AN AUTOMATED TELLER MACHINE

A PROJECT REPORT

Submitted by

Akansh Arya (22BDO10027)
Krishna Sharma (22BDO10029)
Ayush Pandey (22BDO10038)
Adarsh Kumar Singh (22BDO10053)

in partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE ENGINEERING IN DEVOPS

Chandigarh University

APRIL 2024

BONAFIDE CERTIFICATE

Certified that this project report "**AN AUTOMATED TELLER MACHINE"** is the bonafide work of "**Akansh Arya (22BDO10027), Krishna Sharma (22BDO10029), Ayush Pandey (22BDO10038), Adarsh Kumar Singh (22BDO10053)"** who carried out the project work under my/our supervision.

SIGNATURE

HEAD OF THE DEPARTMENT

Aman Kaushik

SIGNATURE

SUPERVISOR

Tejinder Pal Singh (E16552)
Professor
AIT-CSE

Submitted for the project viva-voce examination held on:

INTERNAL EXAMINER

EXTERNAL EXAMINER

Table of Contents

List of Figures

List of Tables

Abstract

In our paper, we delve into the critical aspects of Automated Teller Machine (ATM) management, including cash forecasting, security measures, user-friendliness, and more. We explore various challenges such as predicting cash demand, detecting fraud, addressing ATM failures, optimizing user interfaces, determining replenishment strategies, selecting optimal ATM locations, and understanding customer behaviour. We specifically focus on leveraging Artificial Intelligence (AI) techniques for tasks like fraud detection, failure prediction, and replenishment planning. Additionally, we discuss several statistical methods utilized for evaluating these forecasts. Throughout the paper, we examine AI methodologies such as neural networks, regressions, and support vector machines, illustrating their outcomes through graphical representations across different sections. We review relevant literature spanning the past decade (2006–2016) and compare the effectiveness of various approaches based on factors like dataset characteristics and prediction accuracy. Furthermore, we compile a list of datasets accessible to researchers in this domain to facilitate further investigation. Lastly, we highlight unresolved issues and outline potential avenues for future research in each of the discussed areas. Data security is the critical problem in the current scenario of banking and financial institution. So primary criteria to design this system to provide the security for data which is transmitted during the ATM transaction. In this paper we will discuss the two kind of mechanism which is used for the ATM transaction. In the first mechanism while data transmission it will be in the encrypted form then unauthorized user can't access it. And in the second mechanism is Light Fidelity (Li-Fi), remove the issue of the slow rate of data transmission. In this paper define concept of Li-Fi on ATM transaction. As suggested by germen physicist Harald Haas It is the technique to taking the fibber out of fiber optic by sending data through an LED light bulb that is used to flickers the intensity of light faster than the human eye.

CHAPTER 01 - INTRODUCTION

1.1 Introduction:

Automatic Teller Machines (ATMs) are computerized devices facilitating financial transactions without human assistance in public spaces. As reported by ATMIA, there were approximately 1.6 million ATMs worldwide in 2007, primarily financed and managed by financial institutions. These machines offer customers convenient access to financial services with minimal human involvement [1]. ATM management involves various predictive tasks such as cash management, fraud detection, and understanding customer behavior, enabling organizations to enhance planning and service delivery. This is particularly crucial in the competitive landscape of financial institutions striving to attract investments and offer cost-effective services. In Section 2 of our discussion, we categorize the paper into seven main areas: forecasting cash demand, fraud detection, ATM failure, user interface, replenishment strategy, ATM location, and customer behavior.

We deal into data sets, where we introduce and analyze several data sets, examining their specifications and features The paper introduces AI techniques utilized in ATM management prediction. The literature is organized based on these techniques, and we aim to comprehensively review these studies, analyzing various aspects to offer valuable insights for researchers interested in this domain. In this paper proposed an idea using the Encrypted Li-Fi Communication. In this technique we transmit data through Li-fi [1] and data is in the encrypted form then no one can’t easily predict it. Encryption techniques used to convert the simple text in the unreadable code by using a suitable algorithm. Different type Encryption algorithm provides the different level security. Li-Fi used as a bidirectional, high-speed network for wireless communication, using visible light

communication (VLC). And VLC used for indoor communication by switching LED ON/OFF.

In today's business world, every individual wants to develop and expand their businesses. To sustain their business in the existing modern and globalised world, people in business employ smart work to achieve their common goal of fast growth and huge profits. The financial service sector is one of the major fastest growing industries in the world economy. The development of the financial sector in a country is critically necessary for the rapid growth of the economy. The growth of the financial sector is dependent on the progress of various intermediary banking and non-banking institutions existing in the country. Hence there is a prerequisite for banking sectors to divert their objectives from their existing goal of consistent profits to growth-oriented, future plans. This can be achieved by the banking sector by adopting technology in the business which will result in innovation. One such innovation in the banking sector is automated teller machine (ATM) which is widely accepted by all banks. Even though technological developments like mobile banking and internet banking have helped in completely reforming the banking sector.

Fig 01. Existing ATM transaction system

ATMs remain to be an important factor in the sector. Raj (2018). The Indian financial system is the most massive growing sector in the country. The country has adopted technological innovation on a regular basis to implement change in its business. ATM plays an essential role in India especially when the country is trying to achieve the status of complete financial inclusion. The evolution and the development can be implemented successfully only when the customer is supportive and satisfied. The customer satisfaction can be achieved only when the bank premises gratify the expectation of the customer through their user friendly, solution seeking ideas which can be better achieved through technology rather than their bank employees. This paper throws light on the recent development and growth in ATMs in the Indian financial sector[2].

1.2 Objective of the study:

- The main objective of this study is to analyse the satisfaction of ATM users. The specific objective of this study is to understand how people perceive the ATM facility.
- There has been extensive research on the ATM in the world. Many regional and nationwide similar studies can be found. Even few papers explored the ATM on Nepalese case. However, the issue of ATM service is new one and very less explored. In case of Nepal no research has been conducted on the area of all age groups.
- Therefore, this study contributes how people perceive ATM in terms of usefulness. The main aim of this study is to analyze the satisfaction of ATM users. Once the study will be completed, it would be highly useful to the related institutions and individuals.
- Designing of a software that reads an ATM card and display for interaction with the customer, a cash dispenser in multiples of Rs 100, Rs 200 and Rs 500 to dispense money, a printer for printing customer receipts.

- Implementing data encryption between the ATM and the processing center, preventing arbitrary code execution, and safeguarding against network attacks targeting ATM transactions. Additionally, securing communication with the card reader, encrypting card data, and adhering to best practices outlined in the report are essential to mitigate card data theft.
- To develop a framework or guidelines for integrating advanced authentication technologies into ATM systems while ensuring usability, reliability, and compliance with regulatory requirements.
- To explore and evaluate advanced authentication technologies such as biometrics (e.g., fingerprint scanning, facial recognition) and token-based authentication (e.g., dynamic CVV) for their suitability in ATM environments.

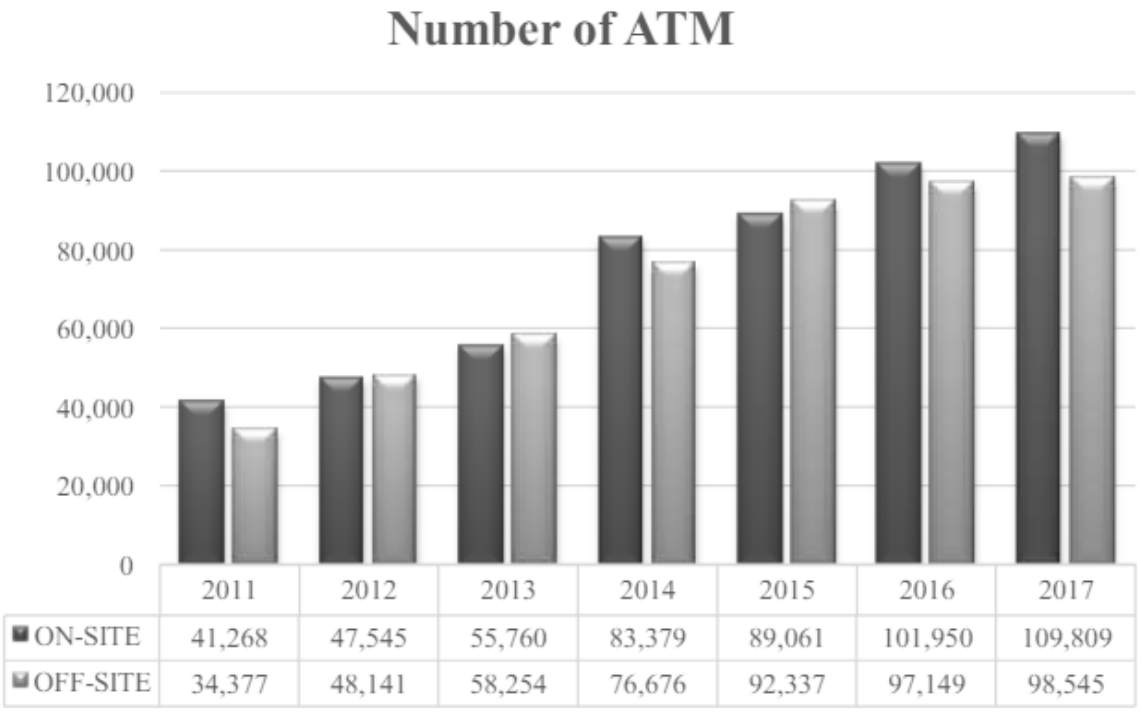
1.3 Growth of ATMs:

Automated teller machines or ATMs is one of the most popular and notable banking products resulting from innovation in information and communication technology. Automated Banking Machine (ABM) or Cash Machine are other synonyms for ATM. Use of ATMs not only assisted banks in extending their banking services, it also provided convenience and ease to customers [3]. The RBI database regarding ATM installation for the past eight years for the month of March is given below in Table

YEAR	ON-SITE	OFF-SITE
2011	41,268	34,377
2012	47,545	48,141
2013	55,760	58,254
2014	83,379	76,676
2015	89,061	92,337
2016	1,01,950	97,149
2017	1,09,809	98,545

Table 01. Number of ATMs a/c to its type.

The above table gives details about the number of ATMs available in India. As per the table during 2011 (March) only 41,268 onsite ATM and 34,377 offsite ATM were present. But according to the latest report of March 2017The above table gives details about the number of ATMs available in India. As per the table during 2011 (March) only 41,268 onsite ATM and 34,377 offsite ATM were present. But according to the latest report of March 2017, there are nearly 1.1 lakhs onsite ATM and 1 lakh offsite ATM in India depicting the high increase in the number of ATMs within a short span of 6 years. The graph for the above data is as follows [4].



	2011	2012	2013	2014	2015	2016	2017
ON-SITE	41,268	47,545	55,760	83,379	89,061	101,950	109,809
OFF-SITE	34,377	48,141	58,254	76,676	92,337	97,149	98,545

Fig 02. Number of ATMs

Initially the ATMs were introduced to provide cash to the customers but subsequently with technological developments its services have been extended to include cash withdrawals, funds transfers from one account to the other and make payments (Abor ,2004). In the early 1990s, ATMs initiated by foreign banks were introduced to the Indian banking industry. At that time, most international banks

and some private sector players were suffering from a severe challenge of absence of a strong network of branches [15]. As per the Global ATM Market and Forecasts to 2016, the maximum growth of ATMs is happening in Asia pacific region. India and Indonesia are having one fourth of the number of ATMs, and china is accounted for half of the New ATMs. Worldwide growth of ATMs is steadily increasing in the given below figure [5]:

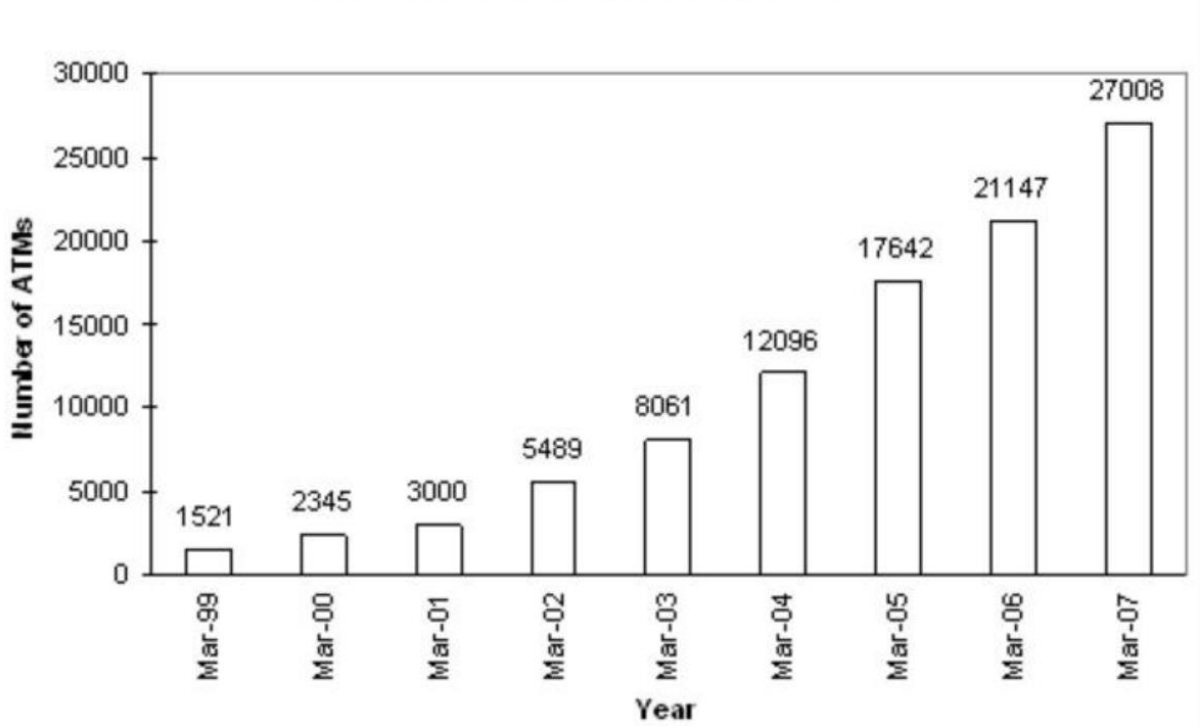


Fig 03 Total number of ATMs in INDIA

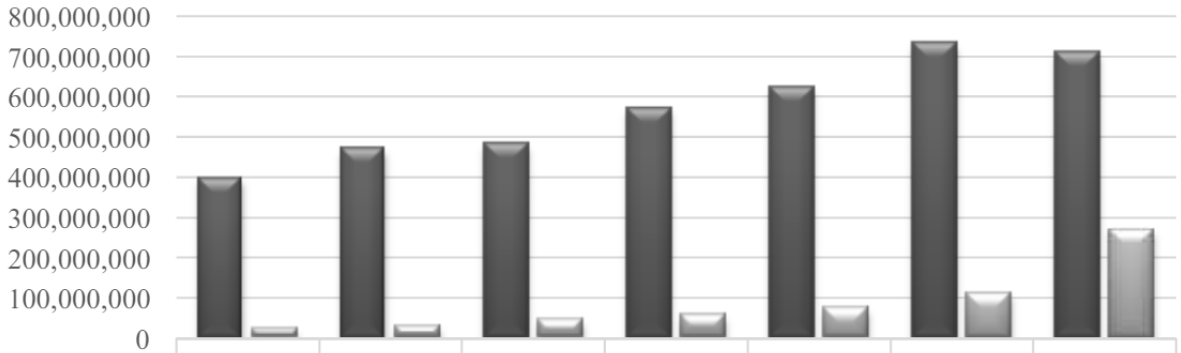
1.4 Usage of ATM in India

The following details were extracted from the RBI database for the past eight years. The ATM card usage details taken are depicting in the table below:

