memory cards.

Examples of downloadable applications include: Java based bytecode.

MULTOS: A highly secure, open standard that enhances the ability of smart cards to host applications was developed by a consortium of international organizations.

Basic card: This supports the creation of smart card based applications using the basic programming language.

Windows for smart cards which is Microsoft's standard for interfacing smart card technology with the windows operation system. The company describes it as "...an 8-bit, multiapplication operating system for smart cards with at least 8K of ROM" (www.microsoft.com/SMARTCARD/background.asp). Processor-enabled smart card software is stored in permanent non-volatile, read-only memory. Application data stored on the card is kept in EEPROM or Electronically Erasable Programmable Read Only Memory. The contents of this memory can be erased, and new data can be reloaded electronically. Such cards have an embedded silicon-based 8, 16, or 32-bit processor with even the 8-bit microprocessor based smart card almost as powerful as the desktop PCs of the early1980's. A cut away, side view of the component architecture of a processor-enabled smart card includes an electronic module (processor) and a silicon based integrated circuit, which are set into the surface of the card. The stacking order, from top to bottom.

Some of the possible components of an electronic module, which serves as the second layer of an embedded smart card processor chip. Depending on their intended capability, some chips may not include every possible type of memory. Security is increased and card size is minimized by combining all the depicted elements into one integrated chip.

The smart tools being used in India: For Driving License/ Vehicle Registration Certificate (DL/RC), Multi-purpose National Identity Card (MNIC), Rashtriya Swasthya Bima Yojana (RSBY) and electronic Passport (e-Passport) are jointly tested by NIC and STQC by using test tool and test script developed by IIT Kanpur.

- Contact smart cards.
- Contactless smart cards.
- Dual interface cards.
- Memory based smart cards.
- Microprocessor based smart cards.
- Hybrid smart card.

Smart banking systems and techniques

Programmed teller machines is the most utilized innovation in the expanding money related exchange of the current world. There are numerous conceivable methods to abuse ATM card utilizing PIN. Unique mark acknowledgment serves to accomplish a credible condition of security access through confirmation and approval. This paper distinguishes a high-level model for the adjustment of existing ATM frameworks utilizing both security conventions as PIN and biometric unique mark technique and GSM innovation. We have had the option to build up a unique finger impression system as a biometric measure to upgrade the security highlights of the ATM for viable banking.

Proposed system

There are two main phases in our system *i.e.,* enrolment phase and authentication phase.

Enrolment phase: Enrolment phase is also known as the registration phase. In this phase an individual registers his fingerprint using the fingerprint scanner and stores it into the database.

Authentication phase: In authentication phase, an individual is authenticated by matching the test image provided by him with the stored image *i.e.,* it is checked that he is who he claims to be.

Detailed working of the subunits is as follows:

Data collection unit: The most basic and equally important requirement for this stage is that of an optical sensor *i.e.,* r 305 optical scanner. The user fingerprints are collected in this unit. This unit adds a fingerprint of the user to database unit and further returns a byte every newly added ID. The return values range from 0x00 to 0xFE. The return code is 0xFF in case when there is an error, *i.e.,* no finger is placed on the sensor. Here 0xFF means error executing function.

Image pre-processing unit: The scanner takes input of the image then the pre-processing is done on the image in the scanner during the processing time, test image is in the form of analogue that is converted into digital form and if the quality of the pre-processed image is sufficient then the image is converted into the template.

Data storage unit: Each pre-processed image is of certain template size (approximately 512 bytes per template). And the template is stored into the database for further use. This unit allows the user to store the fingerprint data in the module and further configure it in 1:1 mode for storing an individual's fingerprint.

Search unit: A finger is placed on the fingerprint module (sensor) and the search function is called. The existing memory is then checked and returns a matching ID if found.

Decision unit: The system compares the input image with those stored in the database. The database image is stored after several processes, so it would be easier during transaction. Stored template and test image is compared and the needed resolution of the test image is 500 dpi (dot per inch). When the image comparison gets satisfied, then the user of the input is an authorized user.

Transaction unit: if the decision making unit authorizes the user, then the transaction is successfully carried out.

Empty function: This function is used to empty the database containing fingerprints stored in it. After executing this function, you will get following: 0xCC if operation was successful.

0xFF in case of error: There are various ways to authenticate the biometric data fed. Combination of biometric data along with the pin number is used to increase the security. Since the biometric data cannot be stolen or forged, the transaction would be safe and secured. While there may be chances for the pin number to be forged. The transaction time of the proposed system is about 10 seconds. This is achieved with greater care, as the clients desire and expect low transaction time [2].

Types of smart card applications

- Enterprise ID
- Financial
- Government
- Healthcare
- Identity
- Internet of Things (IoT)
- Telecommunications
- Transportation

Use of smart cards

Smart cards can provide personal identification, authentication, data storage and application processing. Applications include identification, finance, public transit, computer security, schools and healthcare. Smart cards can provide strong security authentication for Single Sign-On (SSO) within organizations. Intelligent cards, for example, are mostly intended for use as ATM cards or debit cards, using a Lock. Organizations also use it for security purposes, the cards can also be used to authenticate individual sign on users in addition to their use as multifactor automation tokens [3].

While by no means an exhaustive list, we have identified three categories of smart card applications: Authentication, authorization and transaction processing of authentication. Smart cards provide ample information to authenticate an individual's claim of personal identification using either token

based or knowledge based authentic approaches. Token based systems use an item such as a passport, driver's license, credit card or key for identification; while knowledge based systems tend to rely on memorized information such as PIN numbers or passwords.

High-tech smart card based driver's licenses not only serve as a means of identification but can also contain driving records and unpaid traffic fines. Potentially, new traffic offenses could be updated to a person's smart card within minutes of the offence, although such an application could present some interesting legal issues, depending on which country or state issued the license of authorization. As mentioned earlier, smart cards offer data encryption and the ability to store bio metric information for the purpose of authenticating the cardholder. Smart cards have the potential to facilitate the storage of demographic information for voting purposes and they are playing a growing role in the healthcare industry, which is experiencing a technological overhaul as electronic data management becomes more widespread and sophisticated. The smart card industry Association reports that over 80 million smart cards are currently used in Germany's healthcare system. France's Sesame Vitale program includes 10 million cards in its family plan and some 35 million individual cards. Smart cards could help automate and standardize patient demographic information on medical records, including those of insurance carriers. Smart cards with optical storage could store and transfer both text and image based medical records between patient and healthcare providers. These cards can also assist patients whose care depends on complicated equipment, such as kidney dialysis machines. Configuration for dialysis equipment, as well as medication information, could be stored on smart cards and inserted into a smart card-enabled dialysis machine anywhere in the world. Of course, privacy, technology, legal, and cost issues must be addressed before such health related applications become widespread. Smart cards could also facilitate drug prescription fulfilment. Prescription information could be loaded onto a smart card at the doctor's office and read by the pharmacist's reader for patient and doctor information, and dosage and replenishment specifications. With proper encryption, prescriptions could also be sent electronically from the doctor's office. Again, patients could have their card swept at the pharmacy for fulfilment. Payment terms can also be arranged through the card.

Processing of transactions: There are also numerous ways smart cards have the potential to assist in goods and service transactions, both in web based and traditional "brick and mortar" establishments. The cards could be reloaded with cash value in ATM machines and used as a credit card. The currency carried on a smart card could be used in different countries, as an electronic, multinational traveller's check. Smart card technology also provides a secure Internet-based payment mechanism through data encryption. The contactless version of a smart card is now used in situations requiring short transaction times, including issuing driving tickets and paying toll rates Smart cards are helping to expand the application of Global System for Mobile Communications (GSM) phones in regions such as Asia, Europe and South America. Using a smart card equipped with a Subscriber Identity Modules (SIM) chip, an individual subscriber can be identified and charged for services by his or her telecommunications system. The card can facilitate this identification through any GSM phone. The SIM chip can also store a subscriber's personalized electronic phonebook. Such an application represents a rapidly expanding segment of the smart card industry. Some GSM phones have two smart card slots, with the second slot allocated for an electronic wallet, thus allowing the mobile terminal to also serve as a "pocket ATM machine".

Voting is another type of transaction, but instead of having a basis in commerce; it is based on authorization as previously mentioned and information exchange. Smart cards have the capability of biometric based voter registration, using fingerprints, for example, which can help prevent voter fraud.

Standards of smart cards

A chip card is a standard size plastic debit or credit card that contains an embedded microchip as well as a traditional magnetic strip. The chip encrypts information to increase data security when making transactions at stores, terminals or Automated Telling Machines (ATMs). ATM cards are not credit cards or debit cards. ATM cards are payment card size and style plastic cards with a magnetic strip and/or a plastic smart card with a chip that contains a unique card number and some security information such as a expiration date or CVVC (CVV).

Smart card infrastructure and standards: Smart cards are generally placed in a special reading device for the duration of the transaction *i.e.*, reading from the card, processing, writing back to the card. While in the reader, the card's electrical contacts contact the readers' electrical connectors, through which data is read from and written to the card's chip. Standards help ensure smart cards can be read by any retailer equipped with a smart card reader. The reader also serves to provide the power necessary to retrieve, process and store information on the card. From a backend transaction processing perspective, purchases or credits made with a credit card are generally handled through an electronic connection between a vendor and a credit card company. Purchases made through a smart card's magnetic strip (if included) are processed much like a traditional credit card. However, due to the relative sophistication of a smart card's processor and memory chips, monetary value can be stored on and distributed directly from, the card. There is no need for validation through an online connection to a centralized database. Transaction related data can either be communicated to an organizational computer or simply collected by the smart card reader and later uploaded to a central computer as a batch process [4].