YEAR	ATM	POS
2011	39,95,53,342	2,24,61,539
2012	47,10,31,623	3,06,68,922
2013	48,20,04,645	4,53,76,619
2014	57,14,97,661	5,69,81,333
2015	62,42,05,135	7,61,05,726
2016	73,17,22,405	11,28,68,336
2017	71,01,08,656	27,11,72,292

Table 02. Number of Transaction in India

The above table expresses the number of ATM transactions in India. ATM depicts the cash withdrawal directly from the ATM centre while POS depicts the swiping of the card at the place of sale. POS helps the customers to carry less amount and with high safety. There is a considerable increase in POS transactions in 2017 as compared to 2011. The usage of POS transactions has increased 15 times while ATM transactions how only two times increase. The following graph 2 explains the number of transactions in India. The graph expresses the number of ATM card transactions in ATM centres and point on sale machines.During the year 2016,the number of ATM centre usages were very high duetothe effect of demonetization. The point on sale (POS)had increased at a rapid rate during the current year 2017. Every customer who has adopted the digital India system prefers cashless transactions [6].



	2011	2012	2013	2014	2015	2016	2017
ATM	399,553,3	471,031,6	482,004,6	571,497,6	624,205,1	731,722,4	710,108,6
POS	22,461,53	30,668,92	45,376,61	56,981,33	76,105,72	112,868,3	271,172,2

Fig 04. Number of Transaction in India

Chapter 02. LITERATURE REVIEW

- (Moutinho & Meidan, 1989) states that technological development leads to the usage of a new product like Adarsh Kumar Singh, Ayush Pandey, Krishna Sharma, Akansh Arya Professor Tejinder Pal Singh (E16552) ATM. It helps in reducing the usage of the bank and interaction between the banker and the customer.
- (Choodambigai, 2011) This study aims to find the usage of ATM among the customers. The result is that most of the customers use ATM for withdrawal of their money and very few of them use to verify the account details. This study only concentrates on public sector banks. The paper also aims to study credit card and ATM services based on customers' perception.
- (Jetley, 2004) The technological development in various sectors illustrates the need for new innovative concepts like ATM in the banking sector as well. The advancement in ATMs in the recent times is shown through the environment friendly approaches adopt by the banks such as solar power ATM centers.
- Solar power ATM centers will become a necessity in the near future as India is suffering from the lack of adequate supply of electricity in most of its areas. Power is the biggest barrier for the development of ATMs in India.

YEAR	ON-SITE	OFF-SITE
2011	41,268	34,377
2012	47,545	48,141
2013	55,760	58,254
2014	83,379	76,676
2015	89,061	92,337
2016	1,01,950	97,149
2017	1,09,809	98,545

Table 03. Total no of ATMs

- (Kumar, 2011) This study expresses the reason for increasing usage of ATM in India. The ability to provide major facilities like bill payment, money transfer and other financial services helps to customers to save their time. The trust prevalent over the ATMs is high that the customers do not even count after withdrawing their cash from the machine.

Adoption Models	Study	Insights
Theory of Reasoned Action (TRA)	Ajzen and Fishbein (1980); Fishbein and Ajzen (1975);Davis et al.1989	TRA has been most applied in consumer behavior literature. As per this model, attitude of a person and subjective norms drive a person's behavioral intention.
Technology Acceptance Model(TAM)	Davis,F.D., Bagozzi,RP. and Warshaw, P.R.(1989)	This theory adds ease of use and usefulness to TRA which are attitude measures .This model is quite individual focused while other models are organization focused.
Model of PC Utilization(MPCU)	Thomson et al.(1991)	This model is a modification from a particular set of variables of the proposed model of Triandis (1977) which deals with human behavior. This model has been used to predict PC Utilization. Thomson adaptation deals with information systems environment.
Social Cognitive Theory(SCT)	Bandura(1977); Compeau and Higgins(1995)	This theory explains own competence of a person in relation to the capabilities and social perception of those around them rather than how the individual perceives the technology itself. This theory is deviated from other adoption theories which are derived from the foundation of TAM and innovation diffusion.
Unified Theory of Acceptance and use of Technology (UTAUT)	Venkatesh et.al.(2003)	UTAUT's goal is to clarify user intention to use an Information system and further usage behavior. This is a technology acceptance model which is formulated by Venkatesh et.al. (2003).
Innovation Diffusion Theory (IDT)	Agarwal and Prasad (1998); Moore and Benbasat (1991); Rogers (1995)	This theory guides the way to increase the rate of adoption. It also explains how, when and why innovations spread through a society.
Motivation Model(MM)	Davis, Bagozzi, and Warshaw (1992)	This model explains extrinsic and intrinsic motivation.
Theory of Planned Behavior (decomposed) (DTPB)	Taylor and Todd (1995)	This model provides complete understanding of intention and usage behavior. It may also provide more effective guidance to Researchers and IT Managers who are keen to study system implementation.

Table 04. Theories of Technology Adoption

- (Tuli, Khatri & Yadav, 2012) This study aims to compare public sector and private sector bank ATMs, usage and other facilities. Only two banks- SBI and ICICI were taken for the study. The result reveals that the public-sector bank dispenses old currencies and private sector bank run out of cash most of the times. Thus, both the banks have their limitations. The paper does not consider the bank employee perspectives and concentrate only on the customers who are using the ATM.
- (Premalatha & Sundaram, 2012) The primary concern of this paper is about customer satisfaction while using ATM, and it has been found there is a significant effect on age factor and safety, gender and tangibility. But there is no significant relation between occupation and satisfaction level. So, it is concluded that the customers expect safety, assurance and convenience.

Sr. No.	Author with Publication Year	Technique Adopted	Significance	Limitations
1.	Jane Ngozi Oruh (2014)	Three-factor Authentication for Automated teller Machine	In this paper author used smart card, user PIN and fingerprint authentication as a three factor Authentication	Some kind of attack like skimming attack, phishing attack, card stolen issue and No backup method in fingerprint failure situation and OTP Method
2.	Milind Nemade[1], Laukik Karnavat[2], Prachi Dharu[3], Ruchika Desure[4], Sejal Gandhi[5]	A Review Paper on Improving Security of the ATM System	The purposed system used in this paper consist three security levels which are card with PIN, fingerprint as a biometric identification and last one is the OTP.	Purposed system used the RFID reader which contains the radio frequency spectrum, which is harmful for health or intruder easily read data from the RFID spectrum. Issue on card and PIN are attacks. skin diseases are the bad influence using fingerprint identification.
3.	V. Meena Mphil (2015)	Facial Recognition Technology for use in the ATM transactions	User facial image verified during ATM transaction which is stored in the banking database.	Sometime system didn't recognized facial image in different situation like camera distance in facial image clarity, different face angles and lighting condition.
4.	Joyce Soares[1], Dr. A. N. Gaikwad[2] (2016)	A Survey on the Security of an ATM transaction	In this paper techniques used biometrics (fingerprint and Iris Recognition), GSM and image quality.	Iris recognition have high installation or maintenance cost, GSM techniques not feasible for everyone

Table no 05. Adoption and Diffusion of ATM technology

- (Renuka & Paulraj, 2014) This study concentrates on customers satisfaction at the point of withdrawal, 24 hours and on the deposit system. But there is lack of awareness among the customers while using ATM. It is suggested to the bankers that ratifying customers' comments, doubts and suggestions will increase the reputation of the bank among the customers.
- (Sisat & Barbuddhe, 2014) This paper explains the various threats to ATM and Cash Deposit machine. There are three types of risks involved while using the ATM, which are currency fraud, logical attacks and physical damages. This paper explains the security system of ATM and CDM.
- Few years ago purposed of paper to describe the three-factor authentication in ATM transaction when two-factor authentication no longer success. In the two- factor authentication security concept are ATM card and PIN (Personal identification number). Two factor authentications not provided valid level of security then need for more secure mechanism. And purposed method combined of ATM card, user PIN and biometric technique for three-factor authentication.
- The main purpose of this research paper to provide the biometric security in the ATM transaction. And for this purpose used biometric identification (finger print) with the mobile number. When the customers open an account in the branch meanwhile provide the fingerprint or mobile number. And when the customer access the ATM machine then place finger on the figure print module then system generate 4-digit code and send it to the customer's registered mobile number. And if customer valid 4-digit Code then successfully accesses the account or if entered wrong digit then system not allow accessing the account.

- In research paper define that data security is important concept in banking sector when the data transmit from ATM machine to bank server. This data transmit in the Encrypted form then unauthorized user cannot access it. And

define the encryption techniques, that what level of data security provided by these algorithm.

- In research paper define that data security is important concept in banking sector when the data transmit from ATM machine to bank server. This data transmit in the Encrypted form then unauthorized user cannot access it. And define the encryption techniques, that what level of data security.

Table no 06. Comparison between the current of ATM transaction

Sr. No.	Author with Publication Year	Technique Adopted	Significance	Limitations
1.	Jane Ngozi Oruh (2014)	Three-factor Authentication for Automated teller Machine	In this paper author used smart card, user PIN and fingerprint authentication as a three factor Authentication	Some kind of attack like skimming attack, phishing attack, card stolen issue and No backup method in fingerprint failure situation and OTP Method
2.	Milind Nemade[1], Laukik Karnavat[2], Prachi Dharu[3], Ruchika Desure[4], Sejal Gandhi[5]	A Review Paper on Improving Security of the ATM System	The purposed system used in this paper consist three security levels which are card with PIN, fingerprint as a biometric identification and last one is the OTP.	Purposed system used the RFID reader which contains the radio frequency spectrum, which is harmful for health or intruder easily read data from the RFID spectrum. Issue on card and PIN are attacks. skin diseases are the bad influence using fingerprint identification.
3.	V. Meena Mphil (2015)	Facial Recognition Technology for use in the ATM transactions	User facial image verified during ATM transaction which is stored in the banking database.	Sometime system didn't recognized facial image in different situation like camera distance in facial image clarity, different face angles and lighting condition.
4.	Joyce Soares[1], Dr. A. N. Gaikwad[2] (2016)	A Survey on the Security of an ATM transaction	In this paper techniques used biometrics (fingerprint and Iris Recognition), GSM and image quality.	Iris recognition have high installation or maintenance cost, GSM techniques not feasible for everyone

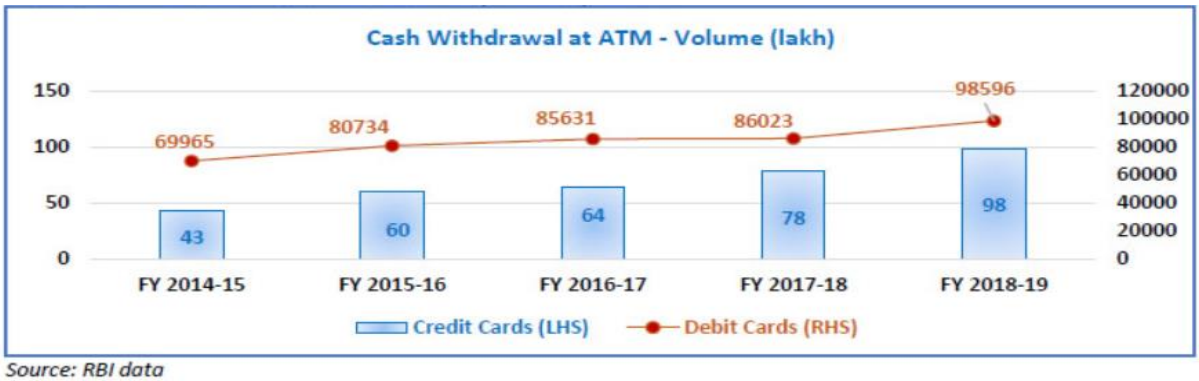
Chapter 03. DESIGN FLOW/PROCESS

- **Bank Account**

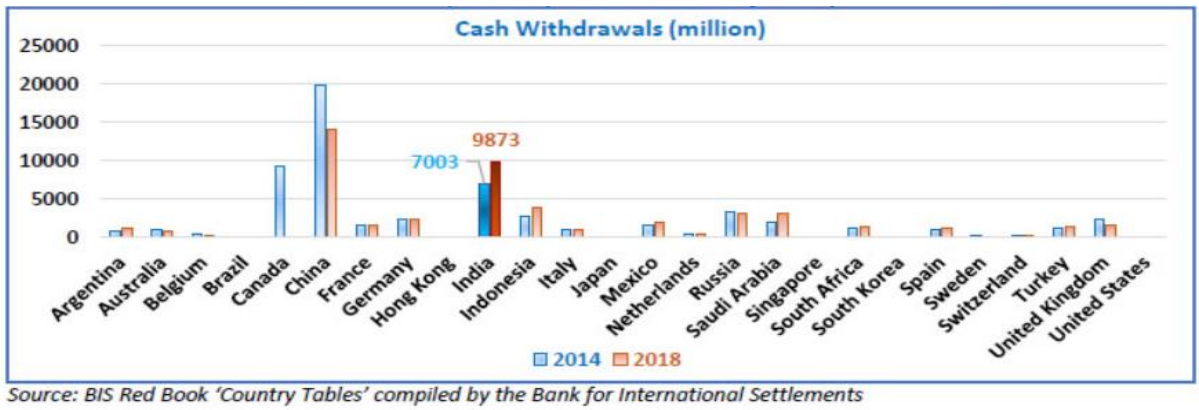
As per the research findings 100% of the people have their personal bank account. About 50% of the respondents have more than one bank account. According to the interview with the respondents, it is clear that 70% of the respondents opened a bank account because of their need. While other 30% of the respondents opened due to the influence of their family, friends, bank employees, and office.

- **ATM Cards**

According to the survey, 95% of the respondent use ATM cards, while 5% of the respondents don't use ATM cards. As per the interaction with the people, it is found that out of 30 respondents, 13 of them use ATM service once a month and others once a week or three times a week. About 60% respondents hold a single ATM card.



Source: RBI data



Source: BIS Red Book 'Country Tables' compiled by the Bank for International Settlements

Fig 04. Cash withdrawals from ATMs

- **Problem of having no cash in ATM machine**

As per the research findings, among 26 respondents who use ATM card 15% of them have faced the problem of having no cash in the ATM machine. The problem of having no cash in the bank takes place rarely. Among 30 respondents, 11 of them use mobile banking facility while 19 of them don't use mobile banking facility.

3.1 Research Methods Used

Research methodology is the science of finding out and it is a subfield of epistemology, which is the science of knowledge. Indeed, utilizing an appropriate methodology is not only the right path to the truth, but also the duty of every researcher. The methodology covers issues that relate to the type of data collected, the way it was collected and analyzed [7].

3.1.2 Study Area and Sources of Data

• Within the study area, the study is based on primary data. We use primary data since our study is related to ATM which isn't available from secondary sources

• Our study area is Jawalakhel of Lalitpur. The study area is presented on the figure given below

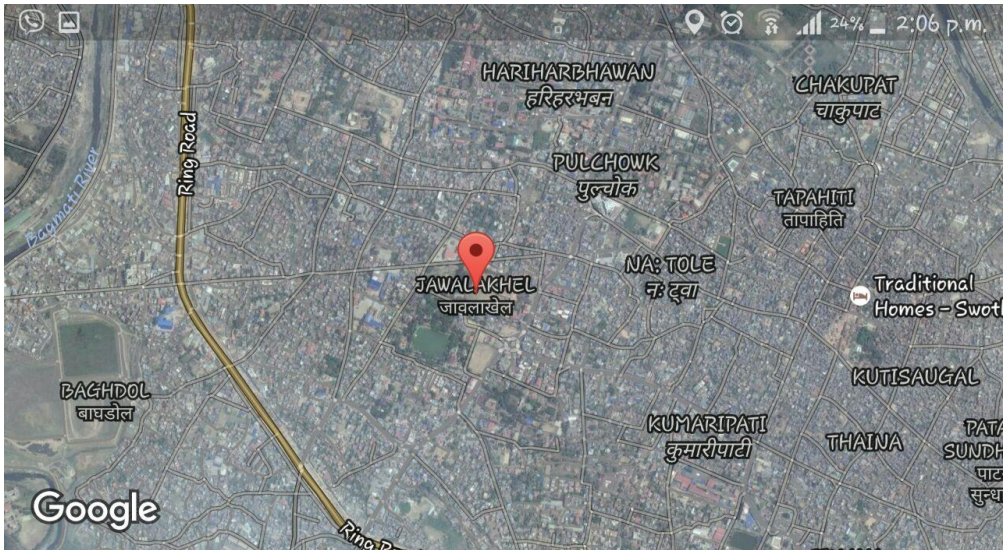


Fig 05. ATM's location

3.1.3 Study Population and Sample

• The population of this study was from the selected locations. From the population we select total 30 HH/ respondents/ businessman etc. as a sample. We prepared a structional questionnaire with both closed and open ended questions to obtain information on stated objectives. The questionnaire was divided into three sections; Section A: Information regarding research and researcher.

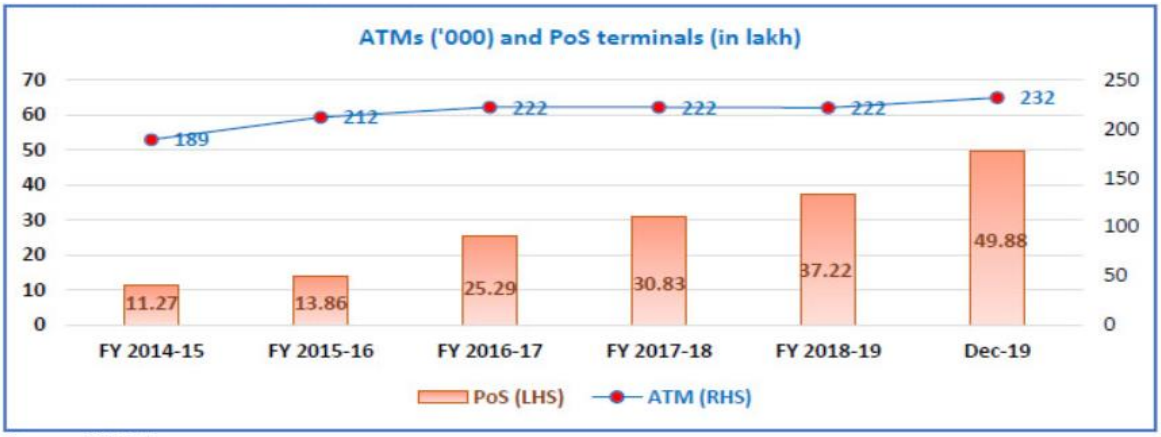
3.1.4 PreTesting of Questionnaire and Survey Implementation

• The questionnaire was pre-tested on respondents that lie on the study area to check their reliability and validity before the main survey (actual data collection). The reason behind conducting pre-test survey was to avoid ambiguity of some of the questionnaire's items. The pre-testing of questionnaire was conducted on September, 2016 A.D. The final interviews were conducted in purposive sampling

3.2 Types of ATMs:

An Automated Teller Machine (ATM) is a self-service banking terminal that allows customers to perform various financial transactions without the need for a human teller. ATMs have become an integral part of the banking landscape in India, providing customers with convenient access to their accounts and a range of banking services [8].

In India, the ATM market has seen significant growth and evolution over the years. As of 2024, there are over 300,000 ATMs installed across the country, catering to the diverse banking needs of both urban and rural populations.

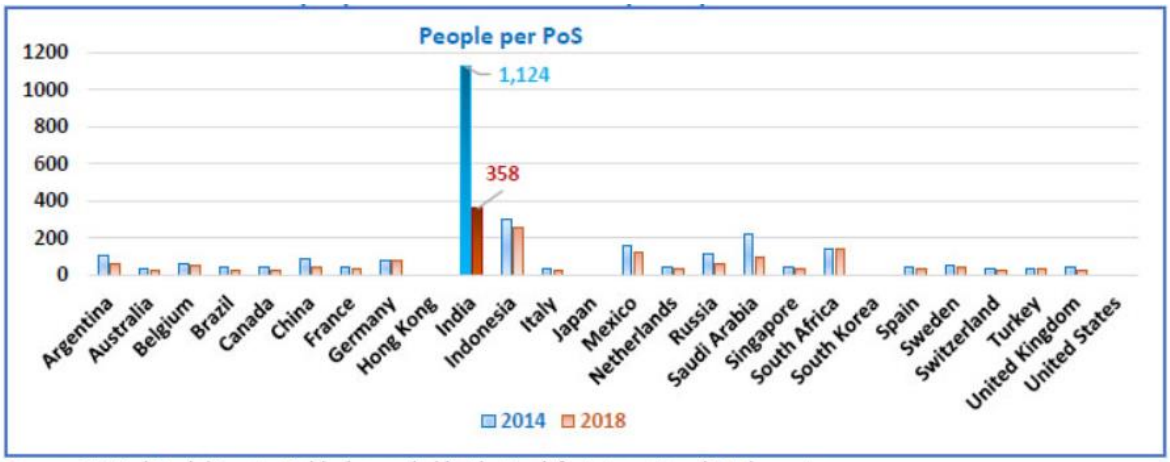


Source: RBI Data.

Fig 06. ATMs Users per Year

3.2.1 Classification of ATMs in India

Based on various parameters, ATMs in India can be categorized into the following types:



Source: BIS Red Book 'Country Tables' compiled by the Bank for International Settlements.

Fig 07. No of People per Point of Sale

3.5.2 Location-based Classification

1. **Independent ATMs**

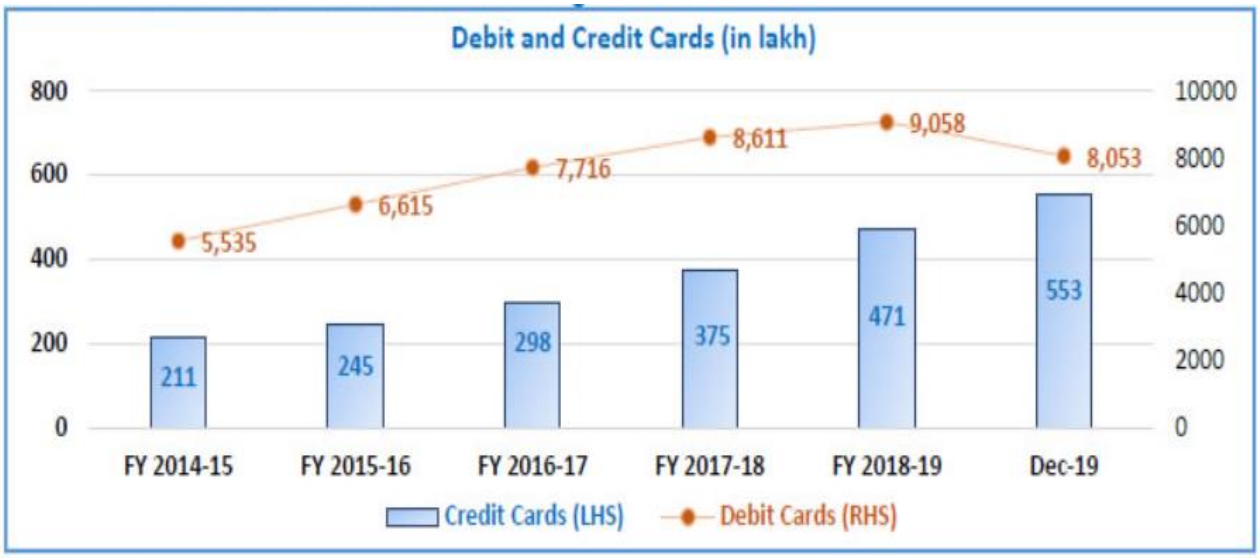
These are standalone ATM units that are not located within a bank branch or any other establishment. Independent ATMs are typically placed in high-traffic public areas like shopping malls, airports, railway stations, and other convenient locations to provide easy access to cash and banking services.

2. **Interior ATMs**

Interior ATMs are installed within the premises of a bank branch or other financial institution. These ATMs are typically located in the lobby or other designated areas, providing customers with a secure and controlled environment to perform their transactions.

3. **Outdoor ATMs**

Outdoor ATMs are installed in public spaces, often in the vicinity of bank branches or other commercial establishments. These ATMs are designed to withstand various environmental conditions and provide 24/7 accessibility to customers. Outdoor ATMs are particularly useful in areas where space within a bank branch is limited.



Source: RBI Data

Fig 08. Debit and Credit card uses

3.5.3 Ownership-based Classification

3.2.1 Bank-owned ATMs

Bank-owned ATMs are operated and maintained by the banks themselves. These ATMs are typically located within the bank's branch premises or in strategic locations to serve the bank's customers.

Bank-owned ATMs offer a wide range of services, including cash withdrawals, balance inquiries, fund transfers, and bill payments.