A contactless version of a smart card presented quite a technical challenge but was developed in 1998 in response to the need for cards to be read extremely quickly, such as when paying a highway toll fare. A contactless card contains none of the electrical contacts found on a contact based card. Instead of being slid through a reader, contactless cards access/transmit information through a transmission, such as a radio frequency, which originates from a special remote reading device. In addition, this transmission supplies the card with the power necessary to run the card's microprocessor. These cards, which

contain an internal antenna coil, can be read through an external antenna is a part of the remote reader, at a maximum distance of 10 centimetres. According to smart card manufacturer Gem plus, contactless cards can reduce the necessary transaction processing time by a factor of between 20 and 30, compared to the contact version, which must be placed in and out of a reader. The smart card chip is located near the edge of the card, both to protect the chip if the card is twisted or bent and to accommodate institutions that require a magnetic strip on the rear side of the card for backward compatibility to their credit/debit card systems. The Switzerland-based International Organize for standardization defines several specifications for smart card manufacturing, communication protocols and application/backend computer system. Among these are the following:

ISO 7816-1: Defines physical characteristics, including typical smart card size, which is 85.6 mm wide x 53.98 mm high x 0.76 mm thick. Amended in 1998.

ISO 7816-2: Defines location and size of the electronic contacts. Amended in 1998.

ISO 7816-3: Defines electrical signals and transmission protocol. On 1989 base it has been Amended in 1992, 1994, 1998.

ISO 7816-4: Defines, in part, the structure of stored files and communication protocols among applications Amended in 1998.

ISO 7816-7: Defines query language commands 1998.

Incidentally, smart cards are not limited to credit card sized pieces of plastic, although that form is the focus of this article. According to Gem plus, the two most common materials for manufacturing smart cards are Polyvinyl Chloride (PVC) and Acrylonitrile Butadiene Styrene (ABS), but smart card technology could also be applied to items such as key chains, decorative pins, lockets or belt buckles. Any such application that includes a smart chip must be integrated with existing readers to be economically feasible. ATMs are not designed to read key tags, for example, but could accept PVC or ABS-based, credit-card sized cards.

Development of smart card technology

One of the latest developments is the rollout of biometric technology. Visa and Mastercard have been active in this area: The visa ready scheme and the mastercard biometric card combine chip technology with fingerprints to verify the cardholder's identity for in-store purchases (Table 1).

RFID usages: Services using contactless smart card technology use RF technology, but, by design, operate at a short range (less than 4 inches) and can support the equivalent security capabilities of a contact smart card chip. RFID tags are used for inventory control or for Electronic Article Surveillance (EAS). Typically, the RFID inventory control tag has 96 bits or less while contactless smart cards have memory from 512 bits up to 72 Kbytes (and more). Contactless smart cards also have memory that can both be read from and written to.

Integrated Circuit (IC) microprocessor cards: Microprocessor cards (also generally referred to by the industry as "chip cards") offer greater memory storage and security of data than a traditional mag stripe card. Chip cards also can process data on the card.

EVM smart card: EMV cards are smart cards, also called chip cards, integrated circuit cards or IC cards, which store their data on integrated circuit chips, in addition to magnetic stripes for backward compatibility.

PIN: Smart card PIN is verification code that a smart card user must provide to confirm his/her authorization for using the card. In the tax core system, a smart card PIN is always a 4-digit code, selected by taxpayers when requesting each smart card.

Storage: This security takes the form of passwords allowing a user to access parts of the IC chip's memory or encryption/decryption measures that translate the bytes stored in memory into useful information. Smart cards typically hold 2,000 to 8,000 electronic bytes of data and its equivalent of several pages of data [5].

Table 1: Summary of best premium credit card ratings.

Company	Forbes advisor India rating	CTA text
Axis bank magnus credit card	4	View more
SBI elite credit card review	4	View more
Ultimate credit card	3.5	View more
HDFC Infinium credit card	3.5	-

Smart card application segments and sub-segments coverage

- Telecommunication
- National population register project
- Public distribution system
- Pay TV
- Loyalty cards
- Financial services: Credit /Debit cards, Financial inclusion, PAN cards.
- Travel identity: Driving license,Vehicle registration certificates, E-passports.
- Automated fare collection: Metro rail projects, Bus projects, Indian railways.
- Healthcare: Rashtriya Swasthya Bima Yojna, Other healthcare applications.

Focus of the analysis:

- Segment/Sub-segment overview.
- Smart card implementation scenario.
- Historical and future smart card volume demand.
- Historical and future smart card value demand.

The implemented research modules

Initial exploration of the Indian smart cards market: Conducted primary and secondary market research to complement/enhance our current knowledge and to identify key market segments and sub-segments.

Qualitative market research: Interviewed various industry stakeholders to gain a comprehensive insight into all major segments and sub segments. This included understanding key metrics and events such as smart card requirements, current and future demand, implementation timelines, success and risk factors, costs, etc.

Quantifying the current and future market potential: Consolidated our results to quantify the value and volume potential of smart cards in each segment and sub-segment.

Validating our results: Collaborated with industry stakeholders to validate our results and findings.

E-Banking in India

There are not many inventions that have changed the business of banking as quickly as the e-banking revolution. World over banks is reorienting their business strategies towards new opportunities offered by e-banking. E-banking has enabled banks to scale borders, change strategic behaviour and thus bring about new possibilities. E-banking has moved real banking behaviour closer to neoclassical economic theories of market functioning. Due to the absolute transparency of the market, customers (both business and retail) can compare the services of various banks more easily. If clients are not satisfied with the products, prices or services offered by a particular bank, they are able to change their banking partner much more easily than in the physical or actual bank client relationship.

Indian scenario-an overview: To cope with the pressures of growing competition, Indian commercial banks have adopted several initiatives and e-banking is one of them. The competition has been tough for the Public Sector Banks (PSBs), as the newly established private sector and foreign banks have already sharpened their competitive advantage. Some of the proactive PSBs have been struggling hard to make their structures flexible enough to accommodate technological changes. Adoption of technology has facilitated alternative channels for delivery within the PSBs and in turn, put pressure on them to restrict or limit the branch network and employ a better skilled workforce. E-banking, facilitated by the technological revolution, has strongly impacted strategic business considerations for Indian banks (including the PSBs) by reducing costs of delivery and transaction massively. In India, currently, there are two types of customers-one who is a multi-channel user and the other who still relies on the branch as the anchor channel. The primary challenge for banks is to provide consistent service to customers regardless of the type of channel they use. The channels broadly cover the primary canals of branch (i.e., teller, platform, ATM), telephone (ee, call centre, interactive voice response unit) and internet channel (e, personal computer, browser, wireless) banking.

Major concerns for Indian banks:

- First, in India, there is a risk of the emergence of a "digital divide" as the poor are excluded from the use of the internet and so from the financial system. Empirical evidence shows that richer countries possess higher concentrations of internet users (higher than income concentration) compared with poorer countries.
- Second, even today, the operating environment for public, private and foreign banks in the Indian financial system is quite different. However, the challenges before the public sector banks are plentiful and of a different kind. While, they have to handle volumes that are mind-blowing, there are also issues of legacy, old habits and political pressures.
- Third, confidentiality, integrity and authentication are very important features of the banking sector and were very successfully managed worldwide in pre-internet times.
- Fourth, e-banking has created many new challenges for bank management and regulatory and supervisory authorities. They originate not only from increased potential for cross-border transactions but also for domestic transaction based on technology applications that raise many security related issues.
- Fifth, there are some serious implications of international e-banking. It is a common argument that low transaction costs potentially make it much easier to conduct cross-border banking electronically. Sixth, there is no commercial bank in India, which has exclusively specialized in the small business segment. SMEs in India have generic problems such as the inability to provide quality data, to exhibit formal systems and practices and the lack of asset coverage.

State of E-banking regulations in India: Currently, there are three major statutes or guidelines governing e-finance operations within India, namely, the Information Technology Act, 2000; The Information Technology (Certificating Authorities) Rules 2000; and the Central Bank (Reserve Bank of India (RBI)) Guidelines on Internet Banking in India. The RBI guidelines have defined the operational framework on internet banking with a focus on security issues. Although the RBI has mandated that the commonly used PKI technology standard should be followed, no mandatory timeframe has been set for the same so far. However, the guidelines detail the organizational, operational and supervisory structures that banks will have to implement while offering internet banking. The IT. Act 2000 and the IT Rules for certificating authorities set the framework for the appointment of digital certification authorities, acceptance of digital signatures, etc., which would enable the orderly development of cyber business [6].

Exploiting E-banking in India for strategic advantage: No one would deny that electronic banking is the wave of the future. Although the practice of e-banking in India is quite limited, there is a huge potential for it given its impact on the cost and efficiency of financial intermediation. It may even be possible for them to leapfrog straight to the most advanced technologies.

They can put in place appropriate policies (especially regarding security aspects) before e-banking becomes widespread rather than reacting to it at the time of implementation. In this section, an attempt is made to see how India can exploit the ongoing e-banking wave to reap maximum possible benefits without incurring any major risks. As for the problem of a possible "digital divide", there is much one can learn from the experiences of other developing countries to include the poor within the net of e-banking. There is also a awareness that such large-scale computerization is not going to help in other operational areas such as back-office functions, Management Information Systems (MIS), fraud prevention, marketing and higher value added business. To avoid potential risks involved in cross-border e-banking, India can make a gradual start. For example, as suggested by Mathew and Nitsure, to begin with, Indian banks should seek benefits in the export of remote processing services for which they have developed comparative advantage in recent years.

RESULTS

International standard trends in E-banking

Although data on internet banking is scarce and differences in definitions make cross-country comparisons difficult, a preliminary analysis by the International Monetary Fund (IMF) shows that internet banking is widespread in Austria, Korea, the Scandinavian countries, Singapore, Spain and Switzerland, where more than 75 percent of all banks offer such services. The Scandinavian countries have the largest number of internet users, with up to one third of bank customers in Finland and Sweden taking advantage of e-banking. In the US, Internet banking is still concentrated in the largest banks. While most US consumers have accounts with banks that offer internet services, only about 6 percent of them use these services. As of today, most banks have combined the new electronic delivery channels with traditional brick and mortar branches, but a few that have emerged offer their products and services only through electronic distribution channels. These "virtual" or "internet only" banks do not have a branch network but may have a physical presence, for example, an administrative office or non-branch facilities such as ATMs. The US has about 30 virtual banks; Asia has two, launched in 2000 and 2001; and the European [7].

Challenges in E-Banking for developing countries

Based on best practices in developed countries, the United Nations Conference on Trade and Development (UNCTAD) report has identified four challenges that developing countries, in general, are expected to overcome to the advantages that e-banking initiatives can bring about.

The ability to adopt global technology to local requirements: An adequate level of infrastructure and human capacity building are required before developing countries can adopt the global technology for their local requirements.

The ability to strengthen public support for e-finance: Historically, most e-finance initiatives in developing countries have been the result of cooperative efforts between the private and public sectors.

The ability to create a necessary level of regulatory and institutional frameworks: The lack of regulatory frameworks, trust, security and privacy standards, high trade barriers, customer and investor protection hinder progress in implementing e-banking initiatives on a larger scale in many developing countries.

Review of related literature

Yerram Sneha: This paper manages the arrangements identified with the ATM (Automated Teller Machine) security. Today, ATMs and credit cards are utilized with the end goal of cash exchanges which assume a fundamental job in exchange. The shortcomings of existing validation plan, for example, secret key and PIN number caused the spillage of data put away in ATM smartcard which led to the loss of cash in ledger and private data abuses. To conquer this inadequacy of theft in cash exchanges, we propose the thought of utilizing fingerprints of clients as secret phrase included with conventional PIN number. After approved confirmation, the client will have the option to continue for exchange else after three progressive wrong endeavours, the ATM card will be obstructed for 24 hours and a message will be sent to the enlisted versatile number. Unique mark biometric of everyone is exceptional and unchangeable just as one of the well-known strategies for Savvy card security.

Katherine S: In their article, discussed various types of smart cards as well as current and emerging applications for the cards. We label as smart cards any credit card sized card with more memory than the traditional magnetic stripe, the common technology of credit cards and debit cards, but technically speaking, the "true" smart card has an on-board embedded processor or smart chip. Related technologies that also utilize microprocessor miniaturization include Dallas Semiconductor's. While our usage of the term is less than precise, this liberty is taken by many authors.

In 2001 financial years, 500,000 Federal cardholders spent nearly $14 billion *via* 24.4 million transactions using the smart pay smart card program. Hence, from their studies majority of the people aware about the use of smart card technologies and smart banking solutions.

Research methodology

To meet the objectives of this research, survey methodology was used to process the data. According to the relevance of the following elements, banking process, card details, customer details, processing works, types of conditions, purpose, acceptance to use smart card techniques, online usage platforms of smart cards, awareness of online transaction details and smart card usage learning systems, consciousness of various biometric techniques, retrieval of digital information related to the account, use to promote the new digital techniques and systems, uploading of customer documents (text, scanned, photos, other types), hosted or drawback information, withdraw facility details has been adapted to analyse and evaluated to find the result. There are 63 research articles quoted by the researchers related

to the smart card uses and techniques, Fakers' techniques, digital transformation, PIN usage, do not share PIN to unknown person. Be aware of PIN sharing information, system error and Faker's emergency address to update smart card and its various functions starting from 2011 to 2022. The researcher boasts that most of the articles are related to the smart card usage systems and awareness of online transaction and its management considered.

Need for the study

The smart card technologies or smart banking system are enabled to provide better service to the world community. The study observed that few considerable types of points mentioned below.

- To know the different types of technical requirement used by the user community.
- To know the majority reputed demanded online facilities used by customers.
- To know the interest of using smart banking environment and new learning techniques.
- To know the basic rules of the banking act.
- To know about the online banking rules of amount transformations within the group.
- To know the quick recovery of the amount and its selection of online transaction.
- To know the web portal facilities to learn specific bank related information that may help their banking databases related to their facilities for customer various purposes.
- To know the specific time, spend on the digital banking environments.
- To encourage cooperative efforts to save and use the online portal and various functions and structure of digital or online smart banking system.
- To know the advantages of smart banking systems for future development.
- Analysed the purpose of using this digital smart banking techniques and the importance of the online facilities provided by the private and government national or state government goals.
- To promote efficient delivery to all types of customers for their business and entrepreneurial growth and future development.
- To know other future requirements for digital or smart banking systems to utilize for online facilities to the customer categories and expert feedback to add new IT facilities for international development.

Objective of the study

In this study, the following hypotheses have been framed: Multi-type customers are interested in using online or digital smart card online banking facilities. School students to college graduates are using digital online and web banking environmental facilities for related to their various purposes. Experience business companies and facilitators are eager to use digital environmental facilities for digital smart card system for their business growth. The savings bank account holders feared about their security deposits. They are situated with the base of economic factors which helps to their lively hood live to eat. The multi-company business developers cited relevant corrigendum and tenders' facilities that have been announced by the banking sector to invest their amount for multiplication within a few days. The shareholders are waiting to procure the stack market shares which are down and will rise suddenly to give good benefits. It is the global activities for feature generation networks of high resolution and computer programming of the online banking system through digital card technology accessing, preserving, retrieving the digital account system and retrieve digitized data through their respective centres.

Data analysis and hypothesis formation

The researcher cited 63 documents out of 67 research papers, which have been published in various sites for the purpose of feature innovative services. Out of 67 research publications, 93% of the author or researchers studied about digital banking systems and they give assurance for digital Banking or online smart card systems through digital technologies. Low-level publications only related to faking techniques through mobile banking techniques or smart card using systems. Most of the studies are done and utilized for the creation of digital and IT related technical tools for new formation of new smart technology. The digital banking and smart card technologies are the backbone for every digital base innovation to discover new ideas for the future. From this study, the researcher analysed the null hypothesis, smart card system has more future and deliver the respective all kinds of services and information at any time for quick recovery to meet all types of customer demand at the end (Figures 1-3 and Tables 2,3) [8].

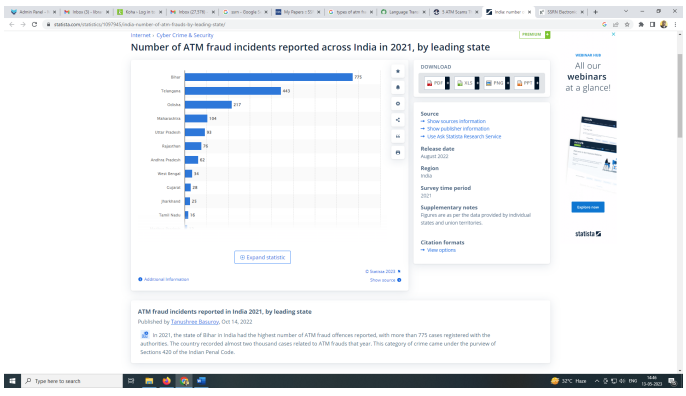

Figure 1: Number of ATM fraud incidents reported across India in 2021-2022.

Table 2: Transaction by smart card frauds (2021-2022).

ATM fraud's types global	Debit card fraud	Credit card fraud	ATM card theft	Cash withdrawal fraud	Exchange fraud	Bank related fraud	Synthetic account fraud	Loos of money in ATM	General fraud	Other fraud
Fraud ratio	25.27 million	38.97 million	14.14 million	48.97 million	38.98 million	34.78 million	4.5 billion	57.42 million	88.35 million	21.92 million
Overall fraud radio	28.58 billion	28.58 billion	28.58 billion	28.58 billion	28.58 billion	28.58 billion	28.58 billion	28.58 billion	28.58 billion	28.58 billion

Figure 2: Banking or online smart card.

Table 3: ATM frauds (2021-2022).

ATM fraud's types	Card trapping	Card skimming	Card jamming	Card phishing	Card steeling	SMS fraud	Program cracking	Other fraud
Fraud ratio	17.92	21.37	18.41	16.45	12.2	29.26	12.73	21.92
Overall fraud radio	32.2 billion	32.2 billion	32.2 billion	32.2 billion	32.2 billion	32.2 billion	32.2 billion	32.2 billion

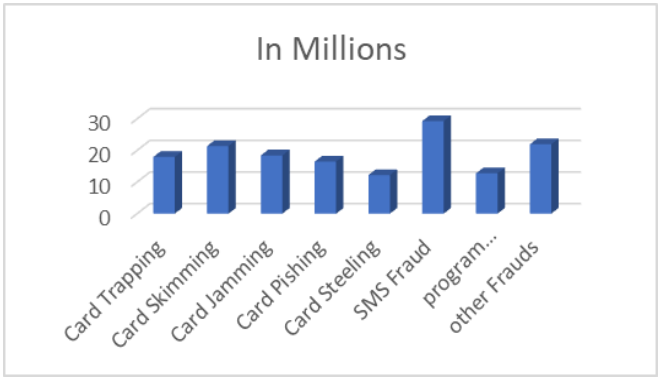

Figure 3: Types of ATM fraud.

Recommendation for security and future research

ATM security of the 21st century: ATMeye.iQ is an all in one ATM security, dispute handling and anti-fraud solution developed by BS/2, a software ATM security company, for banks and financial institutions. BS/2, part of the Penki Kontinentai Group has been a distributor for Diebold Nixdorf in 13 countries for over 25 years. BS/2 complies with strict financial industry regulations such as ISO-27001, ISO-20000 and ITIL V3.

Essential of ATM protections: Since 1967, when the first ATM was installed, these devices have changed significantly. Modern ATMs are not only used to accept and dispense banknotes but are full featured mini-offices of banks: They allow exchanging currency, obtaining loans and making deposits without visiting banks. Moreover, as technology develops, the methods of ATM fraud are also improving. According to ATMIA, cyber-attacks are primarily aimed at obtaining data from bank cards. Financial institutions use specialized software to protect ATMs. Modern solutions make it easier to resolve disputes and monitor ATMs, getting photos and videos in real-time.

Leading secure ATM solution: ATM eye.IQ is ATM software designed to ease the work of ATM security services. Easily secure your ATM network with real time video analysis, anti-skimming devices, facial recognition and various sensors.

Ease the work of your customer service: ATM eye.IQ ties every transaction to the ATM user making it easier to solve disputes. Effortlessly retrieve event footage from the integrated cameras, simply searching by card number.

Event based ATM alarm system: When various sensors detect malicious activity an immediate alert is sent. Security operators respond to threats or robberies with one click by launching configurable scenarios.