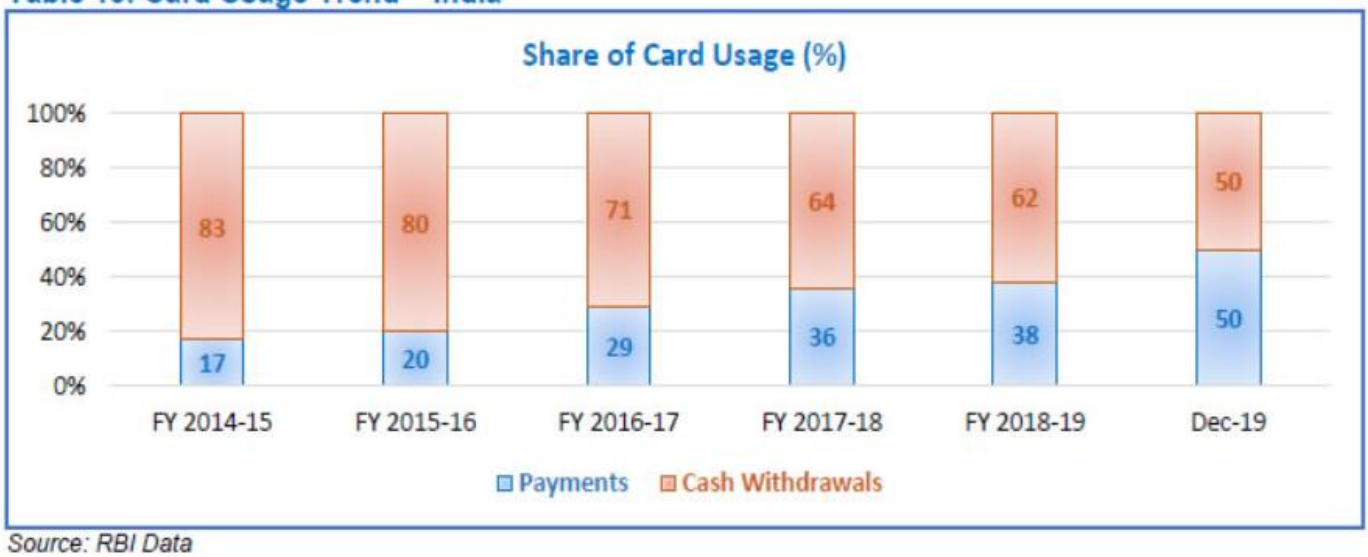
3.2.2 White-label ATMs

White-label ATMs are owned and operated by non-bank entities, such as independent ATM operators or cash management companies. These ATMs are not directly affiliated with any particular bank and can be used by customers of various banks. White-label ATMs often charge a fee for their services, which can be higher than the fees charged by bank-owned ATMs.

3.2.3 Brown-label ATMs

Brown-label ATMs are a hybrid model where the ATM is owned by a non-bank entity, but the branding and operations are managed by a partner bank. This arrangement allows banks to expand their ATM network without the need for significant capital investment, while the non-bank entity provides the infrastructure and maintenance.

Table 13: Card Usage Trend – India



Source: RBI Data

Fig 09. Card Uses in India

3.3 Functionality-based Classification

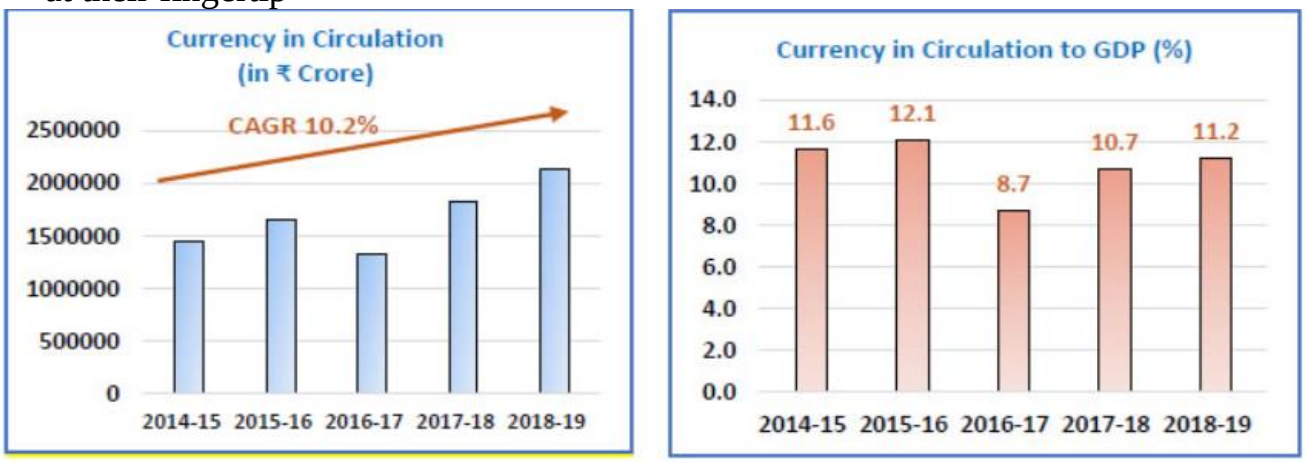
3.3.1 Basic ATMs

Basic ATMs are the most common type of ATMs in India, catering to the essential banking needs of customers. These ATMs typically offer services such as cash withdrawals, balance inquiries, mini-statements, and PIN changes. Basic ATMs are widely available and serve as the primary access points for cash transactions.

3.3.2 Complex ATMs

Complex ATMs, also known as advanced or full-service ATMs, offer a wider range of banking services beyond the basic cash withdrawal and balance inquiry functions. These ATMs may include features such as bill payments, fund transfers, cheque deposits, and even account opening or loan applications. Complex ATMs cater to the evolving needs of customers who seek more comprehensive banking services at their fingertip.

These ATMs may include features such as bill payments, fund transfers, cheque deposits, and even account opening or loan applications. Complex ATMs cater to the evolving needs of customers who seek more comprehensive banking services at their fingertip



Source: RBI Data

Fig 10. Currency circulation in ATMs in India

These ATMs may include features such as bill payments, fund transfers, cheque deposits, and even account opening or loan applications. Complex ATMs cater to the evolving needs of customers who seek more comprehensive banking services at their fingertip

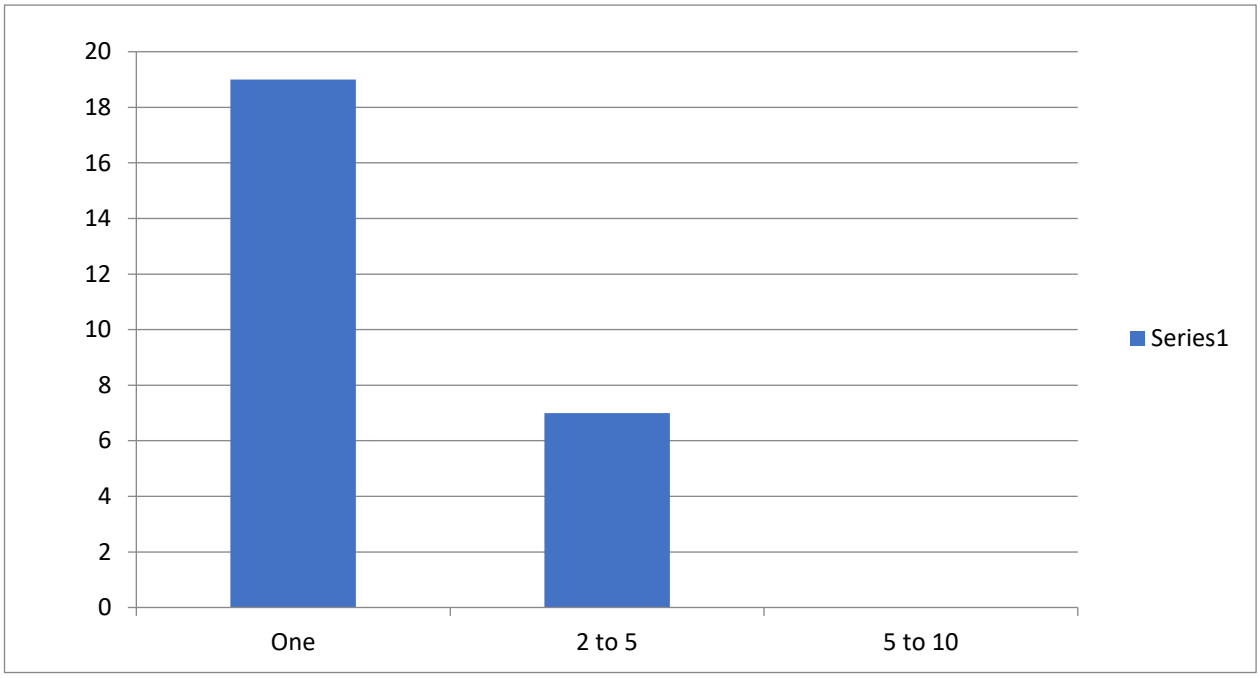


Fig 11. People having number of ATMs

1. Traditional Bank-Operated ATMs

Traditional bank-operated ATMs are the most common type of ATMs found across India. These ATMs are owned and operated by individual banks and are typically located within bank premises, shopping malls, airports, and other high-traffic areas. Each bank has its own network of ATMs, and customers can access their accounts and perform transactions using their bank-issued debit or credit cards [9].

Key Features:

- Withdrawal of cash
- Balance inquiry
- Mini-statement printing
- Funds transfer between accounts
- Cheque book request

- PIN change facility

These ATMs are designed to offer basic banking services to customers, and the range of services may vary depending on the bank's policies and the ATM's capabilities.

2. **White Label ATMs**

White Label ATMs (WLAs) are a relatively new concept in India, introduced by the Reserve Bank of India (RBI) in 2012. These ATMs are owned and operated by non-bank entities, such as independent ATM deployment companies or business correspondents. WLAs are not affiliated with any specific bank and can be used by customers of any bank, providing a shared infrastructure for cash withdrawal and other basic services.

Key Features:

- Cash withdrawal
- Balance inquiry
- Mini-statement printing
- Interoperable with all banks

WLAs play a crucial role in expanding the ATM network in India, particularly in semi-urban and rural areas where traditional bank-operated ATMs may be less accessible. They operate on a surcharge-based model, where customers may be charged a small fee for using the ATM service.

3. **Multibank ATMs**

Multibank ATMs, also known as shared ATMs or inter-bank ATMs, are operated by a consortium of banks or third-party service providers. These ATMs allow customers from multiple banks to access their accounts and perform transactions using a single ATM terminal.

Key Features:

- Cash withdrawal
- Balance inquiry
- Mini-statement printing
- Interoperable with participating banks

Multibank ATMs promote interoperability and convenience for customers, as they can access their accounts from any participating bank's ATM, regardless of the bank's network. This concept helps reduce the need for individual banks to establish their own extensive ATM networks, while still providing widespread access to ATM services for their customers.

4. **Mobile ATMs**

Mobile ATMs, as the name suggests, are portable ATM units that can be deployed in various locations on a temporary or semi-permanent basis. These ATMs are typically mounted on vehicles or trailers and are designed to provide banking services in remote areas, at events, or in locations with limited access to traditional ATMs.

Key Features:

- Cash withdrawal
- Balance inquiry
- Portable and easily deployable
- Ideal for remote areas or temporary events

Mobile ATMs are particularly useful in rural areas where establishing permanent ATM infrastructure may not be feasible due to low population density or logistical challenges. They can also be deployed at large events, such as festivals or conferences, to cater to the increased demand for cash withdrawal services.

5. **Biometric ATMs**

Biometric ATMs are a relatively new innovation in the Indian ATM landscape, introduced to enhance security and prevent unauthorized access to customers' accounts. These ATMs use biometric authentication methods, such as fingerprint scanning or iris recognition, in addition to traditional card-based authentication.

Key Features:

- Biometric authentication (fingerprint, iris, etc.)
- Enhanced security against fraudulent transactions
- Cash withdrawal
- Balance inquiry
- Mini-statement printing

Biometric ATMs provide an additional layer of security by verifying the customer's identity through their unique biometric data. This helps prevent unauthorized access to accounts and reduces the risk of fraud, especially in cases where debit or credit cards are lost or stolen.

6. **Cardless ATMs**

Cardless ATMs are a relatively new concept in India, designed to provide customers with a convenient way to withdraw cash without the need for a physical debit or credit card. These ATMs rely on mobile banking applications or other secure authentication methods to initiate and authorize transactions.

Key Features:

- No need for a physical debit or credit card
- Cash withdrawal using mobile banking apps or secure codes
- Balance inquiry
- Enhanced security and convenience

Cardless ATMs eliminate the need to carry physical cards, reducing the risk of card loss or theft. Customers can initiate cash withdrawals through their mobile

banking applications or by generating secure codes, which are then authenticated by the ATM for completing the transaction.

7. Recycling ATMs

Recycling ATMs, also known as cash recyclers or intelligent deposit machines, are advanced ATMs that not only dispense cash but also accept and recycle deposited cash. These ATMs are designed to streamline cash management processes for banks and reduce the need for frequent cash replenishment.

Key Features:

- Cash withdrawal
- Cash deposit and recycling
- Real-time credit to customer accounts
- Automated cash handling and sorting

Recycling ATMs play a crucial role in optimizing cash management for banks. By accepting and recycling deposited cash, these ATMs minimize the need for frequent cash replenishment, reducing operational costs and improving efficiency.

8. Full-Service ATMs

Full-Service ATMs, or Interactive Teller Machines (ITMs), are advanced ATMs that combine traditional ATM functionality with video conferencing capabilities, allowing customers to interact with remote bank representatives for more complex transactions or inquiries.

Key Features:

- Video conferencing with bank representatives
- Extended range of banking services
- Cash withdrawal
- Account opening or loan applications
- Document submission and processing

Full-Service ATMs aim to bridge the gap between traditional ATMs and in-person branch banking. Customers can conduct more complex transactions, such as account opening or loan applications, while still enjoying the convenience of remote self-service banking.

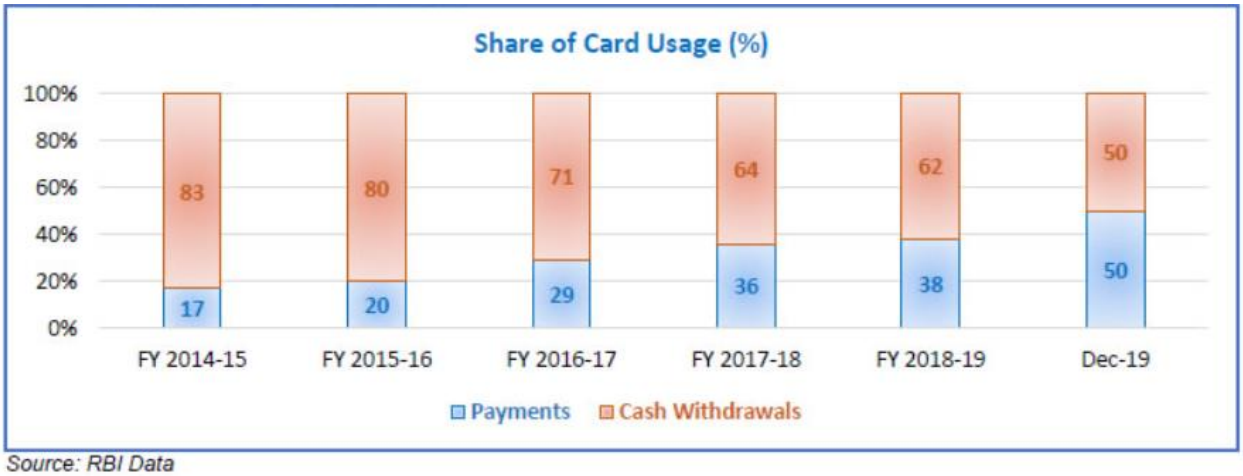
9. Talking ATMs

Talking ATMs, also known as speech-enabled ATMs, are designed to assist visually impaired or low-vision customers by providing audio guidance and instructions for ATM transactions. These ATMs use text-to-speech technology to convey on-screen information through audio outputs.