Preventing threats from card shimming: According to ATM security risks in Indonesia, skimming, shimming and other types of attacks are still relevant in the Asian countries. ATMeye.iQ in tandem with anti-skimming devices, prevents intruders from stealing card data.

All-in-one ATM protection system: Proactive monitoring: Currently, the most visible trend in banking security is the rise of ATM attacks. To solve these banks are demanding an all-in-one solution. Luckily, one such solution has already been developed.

The current state of ATM surveillance: Some banks have basic protection, like 24/7 real time surveillance and physical security. Unless banks implement a smart system, an operator must constantly supervise the situation. Furthermore, cameras that come with ATMs usually do not cover enough ground and are plain easy to cover. Reviewing video is a completely different issue. To resolve a conflict, responsible personnel must manually find the footage in question and analyse the situation. However, because most ATMs only have one portrait camera, it is usually not enough information to identify all the key points of the case.

A modern all-in-one solution: The ATM monitoring system ATMeye.iQ is a multivendor solution aimed at automating video surveillance. The essential difference in the approach to monitoring is that ATMeye.iQ only records relevant video. Thus, video storage is not overloaded with hours of video of ATMs in standby mode. ATMeye.iQ is a tool of proactive video surveillance. It has an array of security scenarios, which can be personally configured by the fleet operator. The system displays all information from the entire ATM fleet in an intuitive way on a single screen. As per emergency handling, event notifications are sent to the responsible staff through various delivery channels, such as SMS and e-mail.

All zones covered: ATMeye.iQ supports additional monitoring periphery installation. Extra cameras on the device permit the operator to monitor all device components, including the safe compartment, cash dispenser, card reader and PIN keyboard. Therefore, client disputes become much easier to handle. Banks are provided only with facts and evidence of every step taken by an ATM user. A range of sensors provided by BS/2 guarantee that tampering with the device in any way will not be left unnoticed. Enhance your ATM security with tilt, temperature, vibration (occurring when a device is being drilled, for instance) and other sensors. Detect ATM component malfunction, improper ATM handling, camera covering or other unusual activity and have responsible personnel react in real time.

Biometric ATM Solution: Compliance and access control: As more countries and regulatory bodies make face recognition a mandatory feature on ATMs, banks are rallying for a simple to implement solution. The big problem with adapting biometric solutions is the difficulty of implementation. It is a task that used to require an in-house team to create personalized software manually. In some cases, the entire production and deployment process could take several years. What is more, due to the task's complexity, software engineers often restrict functionality. Is a multivendor ready-to-use solution. It ensures full compliance with the latest AML and KYC regulations. By using ATMeye.iQ and its face recognition functionality, the bank can be aware of every ATM user. It provides two-factor authentication for bank card users. Biometric identification can also be used as a security measure when no other authentication means is available. However, its functionality is not limited to user authentication. ATMeye.iQ records all user actions, linking ATM processes with the user's identity, operation time and video footage. The feature that truly takes ATMeye.iQ on a whole new level of security is access control. The ATM network operator can create blacklists of cards with fraudulent activity. Upon identification, may trigger an array of security scenarios. Face recognition algorithms even make it possible to determine if a user has their face covered. An array of such security scripts renders the ATM protection proactive, ensuring that every emergency gets properly handled. Whitelists, on the other hand, are used to manage access of maintenance and CIT personnel. The ATM network operator can decide who has access to an ATM and when. Thus, ATMeye.iQ guarantees device protection from internal corruption [9].

ATM anti-skimming solution: IQ technology: Achieve unbreakable ATM security with ASM. Anti-skimming solution: Skimming is the most common type of ATM crime. Being the easiest one to implement, it is a major threat to ATM security, with bank clients being the main victim. Most banks struggle to even detect skimming, fortunately, BS/2 provides a proactive solution to prevent it.

State of affairs: Recent reports indicate that the number of ATM attacks is stably growing year over year. The Global Fraud and Security Survey of 2017 by ATMIA shows that 54 percent of the 10,500 individuals in the ATM industry reported an increase in ATM crime. The European Association for Secure Transactions (EAST) in its 200th fraud alert claims that skimming makes up half of all ATM attacks to date. Despite financial institutions being fully aware of the situation, they still struggle to tackle the issue. Essentially, skimming is the process of recording account data from the magnetic stripe of a card. To do so, a device must be placed on the card reader to scan the card. At the same time, a camera or a fake PIN pad captures the card's PIN number. The next step is data transmission, which is mostly performed *via* radio. To ensure ATM fraud prevention a bank must be able to detect when skimming is taking place. This task requires a complex approach to security not many can provide.

ATM security system with anti-skimming technology: ASM is a solution combining the surveillance system with anti-skimming technology. The advanced skimming protection solution will help battle skimmers at every step. ATM user actions. Any attempts of installing skimming equipment or covering a surveillance camera will immediately initiate security scenarios. The notification sent to the security personnel will have all relevant information, including the trigger description, exact event time and suspect photos. Should skimming equipment

ever be installed, the criminals will simply be unable to retrieve client information. ASM.ATMeye.iQ supports a variety of anti-skimming devices, including Optical Security Guard (OSG), white noise antennas, etc. Thus, any skimming equipment that is installed on an ATM is rendered harmless. Our security solution provides detailed reports of all skimming attempts for the chosen ATMs or the entire ATM network. Reports can be composed on request or based on a predefined schedule. Be aware of the weakest points of your fleet and be ready to act.

ATM grade security for parcel lockers and smart locker systems: The keyless locker market is expected to exceed $ 700 M by 2022; its state of security though, is still in its infancy. However postal related crimes around the world are only increasing. Criminals are always looking for new devices to exploit and unattended package lockers are a great target. These devices are just as, if not more, vulnerable than other self-service terminals. In 2018 in the US alone postal police officers responded to 841 incidents of violent crimes, making a total of 321 arrests. Electronic locker systems are fantastically comfortable and significantly ease the parcel delivery of over a million packages a week. Parcel pickup lockers are a great alternative to home package deliveries. As such, delivery lockers provide operators and mail carriers with some serious benefits to their supply chain:

- Bundling of parcels and packages.
- Saving on personnel costs of delivery carriers.
- Increased number of successful first time deliveries.
- Optimization of post office operation.
- Optimization of delivery routes.
- Lower operating costs.
- Improved asset management.

DISCUSSION

But just how secure locker systems really are? Currently parcel pick up lockers rely heavily on external security measures like CCTV cameras and local security officers. They are however not much different from other kinds of self-service devices and terminals. This presents lots of opportunities for criminals to break in physically or exploit the vulnerabilities of the parcel locker software. Luckily there is lots of experience that parcel locker deployers can borrow from ATM security and fraud prevention experts. ATM and self-service device operators have been in a constant battle with crafty criminals for ages. These criminals will try everything to get inside cash filled ATMs and get away with the loot. ATMeye.iQ is an all in one self-service device solution for security, fraud prevention and dispute resolution. Used by the banking industry world-wide for over 20 years, ATMeye.iQ can now serve as an effective digital lockers solution. Even though initially ATMeye.iQ was intended for ATMs it is well compatible with all kinds of self-service devices. ATMeye.iQ analyses the video stream in real time, ties photos and video recordings to events and can launch automatic scenarios. The proactive security system also works with a wide range of sensors to stop crime and instantly notify security personnel [10].

ATM monitoring

ATMeye.iQ is an all in one ATM Monitoring system, dispute handling and anti-fraud solution developed by BS/2, a software ATM security company, for banks and financial institutions. BS/2, part of the Penki Kontinentai Group, has been the partner of Diebold Nixdorf in 13 countries for over 25 years.
BS/2 complies with strict financial industry regulations such as ISO-27001, ISO-20000, PCI-DSS, PA-DSS, EcoVadis Silver and ITIL V3.

Classification of ATM monitoring systems: There are four monitoring management systems, they are:

- ATM software for monitoring.
- Boost ATM remote monitoring with remote file management.
- Monitor the ATM fleet on a single screen.
- Reduce ATM costs by decreasing ATM maintenance times.

ATM management system: Real time ATM monitoring and transaction analytics allows managers and tech teams to look deeper into network availability issues, security and failed customer interactions. It provides answers to why incidents are happening, analyzes their frequency, creates alerts and resolves issues more quickly. The ATMeye.iQ ATM Management System offers uninterrupted, fast and reliable link up with all banking systems to actively ensure client satisfaction. The ATMeye.iQ ATM management system can be linked to an unlimited number of terminals, in theory. In addition, you can use the system with devices of any manufacturer, installed anywhere in the world and remotely from each other. After all, IT solutions from ATMeye.iQ contribute to the stable operation of monitoring and control systems 24/7 in all situations. ATMeye.iQ uses state of the art solutions and technologies to ensure absolute control and security of ATMs:

- 24/7 audio, photo, and video recording.
- Monitoring of indicators by built in sensors.
- Automatic notification system in case of non-compliance.
- Protection against the installation of readers and the use of blacklisted cards.
- Automatic software updates and more.

Monitor and manage your ATM network: ATM networks operate 24/7, which requires constant monitoring and remote management to maintain stable performance. ATMeye.iQ's solutions optimize the monitoring and remote management of ATM networks, regardless of the size of the network or the distance between the devices. Software and hardware add-ons ensure that ATM networks run completely smoothly according to the latest security standards. Deployment of control and monitoring systems takes days.

Easily resolve ATM card disputes: Multi-level control and monitoring allow you to get a lot of data on ATM transactions in real time with archiving. This means that if a dispute arises, the client and the bank can immediately get the necessary information about the bank card and the transaction to quickly resolve the dispute.

React immediately with instant incident alerts: ATMeye.iQ's multi-layered ATM security and monitoring system works seamlessly 24/7 to immediately respond to various types of

external interference, break-ins, vandalism or installation of readers. The ATMeye.iQ monitor's rule-based framework flags monitor ATM transactions across multiple dimensions-transaction type, BIN range, customer type, merchant type, terminal ID as well as transaction volume and velocity. In the case of any suspicious action, the security service will be notified, which allows you to take the following steps to prevent illegal actions and protect the material assets of the ATM and the database.

ATM software for monitoring

TM software to monitor and manage your fleet remotely: The number of ATMs per 100,000 people doubled in the last 10 years and ATM physical attacks increased by 27% just this year. Government officials are urging ATM deployers all over the world to implement better solutions to ensure the safety of their self-service devices. Join 232 satisfied banks and ATM deployers in 80 countries and try the award-winning ATM system today. Made by the global ATM software company BS/2.

React to ATM crime in real time with this multi-function solution

Live video analysis with incident notifications: Analysing video in real time to detect threats and notify the ATM operator automatically. Footage analysed from portrait camera, card reader, cash dispenser and others.

Remote ATM software upgrade: Remotely update software, check the status of your self-service devices and much more.

Broad range of sensors for threat detection: With tampering, explosion, fire and other sensors your ATM operator receives notifications on any threat.

Accelerate dispute resolution

Easily retrieve event footage by ATM card number, time or device: ATMeye.iQ ties ATM transactions to the video footage of banking customers helping easily resolve ATM disputes.

One common interface for ATM system management: With ATMeye.iQ you can monitor all your ATM networks with just one customizable screen.

Remote file management: Simplify data management with secure file transfers between devices and workstations.

Supported devices

BS/2 is the part of the Penki Kontinentai Group. It specializes in IT outsourcing, software development, banking equipment supplies as well as system integration and technical maintenance services. The company has been working in banking technologies for 25 years; it is a partner of Diebold Nixdorf in 13 countries. BS/2 software solutions and services are being used in 80 countries around the world including the United States.

- Automated Teller Machine (ATM).
- Automated teller safe.
- Payment and info terminals.
- Ticket dispensers.
- Self-service gas stations.
- Other equipment.

Boost ATM remote monitoring with remote file management

Operation feedback and data processing is an essential element of cyber security in banking. As ATM monitoring becomes more available, most automated teller machine deployers still struggle with data management. RFM.iQ (Remote File Management) is an .iQ family product enabling a secure file transfer between self-service devices and the administrator workstation or data collection server. Here are three main features that make ATM data management convenient as never before.

Automated data collection: After initial device activation in the network, all file transfer jobs can be run remotely according to the predetermined schedule. The setup flexibility will grant the network operator any required report data. Information can be collected from a single ATM, groups of ATMs, as well as entire networks. As per the data itself, transfer jobs can be assigned for a specific date and time, file type and source directory. For example, incident reports can be prepared once a month, while photo and video logs can be backed up daily. RFM.iQ supports transferring any type of files, be it electronic journals, program logs, photos or video footage, making it the only file management platform an ATM fleet needs.

Relevant data archiving: The ATM security system ATMeye.iQ equipped with video content analysis. The system workflow is determined by contextual data received by a variety of sensors installed on the ATM. Video surveillance systems based on DVR allow real time monitoring, but the massive amounts of video of ATMs in standby mode make it costly to store. ATMeye.iQ, on the other hand, can distinguish when the ATM is in use. Post-record, pre-record and record on event features classify video information, allowing all irrelevant data to be disregarded. Therefore, the network operator can both monitor separate ATM machines in real time and easily retrieve relevant data from the archive for revision.

Remote updates: Using our software you can establish an encrypted TCP/IP connection of ATM networks with the ATMeye.iQ server. The benefit of such a connection is the possibility to exchange information both ways securely. Ensure that your version of ATMeye.iQ is up to date on the entire ATM fleet with a single mouse click. The connection can also be used to update security scenarios for entire networks or separate ATMs. Manual software support and maintenance simply become a thing of the past.

Monitor the ATM fleet on a single screen

The top 10 banks in the US have anywhere from 10 to 20 thousand ATMs, each requiring constant attention and monitoring. Traditionally, simple DVR methods of monitoring were employed, but they only helped to compose the events of the crime post factum. To actively identify an ongoing threat, operators at a bank would have to manually monitor hundreds

of screens. Forth comes ATMeye.iQ, a software solution to unify and proactively analyze video streams of entire ATM fleets.

One interface for all events: The ATM security software ATMeye.iQ unites the entire security infrastructure on a single screen. A security operator of a DVR video surveillance system is expected to supervise the entire facility in real time, over viewing dozens of video channels at once. With ATMeye.iQ operators monitor and manage the overall situation in form of statistics, with full access to real-time video if needed. The system gathers all information from the whole ATM fleet and displays it in an intuitive way on a single screen, presenting a complete picture of the operation of the entire system.

Proactive security: The security that ATMeye.iQ ensures is based on proactive monitoring. The ATM solution operates on relevant information received from ATMs. Pre-record, post-record and record on event features ensure that only relevant video footage is recorded. ATM surveillance is enhanced with video content analysis and face recognition. Modifiable security scenarios recognize any irregularities in device use, process sensor data and react immediately. The security operator is provided a detailed report with photo and video evidence in real time. Depending on the situation, the scenario may inform the authorities, capture the ATM card in a specialized card reader compartment or deny service. Event notifications are sent to the responsible staff through various delivery channels. Thus, routine scanning is avoided, and the reaction time is reduced.

Convenient data management: The ATM monitoring possibilities are further enhanced with ATMeye.iQ archiving functionality. All data is tied to a particular transaction, card number and date. Key card information is masked, ensuring the complete safety of client personal data. The system interface is intuitive and user friendly. A system operator can find a particular SSD using the device tree sort and narrow the data to a single ATM transaction. In addition, the status of a single automated teller machine can be checked using the same ATM monitoring software. A system operator receives information about the current operating status of all self-service devices in the network. It allows him to react faster in case of technical problems.

Reduce ATM costs by decreasing ATM maintenance times

It's widely known that millennials prefer digital, contactless and all online payments. And can we blame them? Why would anyone want to touch dirty cash that's been who knows where and touched by who knows how many people. Instead, it's much easier to whip out your phone or credit card and slide it over a contactless payment terminal. Or better yet, just scan a QR code for an instant transaction. The future is here and it's best seen in our everyday lives with the technological innovations in the payments industry. And yet somehow, surprisingly, the number of ATMs per capita only keeps growing. This means that financial institutions, ATM deployers, CIT and private ATM businesses are hard at work with ATM placement and ATM installation duties. If you think about it, there are now more automated teller machines at gas stations than ever before. With all of these ATM machines, ATM installation costs and ATM maintenance costs must be on every fleet owner's mind. Just how much cost an ATM machine can amount to? Depending on the types of ATMs in your fleet here is a breakdown of how much ATM machines cost:

- ATM processing fees.
- The cost to buy ATM machines.
- The personnel costs for monitoring and maintaining your fleet.
- Cash replenishment costs.
- Other ATM fees.
- Cost of physical and hacking attacks.

ATMeye.iQ the proactive ATM monitoring solution has quite a few useful features built in, to help decrease some of these ATM machine costs. ATMeye.iQ analyzes the video stream in real time, ties photos and video recordings to events and can launch automatic scenarios. The proactive security system also works with a wide range of sensors to stop crime and instantly notify security personnel.

ATM dispute resolution

Speed up the work of your support department and heighten your ATM fraud prevention: The most severe negative contact bank clients experience is the perceived sluggishness of support departments. Fraudulent transactions, stolen cards or other ATM disputes are problems that require swift and professional response. However usually this is not the case, disputes take days or even weeks to resolve. This is in part because ATM transactions aren't automatically tied to individuals making them. For example, Cyberabad police have found that 60% of the ATMs surveyed didn't have any cameras at all. We 've created our solution with this problem in mind. ATMeye.iQ ties each transaction with an image of the person performing it. This feature helps to optimize the operations of Bank Support Departments and significantly reduces resolution time for all ATM cases. The built in transaction monitoring system includes quick search by card number. This allows financial institutions to recognize the validity of the user's complaint and speed up the dispute resolution time, leading to a more satisfying user experience, which in turn boosts overall customer loyalty. Take your ATM monitoring to the next level and prevent ATM fraud with ATMeye.iQ. Whenever a user requests a charge-back for an ATM card transaction, you will know with absolute certainty who executed the transaction and who took the cash. If a user approaching the ATM covers camera, the responsible operative receives an immediate notification and can lock the ATM services or set up automatic scenarios. Any number of automatic scenarios can be performed, meaning it has never been easier to manage your ATM fleet.

Types of ATM fraud and fakers techniques

One of the world's largest crypto-asset exchanges is ready for you. Enjoy competitive fees and dedicated customer support while trading securely. You'll also have access to Binance tools that make it easier than ever to view your trade history, manage auto investments, view price charts and make conversions with zero

fees. Make an account for free and join millions of traders and investors on the global crypto market.

What is ATM fraud: ATM fraud is financial scams through these terminals. Just like any other hardware and software device, ATMs have vulnerabilities. To understand why ATMs attracts fraudsters, we should examine the components of an ATM machine. Any ATM has a computer and a safe. Breaking into the peripherals of the safe is often done with common lock picks. As a rule, ATMs operate under Windows. If the operating system becomes obsolete, it needs to be updated. Malware can be introduced *via* a portable device. Today there are 20 known strains of different ATM malware. Hacking into an ATM computer often allows criminals to give the device the command to dispense cash without using the users' card details.

Important: Many ATMs are characterized by weak firewall protection (the screen between the global Internet and an organization's local computer network). Such devices are more likely to be exposed to network attacks. ATM scam can provoke a lack of hard drive encryption and protection from users who have access to the Windows interface.

Types of ATM fraud: Many users think that physical machine robbery is the worst thing that can happen to an ATM. In recent years, however, ATM fraud has become even more diverse than before. Often, today's attackers don't have to be present when a machine attack occurs, ATM crimes are committed through a variety of techniques and types of fraud. Below we will talk about several types of ATM scams.

- Card shimming
- Card skimming
- Card trapping
- Jamming of keyboard
- Card pissing
- SMS fraud

Card shimming: Shimming is one of the most dangerous types of plastic card fraud. A shimmer is a thin board discreetly inserted into a card reader with a card carrier. As a result, the card is attached to contacts that read data from the magnetic stripe, without interfering with the normal bank card service. In this way, the fraudster gets all the information he needs and can empty someone else's bank accounts. Unlike relatively cumbersome skimming devices, shimmers are virtually invisible. Card shimming is used by fraudsters to steal users' personal data and perform illegal banking transactions.