Key Features:

- Audio guidance and instructions
- Accessibility for visually impaired customers
- Cash withdrawal
- Balance inquiry
- Mini-statement printing

Talking ATMs promote inclusivity and accessibility in banking services, ensuring that customers with visual impairments can independently perform ATM transactions without relying on assistance from others.



Source: RBI Data

Fig 12. Percentage of ATMs uses in India

- **Types of ATM service you are willing to use**

The ATM services are Purchasing travel tickets, pay bills, purchasing phone talk time, check account balance, withdrawal and others to specify. It is presented in the bar [10].

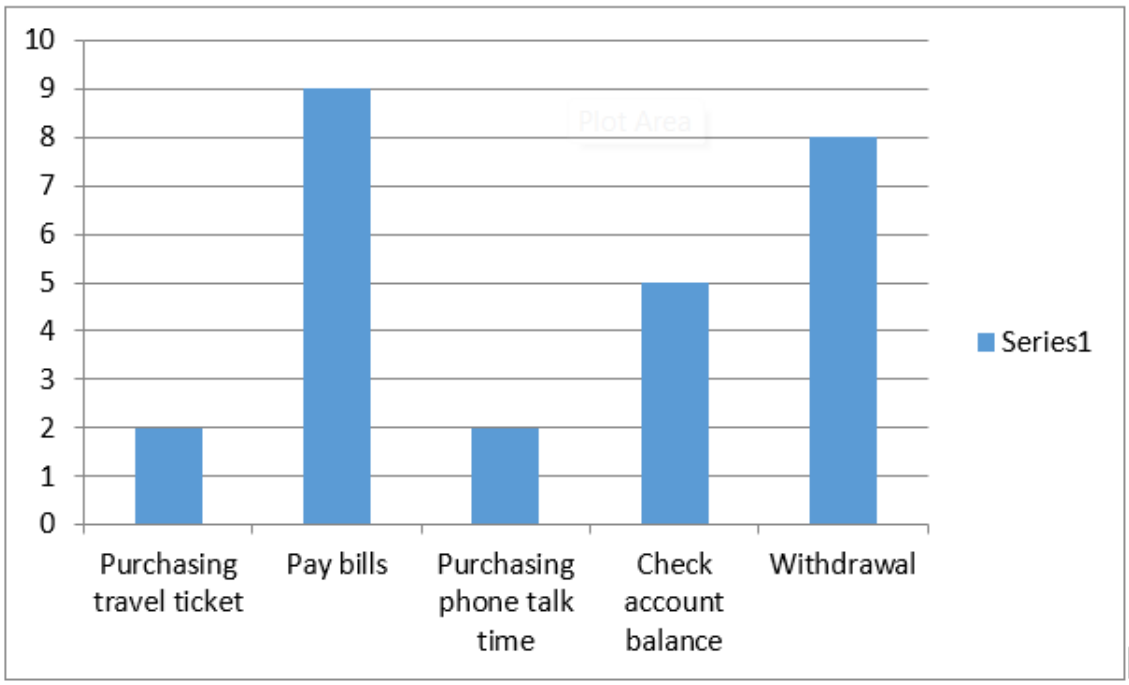


Figure 13: Types of ATM service willing to use

3.4 Security Systems for ATMs

Automated Teller Machines (ATMs) have revolutionized the way we access our cash, offering convenience, flexibility, and service 24/7. However, with the increasing sophistication of criminal activities, ATMs have become prime targets for theft, vandalism, and other security breaches. This article explores the importance of ATM security, the threats these machines are facing, and the role of innovative solutions like fog cannons in securing valuables.

Understanding the Importance of ATM Security:

ATM security is important for both financial institutions and the public. For banks and ATM operators, ensuring the safety of these machines is not just about protecting the valuables but also maintaining customer trust. Security breaches

can result in financial losses, damage to reputation, and legal consequences.

For consumers, a secure ATM is essential to ensure their peace of mind while using these machines. A lack of security can result in personal financial losses, identity theft, and even physical harm in some cases. It is, therefore, imperative to address security concerns associated with ATMs.

Automated Teller Machines (ATMs) play a pivotal role in modern banking, offering convenience and accessibility to millions of people worldwide. Let's explore their significance [11]:

1. Convenience and Accessibility:

- ATMs provide 24/7 access to your bank account, freeing you from the constraints of branch operating hours.
- Whether you're withdrawing cash, checking your account balance, or depositing money, ATMs offer unmatched convenience.

2. Speed and Efficiency:

ATMs allow you to conduct transactions quickly and efficiently without waiting in line for a teller.

The core functions include:

- **Cash Withdrawals:** Easily withdraw cash using your debit or credit card, subject to daily withdrawal limits.
- **Balance Inquiries:** Stay informed about your account balance.
- **Deposits:** Some ATMs accept cash or checks, eliminating the need to visit a bank branch.
- **Funds Transfers:** Transfer money between your own accounts or to third-party accounts.

- **Bill Payments:** Conveniently pay bills, ensuring timely payments and avoiding late fees.
- **Mobile Top-Ups:** Recharge your mobile phone prepaid balance directly.

3. Evolution of ATMs:

- The first modern ATM was introduced by Barclays Bank in London in **1967**.
- Initially, ATMs could only dispense cash, but technological advancements have expanded their functionalities.
- Today's ATMs feature touch screens, cardless access, multi-language support, and contactless payment options.

4. Socio-Economic Impact:

- ATMs provide **convenient 24/7 access** to banked cash near where people live, work, and shop.
- They enable cash withdrawals, deposits, bill payments, ticket purchases, and fund transfers.
- The ATM industry has developed comprehensive security standards to prevent fraud.

3.5 Why ATMs are vulnerable:

Just like any computing device, ATMs have vulnerabilities. And one way to understand why bad guys are drawn to them is to understand its components and the way it communicates with the bank network.

An ATM is composed of a computer (and its peripherals) and a safe. The former is enclosed in a cabinet. This is the same whether the ATM is a stand-alone kiosk

or a “hole in the wall.” The cabinet itself isn’t particularly secure or sturdy, which is why criminals can use simple tools and a lock key purchasable online to break into it to gain access either to the computer or the safe.

The computer usually runs on Windows—a version specifically created for ATMs. ATM users don’t see the familiar Windows desktop interface because access is restricted. What we do see are user-facing applications that aid us in making transactions with the machine [12].

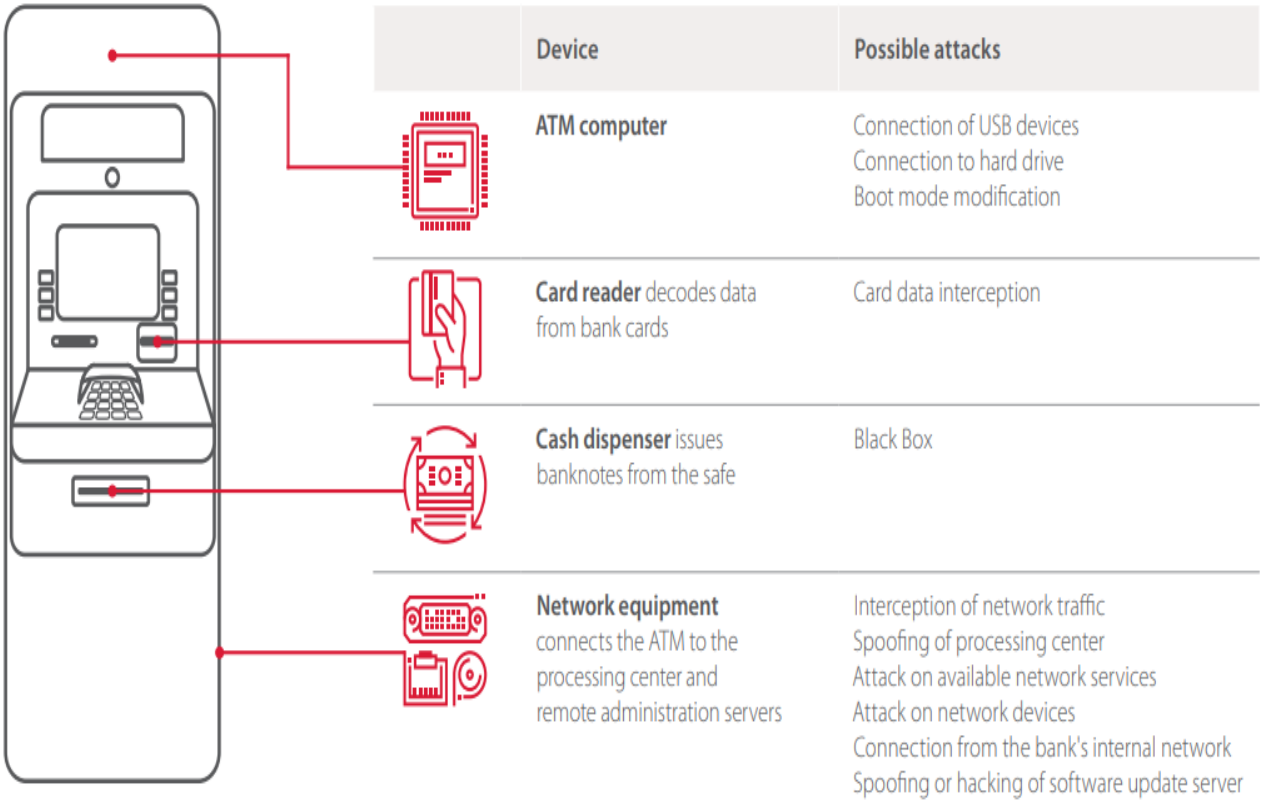
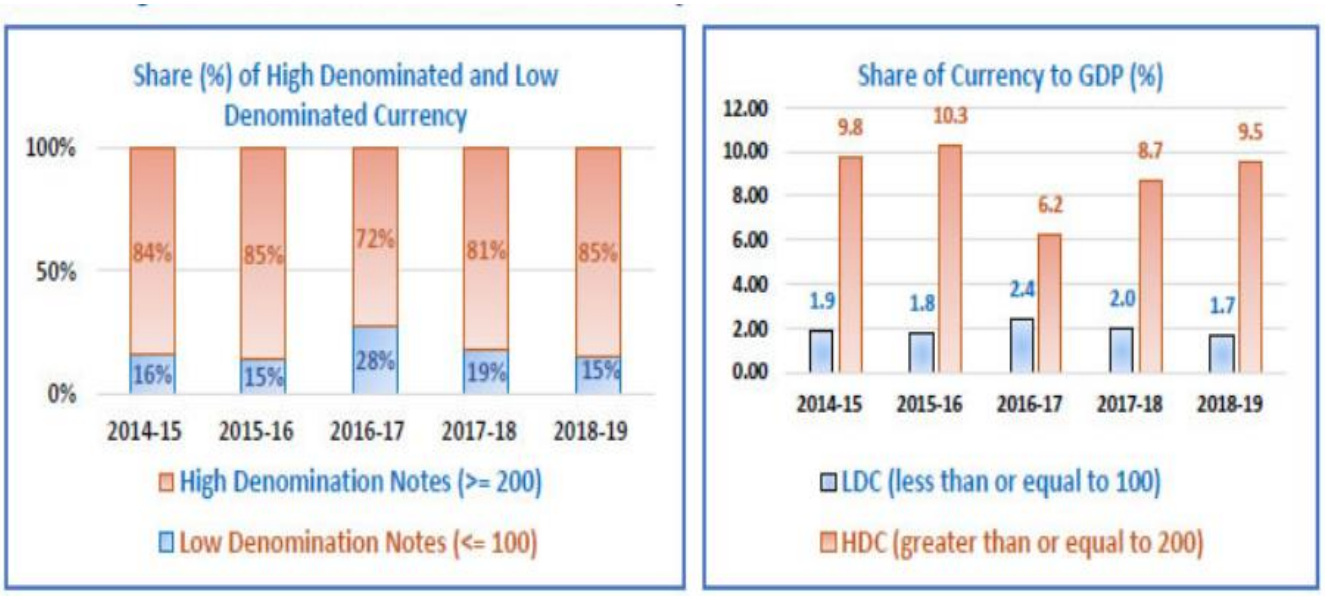


Fig 14. Components of an ATMs

Up to now, many ATMs have still been running on Windows XP. If the OS is outdated, expect that the software in them may need some upgrading as well. That said, criminals can take their pick of which exploits to use to make the most of software vulnerabilities and take control of the remote system.

In some cases, interfaces like a USB port visible in public can encourage users with ill-intent to introduce malware to the machine via portable device. Since security software may not be installed in them, and there is a significant absence of authentication between peripherals and the OS, there is increased likelihood of infection. To date, there are already 20 strains of known ATM malware discovered.



Source: RBI Data

Fig 15. Values of ATMs in India

The cash dispenser is directly attached to the safe where the cash is stored. A compromised computer can easily give criminals access to the interface between the computer and the safe to command it to dispense cash without using stolen customer card information.

The traffic between the ATM computer and the transaction processing server is usually not encrypted, making it a breeze for hackers to intercept transmitted data from customer to bank server. Worse, ATMs are notoriously known for implementing poor firewall protection, which makes them susceptible to network attacks.