Important: To avoid shimming, you should carefully check card reader slots. Have you noticed gaps or seams in the plastic? In this case, it is better to refuse to use a particular ATM. Among the necessary measures that operators use to prevent shimming are regular, thorough inspections of the machine, tracking bank transactions and monitoring and checking the vicinity of the card slot. Customers should be issued keys and codes to ensure maximum security of banking transactions. To avoid shimming, modern banks regularly update ATM hardware and software.

Card skimming: Skimming is a popular type of fraud. In this case, a hidden device is installed in an ATM, which gives the opportunity to read the information from payment cards during the ATM transaction. As a result, criminals create a card duplicate with a PIN code written on a magnetic strip. The card duplicate allows the criminals to make payments at various points of sale. If the card slot is sticking out, it may indicate the presence of an ATM skimmer. Skimmers are miniature devices attached to the main parts of the ATM.

Skimming equipment often contains:

- A magnetic head for data reading and copying.
- Miniature converter.
- A storage device for writing the code to the storage medium.
- Video camera.
- A keyboard, which is usually installed over the original keypad to transmit the entered information to the intruders.

To avoid becoming a victim of skimming, you should use ATMs located in banks and secure institutions. It is best to have a card with a chip, regularly check the data of payments in banking applications and if the card is missing, immediately call the bank to block it. In addition, many ATM users prefer to connect an SMS-informing service about card transactions, as well as to set the limit for disbursement of funds per day and per transaction.

Card trapping: Card trap is the placement of a device in an ATM card reader that prevents the cardholder from receiving the card after the machine transaction. The fraudster usually obtains the PIN number by means of a hidden video camera embedded inside a panel on the ATM. If the customer leaves without retrieving the card, the fraudster removes the payment instrument and then uses someone else's card to make payments or withdraw cash (Figure 4).

Figure 4: Card trap.

Jamming of keyboard: In this case, the fraudsters block important buttons on the ATM keypad (Cancel, Enter, etc.) to prevent the transaction from succeeding. Then, when the necessary data is entered, the criminal uses the ATM to withdraw cash. You should not go near the jammed ATM and use another ATM, because a skimming device may be installed on it. Quite often criminals disable other ATMs beforehand, to attract users to the one on which the skimming device is installed (Figure 5).

Figure 5: Close-up of someone making their secret code on the keypad of an ATM.

Phishing: Literally, phishing means stealing card details from the cardholder. This type of scam involves stealing passwords, credit card numbers, bank accounts and other sensitive information. Cybercriminals use personal information to gain access to accounts to which bank cards are linked, allowing them to steal money from their accounts. Quite often, fraudsters send emails on behalf of government agencies or well-known companies to steal personal data. The purpose of such emails is to make recipients follow the link provided in the email to a fake company website and enter their personal data (Figure 6).

Figure 6: Credit card hooked on a fishing hook concept for addiction to spending with credit or internet phishing crime.

SMS fraud: With this method user receive SMS-message suspicious content. The purpose of such a message is to make a person tell the fraudster the card details. The message may contain information about blocking the card. To unblock it, the fraudster may ask for detailed card details. Another way is to send a life-threatening message to a relative or friend of the cardholder. In this case the fraudster can get both money and card data. To protect yourself from SMS fraud you should not reply to suspicious messages. If fraudsters say that the card is blocked, it is best to call the bank's official hotline number (Figure 7).

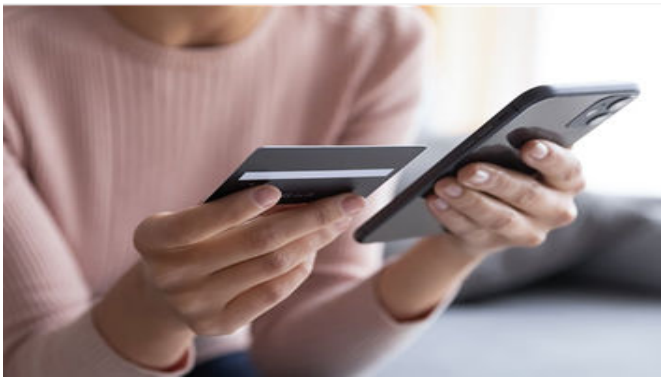

Figure 7: Close up female hands holding credit card and smartphone, young woman paying online, using banking service, entering information, shopping, is ordering in internet store.

How to prevent ATM fraud

Nowadays, ATMs are sophisticated computer systems that allow the use of various bank services. At the same time, fraudsters use more and more new methods to steal confidential information and money from bank cards. Here are a few tips to help avoid ATM scams (Figure 8).

- Choose ATMs that are well-lit and equipped with surveillance cameras. Avoid abandoned ATMs and terminals that have been vandalized.
- Before using a machine, inspect it, paying special attention to the presence of peripheral devices. Pull the card reader to make sure there are no additional devices. If you notice a suspicious device, you should not remove it yourself. It is best to call the bank. If you have already used the ATM and only after that suspect something, go to a safe place, report the incident to the bank and block the card.
- When entering the PIN-code, cover the keyboard regardless of the queue near the ATM.
- If you notice a suspicious person near the machine, do not confront him/her. If the behaviour of the person caused concern, contact the police.
- After withdrawing money from the ATM, you should quickly and discreetly remove the card, cash, and receipt.
- If you see that the person has forgotten to remove the card from the ATM, do not remove it yourself, as the scammer may later try to accuse you of theft.

Important: Do not under any circumstances disclose your card expiration date, bank message codes, PIN code or CVV and CVC code to anyone. Use complex passwords and two factor authentication, set a secure password in the banking application. Do not click on links from email, social networks and SMS if you are not sure about the credibility of the sender or if the message seems strange to you.

Figure 8: Reading and copying information from a magnetic chip.

ATM fraud cases: Skimming, which involves reading and copying information from a magnetic chip, is one of the most popular types of bank card fraud.

Below are a few cases of skimming in different countries:

- In October 2017, the Jordanian man was convicted in the United States of several years of skimming. Driving around Southern California cities, he placed magnetic stripe readers on ATMs and installed hidden video cameras within sight of ATMs. Over three years, the attacker stole financial information from more than 13,000 clients of Wells Fargo and other American banks.
- Quite often skimming is done by criminals from other countries. For example, at the end of 2017, Indian police detained two groups of Romanian citizens, who were paying attention not to studying the sights, but to installing skimming devices. As a result, more than 1,000 people lost about 6.6 million rupees.
- On January 10, 2018, FIA officers caught Chinese nationals attempting to install a skimming device and gain unauthorized access to the Pakistani ATM's information system.
- In 2018, it became known about skimming at the gas station in the U.S. city of Des Moines. Two criminals were charged with identity theft, identity fraud and credit card fraud.
- In May 2019, Brazilian nationals who installed hidden skimming devices and obscura cameras on Eastern Bank ATMs were sentenced in federal court in Boston.
- In 2021, two men were sentenced to 75 months in federal prison for ATM skimming fraud that resulted in $587,529.50 in losses to U.S. financial institutions.
- Faridabad County police arrested two men in 2021 for installing the skimming device and duplicate keypad at more than 30 ATMs in various Indian cities.
- In 2021, criminals who installed skimming devices at pumps at gas stations throughout the mid-atlantic region were brought before a U.S. court.

According to an EAST report, the number of attacks involving explosive devices at ATMs decreased in 2021 in Europe. Attacks involving ATM burglaries dropped 42%, while malware and logical attacks on ATMs dropped 74%. Most of the attacks were carried out using the black box method, which involves disconnecting the external casing of an ATM to gain access to its ports. In 2022, fraud is often perpetrated by initiating payments or withdrawals from victims' accounts. Gross card fraud losses are expected to exceed $49 billion by 2030 (Figure 9).

Figure 9: Hacker in ATM trying to steal pin code of woman's credit card.

As of 2022, there are more than 2.2 million ATMs worldwide. Because of their proliferation, people use ATMs without much thought. These days, however, ATM fraud protection means more than closing the keypad when entering a PIN. Many fraudsters hack into and break into ATMs to steal card and account information from users. Knowing the PIN code, criminals use the cards to instantly withdraw cash from the account. There are various methods an attacker can use to commit ATM fraud, but the action itself is about gaining access to a bank account and withdrawing funds from it. Modern banks use specialized software to protect against ATM fraud. One such solution is ATMeye.iQ. This universal advanced ATM video surveillance software provides protection against vandalism, robbery and fraud. The solution is designed to monitor incidents and has dedicated sensors to identify any suspicious activity. The installation of comprehensive solutions helps to recognize misconduct and ensures absolute security of ATMs.

Designed of smart card modules

Smart card view in Figure 10.

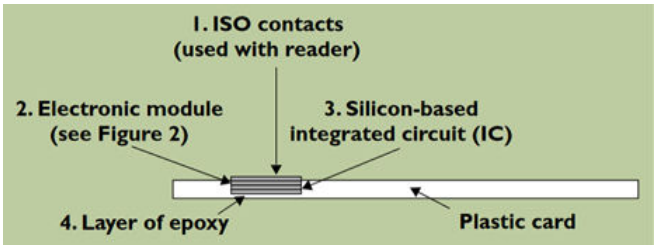

Figure 10: Cut-away view of smart card-top to bottom and side.

Evolution of smart card shows in Figures 11-13.

Year	Event
1968	2 German inventors patent combining plastic cards with micro chips [6]
1970	Arimura invents and patents in Japan [12]
1974	Roland Moreno invents and patents in France [12]
1976	French DGT initiative, Bull (France) first licenses [12]
1980	First trials in 3 French cities [12]
1982	First U.S. trials in North Dakota and New Jersey [12]
1996	First university campus deployment of chip cards [12]

Figure 11: Evolution of smart card.