Other notable weaknesses are missing or misconfigured Application Control software, lack of hard drive encryption, and little-to-no protection against users accessing the Windows interface and introducing other hardware devices to the ATM.

Sr. No.	Control Measures for the ATMs	To be completed by
a.	Implement security measures such as BIOS password, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other softwares, terminal security solution, time-based admin access, etc.	Aug-18
b.	Implement anti-skimming and whitelisting solution	Mar-19
c.	Upgrade all the ATMs with supported versions of operating system. Such upgrades shall be carried out in a phased manner to ensure that in respect of the existing ATMs running on unsupported versions of operating system,	i. Not less than 25% by Sep-18 ii. Not less than 50% by Dec-18 iii. Not less than 75% by Mar-19 iv. All of them shall be upgraded by Jun-19

Table no 07. Control measures on ATMs

3.6 Threats to ATM Security

ATMs are subjected to a variety of physical threats, making it crucial to enhance their security [13].

- **Physical Attacks**

Physical attacks on ATMs pose a significant risk to both financial institutions and public safety.

• **Ram Raids:** Criminals may use vehicles to crash into ATMs, causing extensive damage and making theft possible. Reinforcements around ATMs can lower this threat.

• **Explosive Attacks:** Criminals may use explosives to breach the ATMs. The explosion can result in great losses and even endanger lives.

• **Heavy Equipment:** Some criminals use heavy machinery like backhoes or forklifts to forcibly remove ATMs from their mounts, often leading to significant damage.

To combat these threats, it's essential to implement robust security measures and alarms that trigger during any attempts of damaging the ATM.

➢ Vandalism and Tampering

ATMs are not only targets for theft but also for vandalism and tampering.

• **Graffiti and Defacement:** Vandals may target ATMs with graffiti or other forms of defacement, impacting the machine's appearance and brand image.

• **Tampering:** Criminals may attempt to tamper with the ATM's components, such as card slots or cash dispensers, to compromise its functionality and security.

Preventing vandalism and tampering often requires more than surveillance cameras, but an active response to attempts of damage, and security measures that protect the ATM's sensitive parts.

➢ Shimming

Mentioned, "skimming" is when thieves insert a device into an ATM's card reader to steal data from swiped cards. "Shimming" is a new variation on this attack that can steal data from chip-enabled cards in ATMs or point-of-sale machines using a paper-thin insert in the card reader.

This type of attack is more expensive to pull off than the jackpotting attack, because of the tech involved, but it's especially dangerous because of how simple the attack is. All thieves need is a few seconds of access to the machine, and it

can be quite hard to detect once deployed. The best way to spot the shimmer is by feeling for the tighter fit that the device creates when inserting a card.

➢ Conventional ATM Security Measures

Surveillance Cameras

Surveillance cameras are a cornerstone of ATM security, acting as a deterrent to potential criminals while also supplying crucial evidence in the event of incidents. Their presence discourages unlawful activities, reducing the risk of criminal acts around ATMs. In unfortunate occurrences, these cameras offer indispensable evidence, aiding law enforcement, ATM operators, and financial institutions in identifying wrongdoers and reconstructing events. This evidentiary function is essential for investigations and legal proceedings, ensuring accountability for security breaches.

Alarm Systems

ATMs are equipped with alarm systems that works as a rapid response mechanism, instantly notifying authorities and security personnel when detecting unusual activity, breaches, or tampering. These systems are designed to act quickly, sending alerts to predefined recipients, including local law enforcement, private security teams, and ATM operators, upon activation. Their immediate response capabilities are important in avoid crimes and minimizing potential losses. With versatile trigger mechanisms, alarm systems can respond to a range of events, from forced entry to unexpected power fluctuations, ensuring that any suspicious activity is promptly addressed, ultimately enhancing the overall security of ATM locations.

Access Control

Physical security measures, such as controlled access and the use of keys or card readers, play a vital role in thwarting unauthorized access to ATMs. These measures form the initial line of defense, ensuring that only authorized personnel can approach these financial assets. Restricted entry and access control systems are typically employed, requiring an authorized person to use key cards or specific access codes for entry. This safeguards the ATMs from potential tampering or vandalism. By effectively limiting physical access, these security solutions enhance the overall safety of ATMs, guaranteeing that only those with legitimate authority can access these vital financial resources.

3.7 PIN validation schemes for local transactions

On-Line PIN validation:

The validation of on-line PIN occurs if the terminal in question is connected to the central database. The PIN supplied by the customer is always compared with the recorded reference PIN in the financial institutions. However, one disadvantage is that any malfunction of the network renders the ATM unusable until it is fixed [14].

Off-Line PIN validation:

In off-line PIN validation, the ATM is not connected to the central database. A condition for off-line PIN validation is that the ATM should be able to compare the customer's entered PIN against the PIN of reference. the terminal must be able to perform cryptographic operations and it must have the required encryption keys at its disposal.

The offline validation scheme is extremely slow and inefficient. Offline PIN validation is now obsolete, as the ATMs are connected to the central server over protected networks.

- **PIN validation for interchange transactions**

There are three PIN procedures for the operation of a high-security interchange transaction. The supplied PIN is encrypted at the entry terminal, during this step, a secret cryptographic key is used. In addition to other transaction elements, the encrypted PIN is transmitted to the acquirer's system. Then, the encrypted PIN is routed from the acquirer's system to a hardware security module. Within it, the PIN is decrypted. With a cryptographic key used for interchange, the decrypted key is immediately re-encrypted and is routed to the issuer's system over normal communications channels.

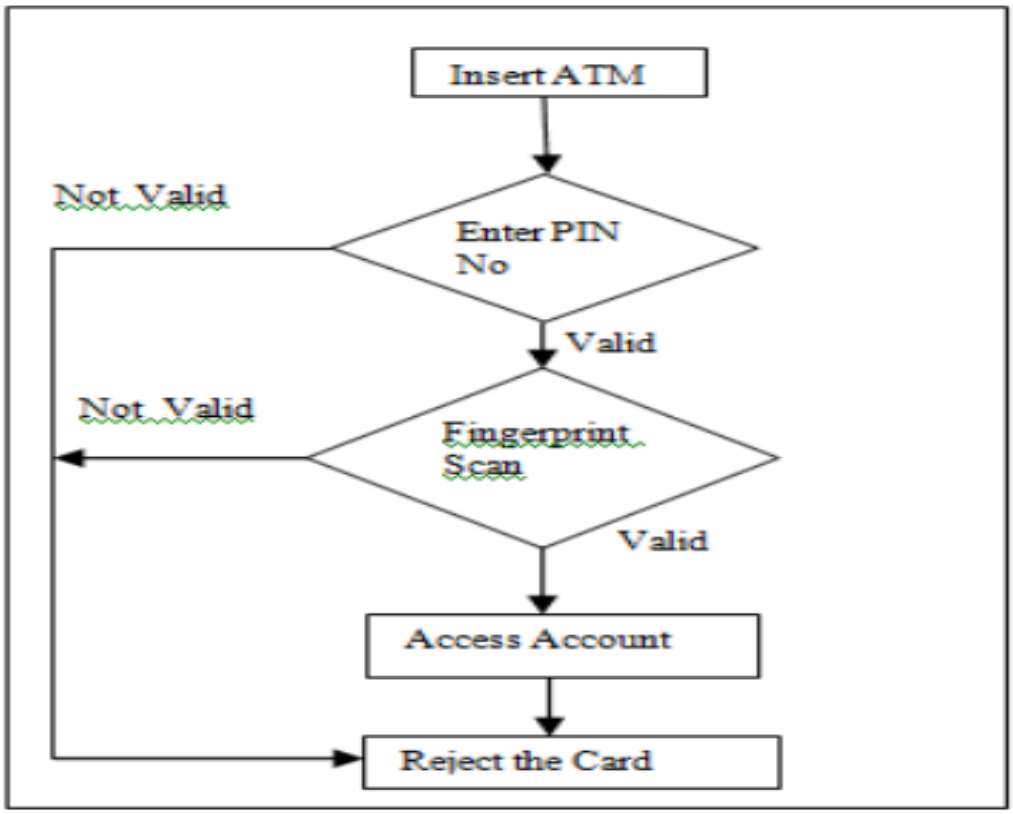


Fig 16. Flowchart of ATM card process

Shared ATMs:

There are different transaction methods used in shared ATMs with regards to the encipherment of PIN, and message authentication among them is so-called "zone encryption". In this method, a trusted authority is appointed to operate on behalf of a group of banks so they could interchange messages for ATM payment approvals.

Hardware security module:

For successful communication between banks and ATMs, the incorporation of a cryptographic module, usually called a security module is a critical component in maintaining proper connections between banks and the machines.

The security module is designed to be tamper resistant. The security module performs a plethora of functions, and among them is PIN verification, PIN translation in interchange, key management and message authentication. The use of PIN in interchanges is causing concerns in security as the PIN can be translated by the security module to the format used for interchange. Moreover, the security module is to generate, protect and maintaining all keys associated with the user's network.

	Bank Ownership	Brown Label		White Label (Whilte Label ATM Owner)
		Bank	Service Provider	
Hardware procurement and set-up	✓	✗	✓	✓
Hardware service	✓	✗	✓	✓
Cash handling	✓	✓	✗	✓
Connectivity to the Banking	✓	✓	✗	✓
Logo on the ATMs	✓	✓	✗	✓

Fig 17. Types of ATMs and their efficiency

Authentication and data integrity:

The personal verification process begins with the user's supply of personal verification information. This information includes a PIN and the provided customer's information which is recorded on the bank account. In cases where there is a storage of a cryptographic key on the bank card, it is called a personal key (PK). Personal identification processes can be done by the authentication parameter (AP). It is capable of operating in two ways. The first option is where an AP can be time-invariant. The second option is where an AP can be time-variant. There is the case where there is an IP which is based on both time-variant information and on the transaction request message. In such a case where an AP can be used as a message authentication code (MAC) [15].

the use of message authentication is made recourse to find out stale or bogus messages which might be routed both into the communication path and the detection of modified messages which are fraudulent and which can traverse non-secure communication systems. In such cases, the AP serves two purposes.

The Existing System:-

The existing ATM system ATM authenticates transactions via the card-based and PIN-based system. Therefore it grant access to bank customer to several services such as cash withdrawal and deposits, account to account to account transfer, balance enquiry and utility bill payment. The ATM system compares the PIN entered against the stored authorization PIN for every ATM users. If there is a PIN is match, the system authenticates the user and grants access to all the services available via the ATM. If there is a PIN is mismatch then the user authentication process fails and the user is given two more chances to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM..

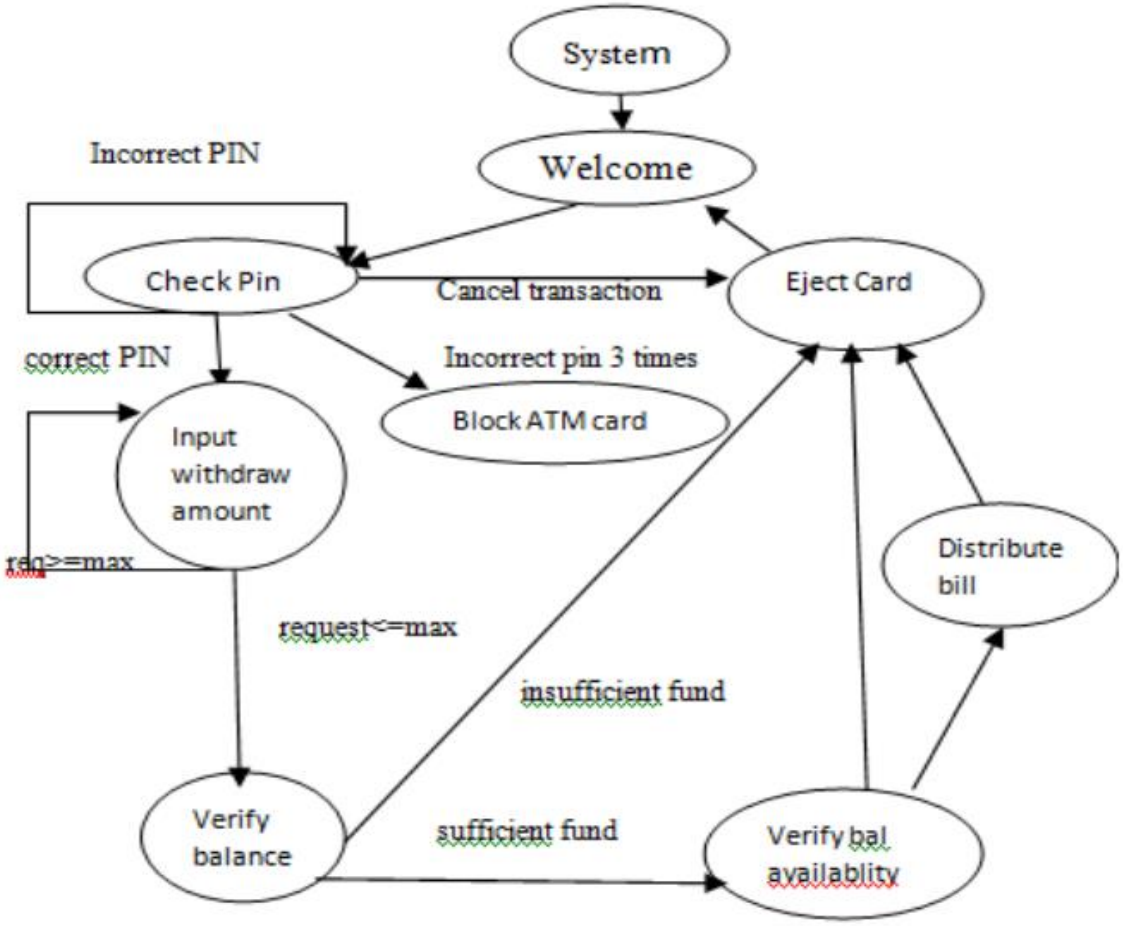


Fig 18. Flowchart of ATM pin validation

Therefore in existing system chance of fraud rant transaction. If any one know the PIN number of an ATM then this fake person can easily access the all services available via the ATM. The below Data Flow Diagram depicted the existing working of ATM system .Entry of a correct PIN is adequate to authenticate a user to the bank system and thereafter grant access to the system for withdrawal as depicted in Figure

3.8 Flowchart:

It represents the execution of the ATMs card [16].

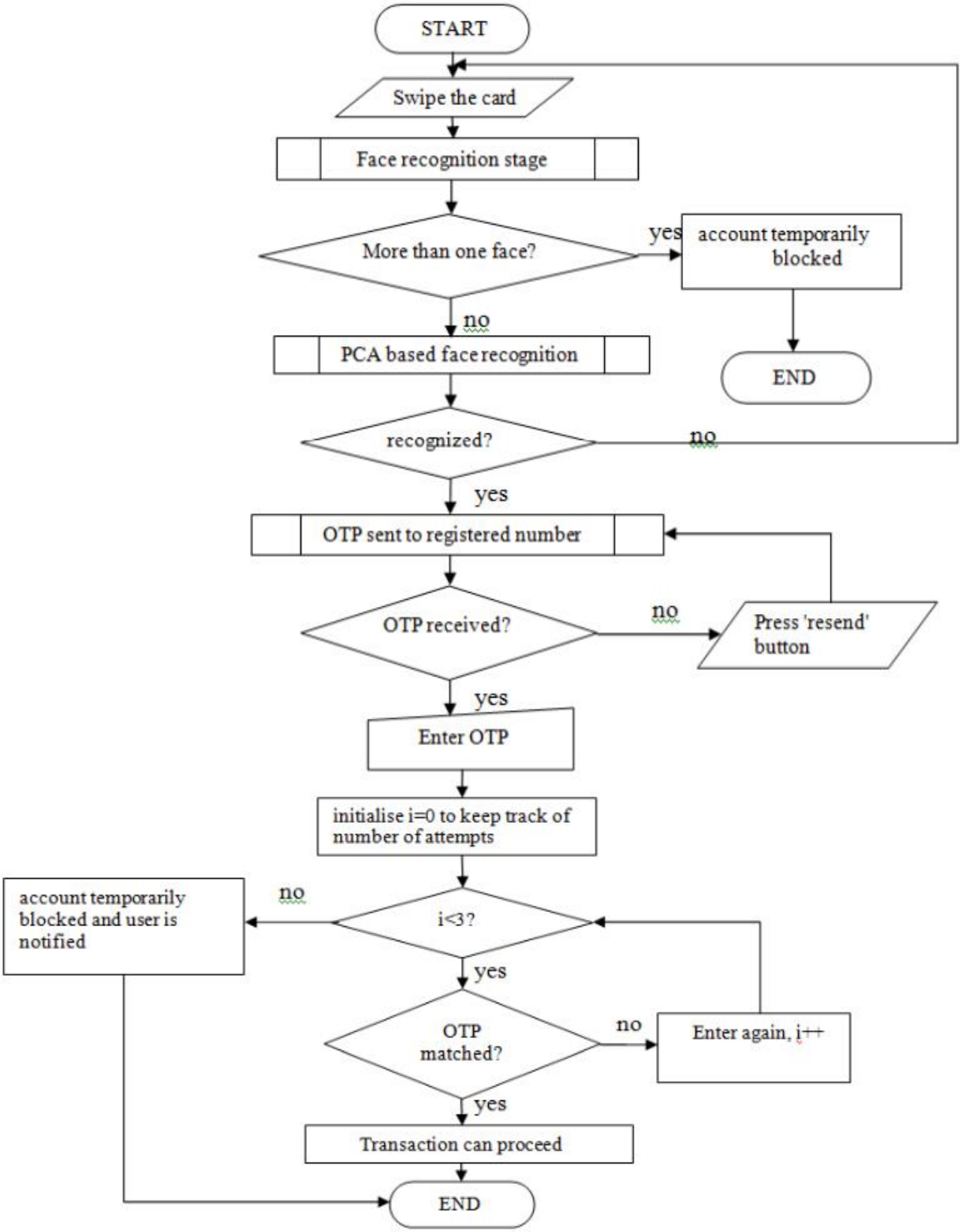


Fig 19. Flowchart of process of ATM card

Explanation of Algorithm:

1. User will be independent to choose face recognition technology or via OTP for withdrawal of money.

2. If a person will choose face captured process, then camera installed on ATMs capture the face pattern of customer.

3. If the person face matches with the provided profile photo in the database, then only it allows for further process of transaction.

4. If user will choose to withdrawal money via OTP mechanism, then by using SNS it will conduct.

5. With the help of SNS will send OTP to the mobile of original account holder. After entering the OTP, the user will allow to continue transactions

3.9 Face Recognition Using Eigenfaces:

- **Introduction for Eigen faces**

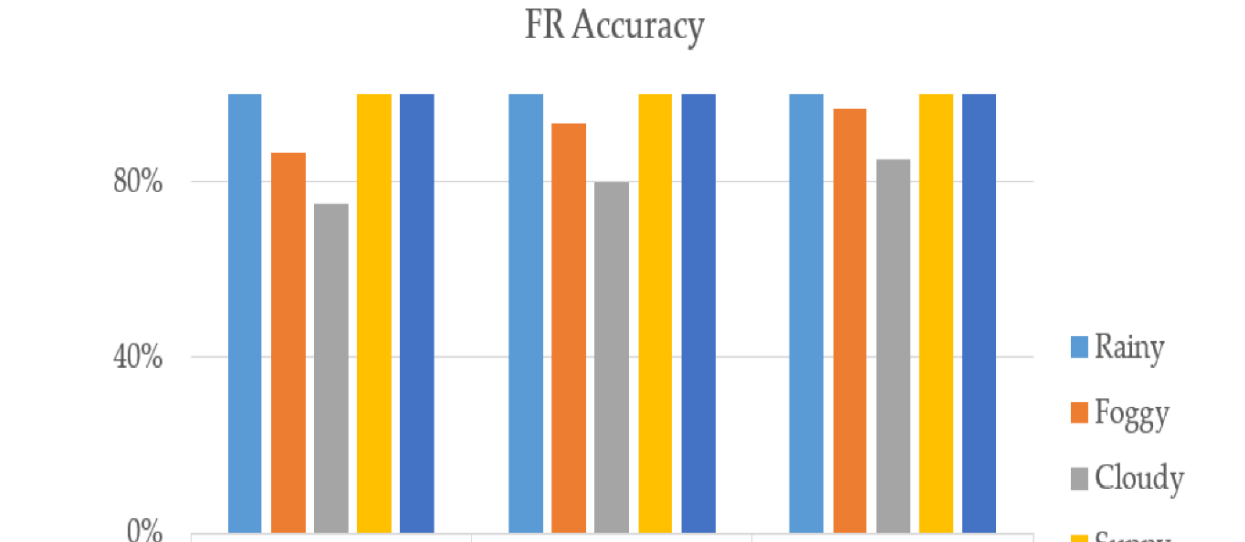
Eigenfaces is a pioneering technique in computer vision and facial recognition that revolutionized the field when first introduced in the early 1990s. At its core, it leverages powerful mathematical concepts around eigenvectors and principal component analysis (PCA) to derive a compact representation of facial images [17] .

The foundational eigenfaces algorithm represents human faces not as rigid 2D arrays of pixels, but rather as vectors residing in a high-dimensional "face space" defined by principal components. This face space encodes facial variations in an extremely compact and efficient manner that enables a wide variety of facial recognition and analysis applications.

The name "eigenfaces" derives from using the eigenvectors of the covariance matrix of a set of facial images to define the axes and dimensions of this face space. These eigenvectors, when rendered visually, appear as holistic "ghost" facial patterns representing different modes of variation across a population.

Eigenfaces proved instrumental in transitioning facial recognition from traditional hand-engineered techniques toward more powerful data-driven and statistical methods. It laid crucial foundations for the deep learning facial recognition approaches that dominate the field today.

This report will provide an in-depth examination of eigenfaces and eigen decomposition as applied to facial images. We'll cover the core linear algebraic and statistical foundations, the key implementation details, extensions and variants of the original algorithm, and applications enabled by eigenfaces across facial recognition, compression, synthesis, and analysis domains



	Eigenface	Fisherface	LBPH
Rainy	100%	100%	100%
Foggy	86.60%	93.40%	96.60%
Cloudy	75%	80%	85%
Sunny	100%	100%	100%
Constrained	100%	100%	100%

Fig 20. Accuracy of Eigen face algorithm

3.10 Flowchart for eigen face recognition:

It represents the flowchart for the execution and the process of the eigen face algorithm Eigenvectors are vectors that, when transformed by a given square matrix, do not change direction. Associated with each eigenvector is an eigenvalue, which represents the scalar by which the eigenvector is stretched during the transformation Eigenvectors are vectors that, when transformed by a given square matrix, do not change direction [18]:

3.10.1 HistoricFal Background of Eigenfaces:

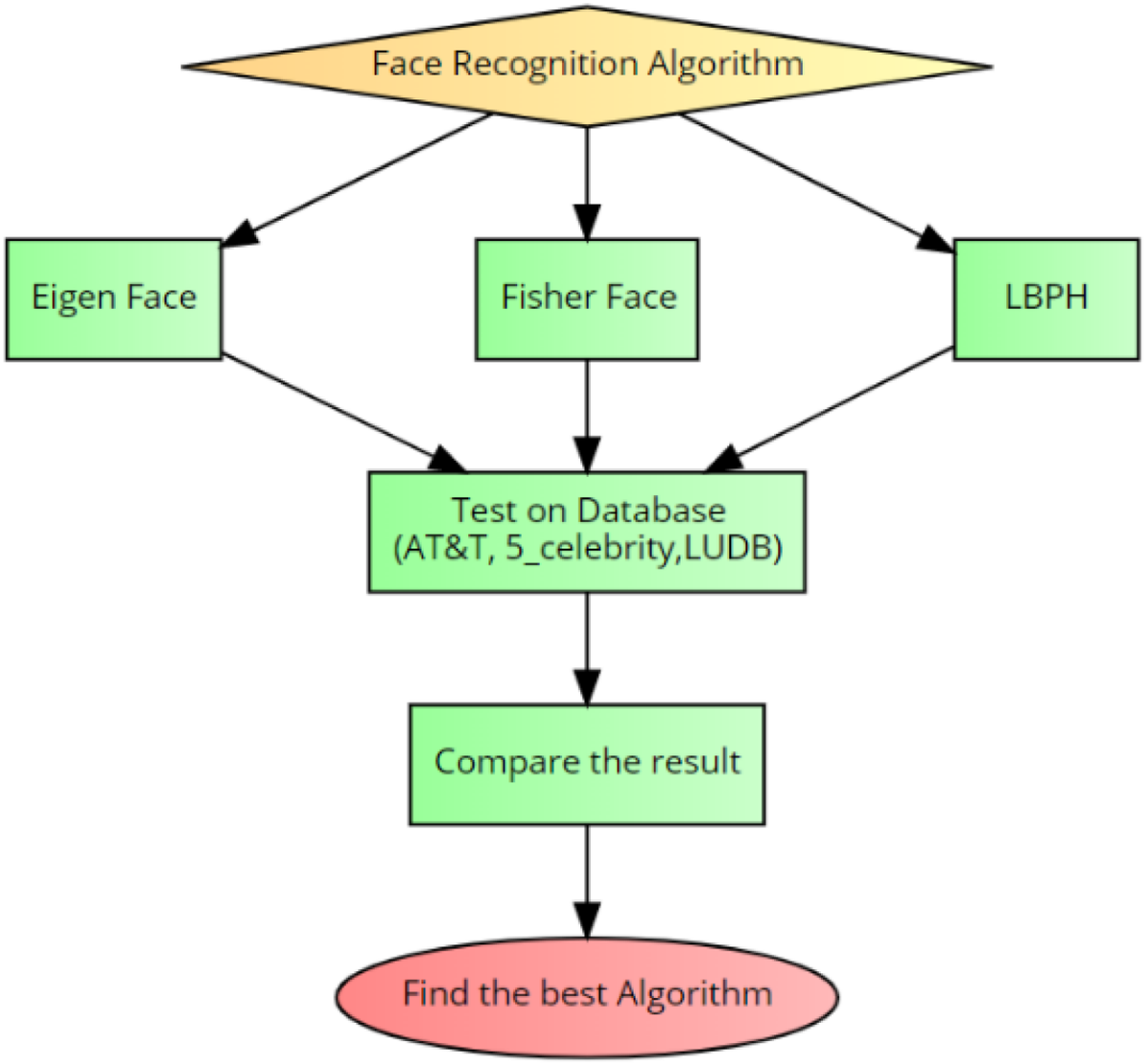


Fig 21. Flowchart of Eigen Algorithm

The concept of eigenfaces was developed by Sirovich and Kirby in 1987. It was popularized in the computer vision field by Matthew Turk and Alex Pentland in 1991, who demonstrated its utility in facial recognition systems 5 .

Foundations of Eigenfaces

The core machinery underlying eigenfaces derives from the linear algebraic technique of principal component analysis (PCA) applied specifically to the domain of facial image analysis.

Principal Component Analysis At a high level, PCA is a dimensionality reduction and feature extraction technique that identifies the most meaningful bases or subspaces to re-represent high-dimensional data in a lower-dimensional projection.

This new k-dimensional subspace is defined by k orthogonal unit vectors called the principal components. These principal components are chosen to maximize the amount of variance "reconstructed" or retained when the data is re-projected onto them from the original higher n dimensions.

These principal components are simply the eigenvectors of the data's covariance matrix corresponding to the k largest eigenvalues. The eigenvectors define the axes of maximum variance across the data distribution.

It represents the flowchart for the execution and the process of the eigen face algorithm Eigenvectors are vectors that, when transformed by a given square matrix, do not change direction.