Feature Component	Smart Card	
	Memory Card	Processor-Enable Card
Read Only Memory?	yes	yes
Random Access Memory?	no	yes
Microprocessor?	no	yes
Contact/Contactless Interface	contact, contactless or both	contact, contactless or both
Data certified secure (ITSEC*)?	no	yes
Example	phone card	multi-application cards

Figure 12: Memory versus process enabled smart card.

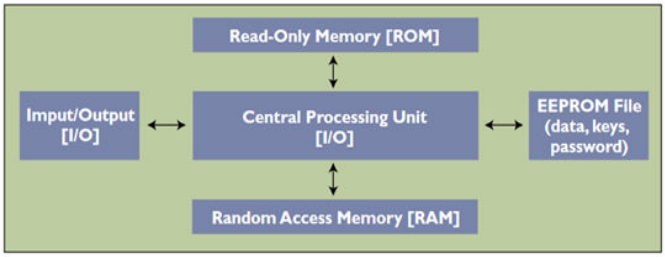

Figure 13: Architecture of smart card electronic module.

Biometric security systems

Today the ATM clients are increment in numbers. An Automated Teller Machine (ATM) is a modernized broadcast communications gadget that empowers the customers of any money related establishment to perform monetary exchanges like stores, moves and balance enquiries, scaled down explanation, withdrawal and quick money. The ATM machine has card reader and keys as info gadgets and show screen, money allocator, receipt printer, speaker as yield gadgets. ATMs are interfacing with a host processor, which is a typical portal through which different ATM systems become accessible to clients. Different banks, autonomous specialist organizations possessed this host processor. ATM card holder's sticks are not the same as every other. The number is confirming by the bank and enables the clients to get to their record. The secret word is just character so anybody can get to the record when they have the card and right secret word. When the card and the secret key is taken by the guilty party they can take more cash from the record in most limited period, it might carry gigantic monetary misfortunes to the clients.

Biometric innovation is the most broadly acknowledged and develop biometric technique and is the simplest to send and for a more elevated level of security. Utilizing biometric identifiers offers a few points of interest over conventional what's more, current strategies. It is easy tointroduce and furthermore it requires some investment and exertion to procure one's unique mark with a unique mark ID gadget. Accordingly, unique mark acknowledgment is considered among the least nosy of all biometric confirmation methods. Even though unique mark pictures are at first caught, the pictures are not put away any place in the framework. Rather, the fingerprints are changed over to formats from which the first fingerprints can't be reproduced; subsequently no abuse of framework is conceivable.

Fingerprint: Fingerprint is reliable biometric quality as it is an eccentric and committed. It is an innovation that is progressively utilized in different fields like legal sciences and security reason. The crucial goal of our framework is to make ATM exchange progressively secure and easy to understand. This framework replaces conventional ATM cards with unique mark. In this manner, there is no need to convey ATM cards to perform exchanges.

Card lass framework: The cash exchange can be made progressively secure without agonizing over the card to be lost. In our framework we are utilizing installed framework with biometrics *i.e.,* r305 sensor and UART microcontroller. The Fingerprint and the user ID of all clients is put away in the database. Fingerprints are utilized to distinguish whether the Person is authentic. A Fingerprint scanner is utilized to secure the unique finger impression of the person, after which the framework demands for the PIN (Personal Identification Number). The client gets three opportunities to get him validated. If the fingerprints don't match further confirmation will be required. After the check with the information put away in the framework database, the client is permitted to make exchanges.

Security operation framework: The principal goal of this framework is to build up a framework, which is utilized for ATM security applications. In these frameworks, bankers will gather the client fingerprints and versatile number while opening the records then client just access ATM machine. The working of these ATM machine is when client spot finger on the unique mark module when it gets to consequently creates each time diverse 4-digit code as a message to the portable of the approved client through GSM modem associated with the microcontroller. The code gotten by the client ought to be entered by squeezing the keys on the screen. After entering it checks whether it is a substantial one or not and permits the client further access.

ATM security framework: The fundamental target of this framework is to build up a framework that will expand the ATM security. Be that as it may, notwithstanding the various favorable circumstances of ATM framework, ATM misrepresentation has as of late turned out to be increasingly broad. In this paper, we give an outline of the conceivable fake exercises that might be executed against ATMs and research prescribed ways to deal with anticipate these kinds of frauds. Biometrics innovation is quickly advancing and offers appealing openings. As of late, biometric validation has developed in ubiquity as a method for individual distinguishing proof in ATM validation frameworks. An 8-piece ATmega16 microcontroller created by microchip technology is utilized in the framework. The fundamental programming is written in AVR studio developer and the framework is tried.

PIN security framework: The current ATM machine uses PIN-card as a security which is exceptionally powerless and simple to repudiate. This paper attempts to discover an answer for the above issues by bringing unique mark validation into the current ATM machine. A program model was intended to emulate an ordinary ATM framework that utilizations unique mark ID to improve the security of the ATMs. The proposed framework showed a three-level compositional structure. The check framework which focused on the enrolment, upgrade, includes extraction and coordinating of fingerprints. The backend database framework that fills in as stockroom of the formats of all ATM account holders' pre-enrolled fingerprints. The framework's stage makes related exchanges, for example, withdrawals, charge installment, purchasing of Visas and equalization enquiries and so forth. The outcomes got affirm that the present methodology could fundamentally diminish ATM misrepresentation if not thoroughly annihilate it.

Self-security systems

Over the last several decades, Automated Teller Machines (ATMs) have become commonplace, from bank lobbies to shopping centres to gas stations. As of 2022, there are more than 2.2 million ATMs around the world. As a result of their ubiquity, people casually use these virtual cash dispensers without a second thought. The notion that something could go wrong never crosses their minds. Unfortunately, things are not always as they seem at the ATM. Most ATM scams involve criminal theft of debit card numbers and Personal Identification Numbers (PINs) from the innocent users of these machines. There are several variations of this confidence scheme, but all involve the unknowing cooperation of the cardholders themselves. The first step in avoiding these schemes is to become aware of them. Let's explore some common ways people get ripped off at ATMs.

Key takeaways:

- ATM scams can involve stealing your debit card number or personal identification number.
- Popular scams that thieves use include using a counterfeit device for access to the door to the ATM and using a false façade on the front of the machine.
- Some criminals can swipe data from free-standing ATMs using cracking programs.
- Other forms of ATM scams include good old-fashioned stealing the entire ATM or placing a fake deposit receptacle at the ATM, and putting an “out of order” sign on the machine.

Every little thing it does is magic: One common scheme begins when a bank customer swipes their debit card in the device that opens the door to the ATM vestibule typically found in a bank's inner doorway. Because most people are unaware of precisely what this magnetic reader should look like, criminals can place a counterfeit device that reads and copies card numbers on the outside door without being detected by customers. Once the customer is inside, a hidden surveillance camera records PINs as customers enter them on the ATM keyboard. The result of this information gathering is the illegal creation of a duplicate card that thieves quickly use to withdraw all the funds in the connected bank accounts as quickly as possible. Detection of this fraud is difficult for the average consumer as there are several dozen manufacturers of legitimate swiping devices. Attempting to distinguish a real one from a fake is almost impossible.

Don't stand so close to me: Another method of trickery involves the attachment of a false façade over the ATM machine. Though the machine looks normal the attachment will "eat" your card and display an error message. Your PIN is usually recorded by a hidden camera or in some cases, by a "helpful" person standing nearby who suggests that you try to enter your PIN again. Of course, this person is a criminal, and moments after you leave, they will retrieve your card from the false front of the ATM and walk away with both your card and the access code. Other times, an overlay will "skim" the card without destroying it, collecting its information along with the pin code and other data you may enter. For the user, it appears to be a normal transaction, but the thieves now have your card number. In 2021, for instance, the FBI identified an ATM skimming fraud of almost $600,000 throughout the midwest.

Ghosts in the machines: Freestanding ATMs are also subject to criminal activity. These devices are in areas as varied as airport terminals and self-service gasoline pumps. In some situations, criminal hackers are able to capture account information by using Wi-Fi scanners and cracking programs to download transaction data when the systems fail to be protected by high-level encryption software. The most audacious of ATM scams is the installation of machines whose only purpose is to steal information. This criminal confidence scheme was once a popular activity of organized crime circles. Seemingly normal ATMs would be placed in small shops, bars and other venues. The machines were never actually loaded with funds, but instead were there solely to entice users to swipe their cards and enter their PINs. After collecting this information, an error message would appear. These seemingly innocent devices provided criminals with a steady flow of stolen banking information. Because of their placement in high-traffic areas, users did not realize that all users were unsuccessful at withdrawing funds.

Making the best of what's around: An old-fashioned scam that still reaps profits for criminals is the placement of a deposit receptacle in an ATM vestibule with a sign over the automated machine stating it is out of order. Here, the scammer's goal is to capture cash deposits that were intended for the more secure electronic banking machine. While it may seem obvious that depositing money in this unsecured fashion is a bad idea, the comfort and trust that people have when entering a financial institution often allows them to suspend their suspicions as they believe that there is no safer place than a bank.

Demolition men: Finally, criminals who are too impatient to go through the complex process of stealing bank accounts and personal identification numbers will simply steal an entire ATM. Typically, this crime occurs in the overnight hours inside a business, such as a supermarket. The thieves will break-in, use the store's forklift (which is normally used for the benign purpose of moving cases of beer and soda) to rip the ATM off the floor and load it onto a waiting truck. As a fully loaded ATM can hold tens of thousands of dollars, these have become prime targets 52.

Other information for safety and security

Bitcoin ATMs: Bitcoin ATMs are terminals or kiosks where individuals can anonymously buy or sell bitcoins electronically. Even though they are connected to the internet, experts agree that today's bitcoin ATMs are safe since they use high-level encryption. Moreover, bitcoin itself uses a public-private key pair, and nobody can steal or move your bitcoins without your personal private key. The machines are also built with safeguards against physical or hardware malfunction as well as software protections against malware.

PIN threats: Will Entering My PIN # Backwards alert the authorities to a possible threat? No. despite the prevailing urban myth, entering your PIN in reverse (or in any other combination) will not alert the police or the bank. This idea gained popularity in the mid-2000's through the 2010's as viral social media posts suggested this emergency measure. However, it has been confirmed to be false.

The bottom line: Don't let a simple transaction like withdrawing money from an ATM be a way for thieves to get the best of you. To avoid scams like these, listen to the cautionary voices in your head and be careful when something seems amiss. Even in what seems like normal circumstances, shield the keyboard with your other hand when entering your PIN-it's no fun to be driven to tears by a crime you could have prevented. And of course, if you spot a scam in action, don't apprehend the criminals yourself-let the police deal with that.

Techniques to avoid smart card frauds

There is nothing to be afraid of. Here are some of the tips that you should follow to steer clear of credit card fraud. Some techniques are classified to avoid smart card frauds. They are:

- Ways to avoid credit card fraud?
- How to detect credit card fraud?
- How to report credit card fraud?
- What should you do if you are a victim of credit card fraud?

Ways to avoid credit card fraud

Keep your card safe: The primary step is to keep your card in a safe place so that it is not easily accessible to others. After swiping your credit card, always check if the magnetic strip or back of the card is hampered in any way.

Monitor online transaction: Most banks send an alert SMS after every online transaction. Another way of tracking your transactions is by installing your bank's app. It helps you check your account balance and other details whenever needed.

Review billing statements: To prevent different types of credit card fraud, one basic thing you should do is review your billing statements. This will allow you to note if any unknown or unauthorised transaction has been reported.

Avoid paper trials: Another easy step that can prevent credit card scams is by shredding your billing statements. Credit card statements generally contain the full credit card number, so when you want to discard them, ensure shredding the document.

Signing blank receipts: While signing credit card receipts, ensure the amount is verified. If you notice any blank spaces, make sure to cross-check with your bank regarding this.

Never make it public: Your credit card details are very sensitive, so always beware of phishing. You must never share your card number, CVV or PIN through any text messages. Keep it memorised and keep changing it after an interval.

Always double check: Scammers can mimic a bank or business' logo that requires personal information. So, it is better to always double check the website or merchant prior to purchasing. If you feel there is any discrepancy, do not complete your payment details.

Report lost/stolen card: Suppose your wallet was lost or stolen and it contained your credit card. Your first step regarding this is to report and block your card as soon as possible. You must always keep the customer service number of your credit card company in your contacts so that you can immediately report the incident.

Create strong pins and passwords: Avoid using a birthdate, anniversary date or contact number as your credit card PIN or password. As most website suggests, you must combine the following to create a responsible password.

- Upper case characters
- Lower case characters
- A special character
- A numerical digit

Using RFID blocking wallets: Contactless cards are embedded with an RFID chip that allows smoother transactions. However, any fraudster can scan the RFID data while standing beside you. This is why it is recommended to invest in an RFID blocking wallet so that your cards become more difficult for scammers.

How to detect credit card fraud

If you regularly follow your monthly credit card statements and credit reports, it is possible to detect any scam at its early stage. However, if the situation has already worsened, you might need the help of professionals. Listed below are some of the popular techniques which experts use to detect credit card fraud.

- Decision tree method
- Clustering technique
- Neural networks
- Genetic algorithm
- Naive Bayes classifiers
- Outlier models
- K-Nearest Neighbour (KNN) algorithms
- Support Vector Machines (SVMs)
- Bagging ensemble classifier
- Global profiling

How to report credit card fraud

The process of reporting scams can differ in different banks. The next section lists down the process followed by certain popular banks. You can also directly let the Reserve Bank of

India know about the type of credit card fraud you are a victim of. Just give a missed call to 14440.

State Bank of India (SBI): Type BLOCK followed by the last four digits of your credit card and send this SMS to 5676791. You can also call the customer service number of SBI and report the same, which is (prefix local STD code) 39 02 02 02 or 1860 180 1290.

Axis bank: Call 1860 419 5555, Axis Bank's credit card customer support and report the incident. You can also visit the nearest branch to report the same.

IDBI bank: You can report any such scams by calling 1800 425 7600 (toll-free) or +91-022-4042 6013 (non-toll-free). Additionally, you can also write to idbicards@idbi.co.in to let them know about such fraud.

HDFC bank: You must also call on their toll-free number, 18002586161, to report if any fraudulent activities are noted.

- Step 1: Log in to your HDFC net banking portal.
- Step 2: Click on the tab marked "Card".
- Step 3: Click "Request" below the credit cards section.
- Step 4: Select "Credit card hotlisting" and put the details of your card.

IndusInd Bank

- Step 1: Log in to the IndusNet portal or its app.
- Step 2: Select "Service Request".
- Step 3: Click on "Credit Card Requests".
- Step 4: Select "Credit Card Blocking Request".
- Step 5: Click on the card you want to block.
- Step 6: Click on "Submit".

Citibank

- Step 1: Log in to the bank's website.
- Step 2: Click on "Credit Card".
- Step 3: Select the card you want to report.
- Step 4: Click on "Account Statement".
- Step 5: Choose "Dispute".
- Step 6: Select the fraudulent transaction.

Punjab National bank: You can call the toll-free number 18001802345 or 0120–4616200 to list your credit card fraud. Another way is to simply send them an email with all the details at creditcardpnb@pnb.co.in.

In case you are unable to do any of these processes, try sending the bank an SMS (HOT>space>card number) to 5607040 from your registered mobile number.

Indian bank: Type <BLOCK> and send an SMS to 092310 00001 or 092895 92895 to block your credit card.

Bank of India: Hotlist your credit card number by calling customer support on this toll-free number 1800 220 088. If you cannot reach this number, try their landline number (022) 40426005/40426006. You can also report theft or scam *via* an email to headoffice.cpdcreditcard@bankofindia.co.in and request to block your card.

What should you do if you are a victim of credit card fraud

Suppose you have detected that you are a victim of a certain type of credit card scam. Your next step would be to report the incident. Here is a step-by-step guide that will help you complete the general procedure.

- Step 1: Call your credit card company and let them know about the incident.
- Step 2: Meanwhile, reset your PINs and passwords.
- Step 3: File a General Diary at your nearest police station.
- Step 4: Keep an eye on your credit card statements.
- Step 5: Monitor your e-commerce websites for any unauthorised purchase.

Situations like this are very difficult, but losing your temper is not the solution. As you must perform a series of procedures to report the incident. Here are some things to remember when reporting a scam.

- Take screenshots of the SMS/ email you get after reporting to the bank.
- Ask the bank to provide a complaint reference number.
- Record your conversation with the bank.
- Follow up the call with an email mentioning the reference number.

Being a victim of any kind of credit card scam is very common these days. Hence it is necessary to keep yourself updated with the process of reporting such crimes. As you have completed this piece here, you are now familiar with the types of credit card fraud, the process of detecting them and other related information. If you stay careful and observant, you can easily dodge fraudulent situations like these.

CONCLUSION

Smart cards have the potential to contribute greatly to the "integration of commercial transactions-data warehousing and data mining". These cards support an impressive variety of applications at present and this variety should expand as the cards become smaller, cheaper and more power. At least for the foreseeable future, we believe smart card technological advances are likely to outlaw legal and ethical concerns, although more Research on privacy and security is needed before universal cards are used. We know of one senior scientist with extensive expertise in smart card technology that has indicated its serious reserve-combination of varied information, such as financial, health and employment information on the single card. As with other technologies that facilitate electronic exchange of information, including the web, email and organizational network-based communication, issues involving privacy, legality and ethics must be fully addressed before smart cards can really take off. The e-banking revolution has fundamentally changed the business of banking by scaling borders and bringing about new opportunities. Also in India, it has strongly impacted the strategic business considerations for banks (including the PSBs) by significantly reducing costs of delivery and transactions. It must be noted, however, that while e-banking provides many benefits to customers and banks, it also aggravates traditional

banking risks. Compared to developed countries, developing countries face many obstacles that affect the successful implementation of e-banking initiatives. In this paper, we have identified some such obstacles in the Indian context and have suggested ways to overcome them to move forward with the wave of e-banking successfully. In India there is a major risk of the emergence of a digital divide as the poor are excluded from the internet and so from the financial system. Even today, the operating environment for public, private and foreign banks in the Indian financial system is quite different. To avoid the risks involved in cross-border e-banking, India can make a gradual start, first by seeking benefits in the export of remote processing services in which it has a strong comparative advantage. In the case of SME-financing, it is strongly felt that after acquiring the necessary technical capabilities, PSBs are better positioned to provide value propositions to SMEs given their comparatively extensive branching networks, close relationship with business clients and a good knowledge of their needs, requirements and cash positions. This offers them another growth channel unmatched by most private players.

REFERENCES

1. Thangavel V. Global Identification of Smart Card Technologies-Safe and Secure: A Research. 2023.
2. Shelfer KM, Procaccino JD. Smart card evolution. Commun ACM. 2002;45(7):83-88.
3. Sneha Y, Sivalenka V. An epic technique to improve the security of ATM Utilizing Biometrics. J Interdiscip Cycle Res. 2020.
4. Omari RK. An assessment of the use of Automated Teller Machine (ATM) of Barclays Bank Ghana Limited Akim Oda Branch (Doctoral dissertation).
5. Schacklett M. These business trends will shape the future of e-commerce. Union Magazine. 2000:14-15.
6. Ravikumar S, Vaidyanathan S, Thamotharan S, Ramakrishan S. A new business model for ATM transaction security using fingerprint recognition. Int J Eng technol. 2013;5(3):2041-2047.
7. Petrlic R, Sorge C. Establishing user trust in automated teller machine integrity. IET Inf Secur. 2014;8(2):132-139.
8. Onyesolu MO, Ezeani IM. ATM security using fingerprint biometric identifer: An investigative study. Int J Adv Comput Sci Appl. 2012; 3(4):68-72.
9. Dutta M, Psyche KK, Yasmin S. ATM transaction security using fingerprint recognition. Am J Eng Res. 2017;6(8):2320-0847.
10. Sneha Y, SIVALENKA V. An epic technique to improve the security of ATM Utilizing Biometrics. J Interdiscip Cycle Res. 2020;9(10):532.