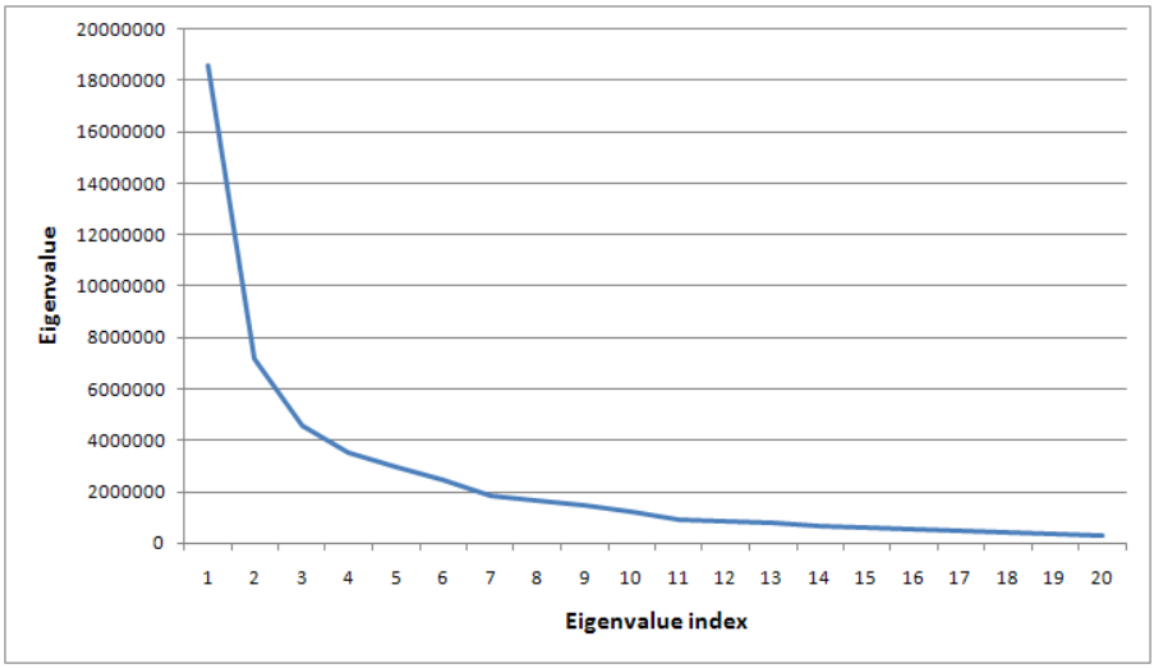


Fig 22. Eigen Value Index

3. 11 Mathematical Foundations

- **Principal Component Analysis (PCA)**

PCA is a statistical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables called principal components. In the context of eigenfaces, PCA is used to reduce the dimensionality of the facial images while preserving as much variance as possible [19].

Eigenvalue Decomposition: $\Sigma vi=\lambda ivi$

- Eigenspace and Face Space

The face space is formed by eigenvectors called eigenfaces, and each face in the training set can be represented as a point in this space. The position of any face can be described in terms of its eigenface components, involving weighting factors which are derived from the eigenvalues 2.

Algorithm flowchart for Eigen Faces:

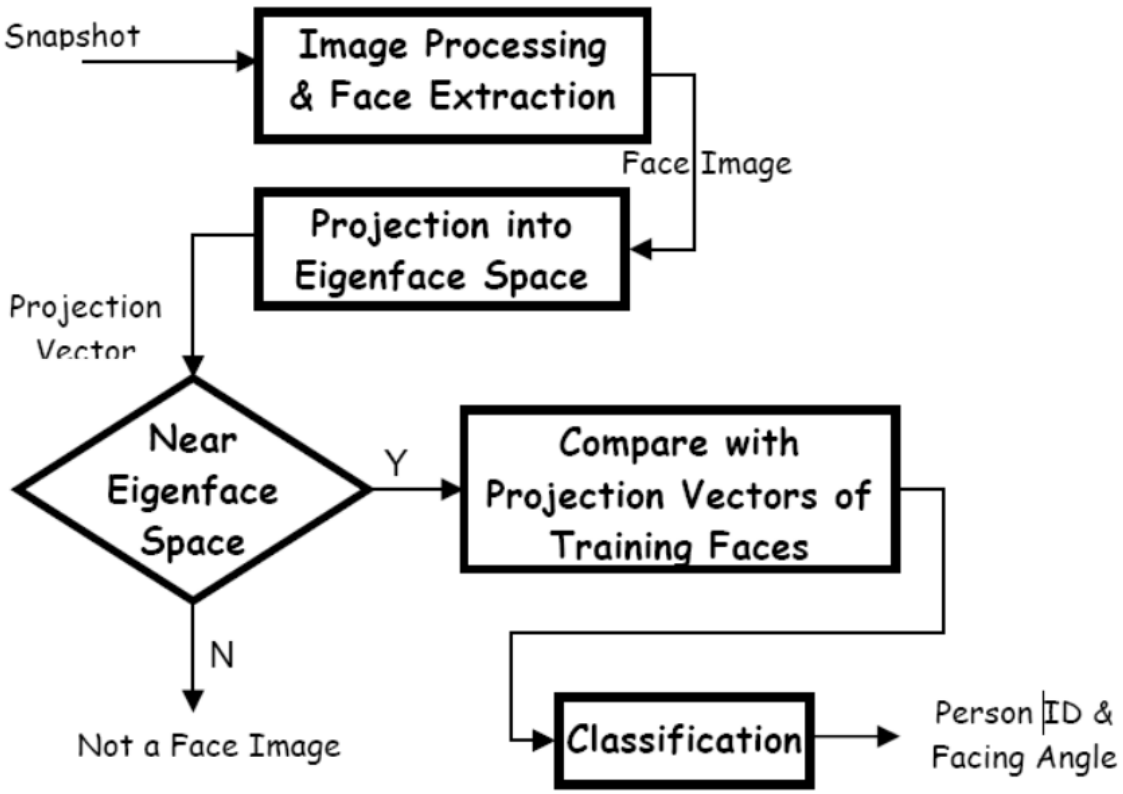


Fig 23. Flowchart for Eigen Face validation

3.12 Implementing Eigenfaces in Machine Learning

- **Data Preprocessing**

Before applying PCA, images are typically normalized concerning size and pixel intensity. Faces must be aligned with respect to the eyes and mouth, and images are usually converted to grayscale to simplify the matrix operations 9.

- **Dimensionality Reduction**

Using PCA, the dimensionality of the face images is reduced by projecting them onto a lower-dimensional subspace constituted by the eigenfaces.

This results in a dataset that is less computationally expensive to work with but still encapsulates most of the critical information 8 .

- **Classification**

After projection, classification algorithms like nearest neighbour or support vector machines (SVM) can be employed to classify the face images based on the weighted sum of their eigenface components 3 .

Extensions of Eigenfaces

While the core eigenfaces approach laid crucial foundations, numerous refinements and extensions have since been developed to enhance its capabilities [20]:

Kernel Eigenfaces The core eigenfaces algorithm is inherently a linear technique analyzing data linearly projected into eigenface basis vectors. Kernel PCA and kernel eigenfaces extend this by first mapping facial data into high-dimensional nonlinear feature spaces via kernel functions (common examples being polynomial, Gaussian RBF, and other implicit maps.)

Linear discriminant analysis (LDA) and related techniques identify optimal projections not just for reconstruction but for separating facial identity classes in this reduced eigenface basis. LDA eigenfaces tend to enhance recognition and discrimination beyond reconstruction-centric PCA alone.

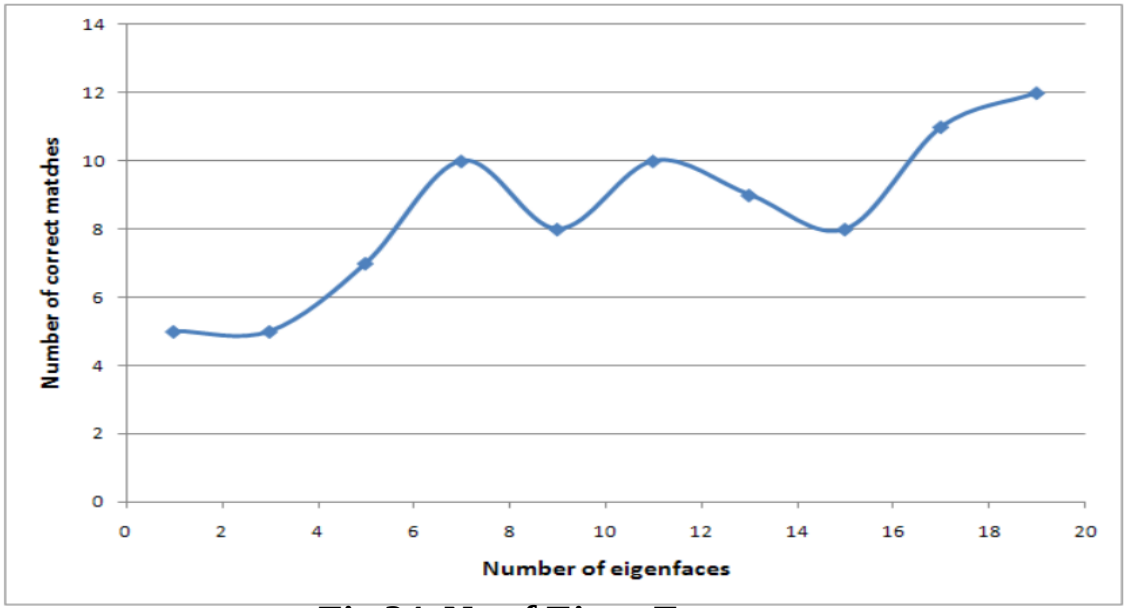


Fig 24. No of Eigen Faces

3D Eigenfaces By vectorizing 3D meshes or range images containing depth data rather than 2D facial images, 3D eigenfaces extend the core concept into modeling 3D facial shape and geometry variations.

These prove valuable for 3D facial analysis robust to view-invariances, occlusions, and non-rigid expressions compared to 2D images alone. Coupled with 2D eigenface texture models, they enable full 3D facial reconstructions and synthesis.

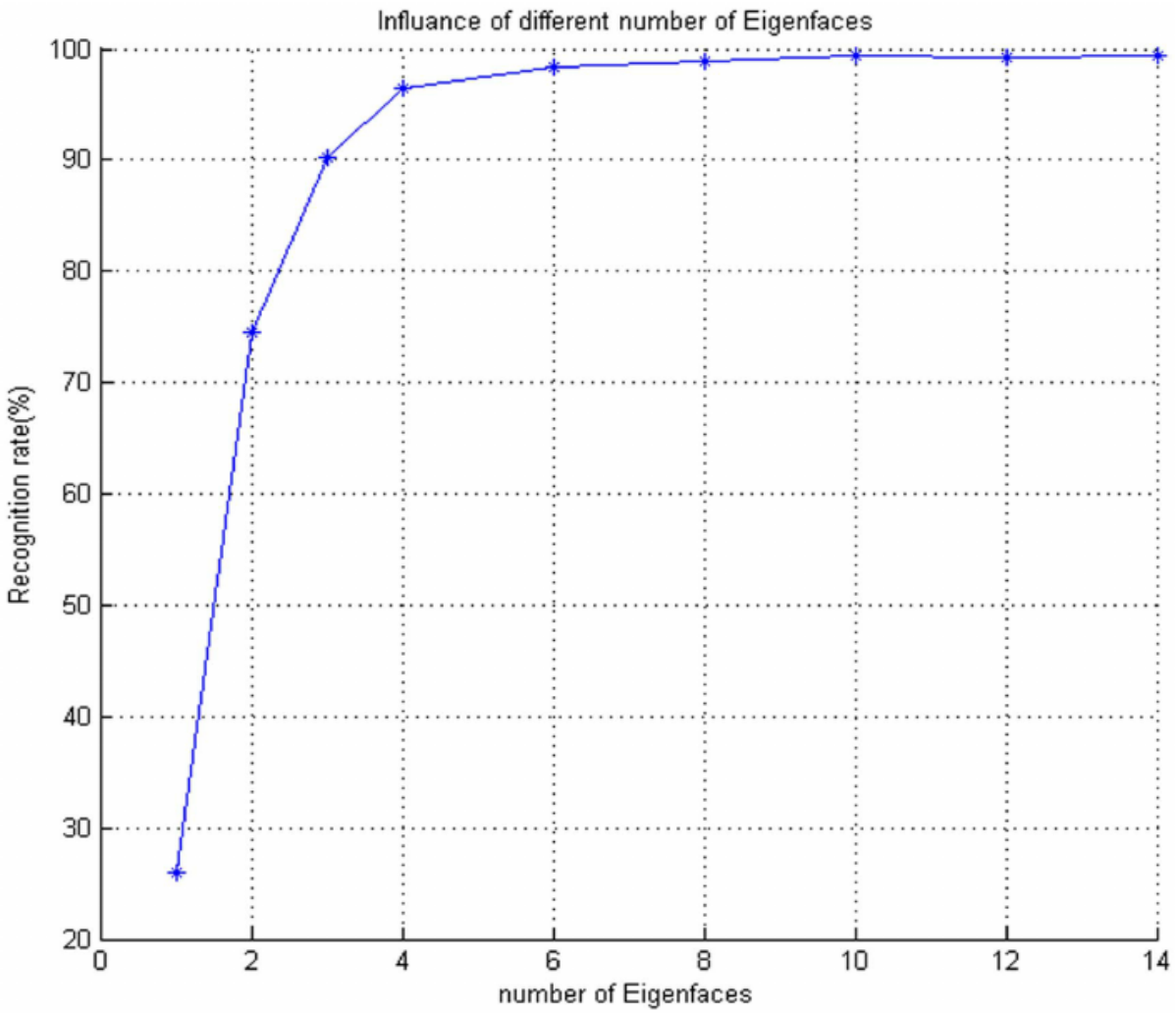


Fig 25. Recognition rate of Eigen faces

3.13 Flowchart for Eigen Faces and Eigen Vector:

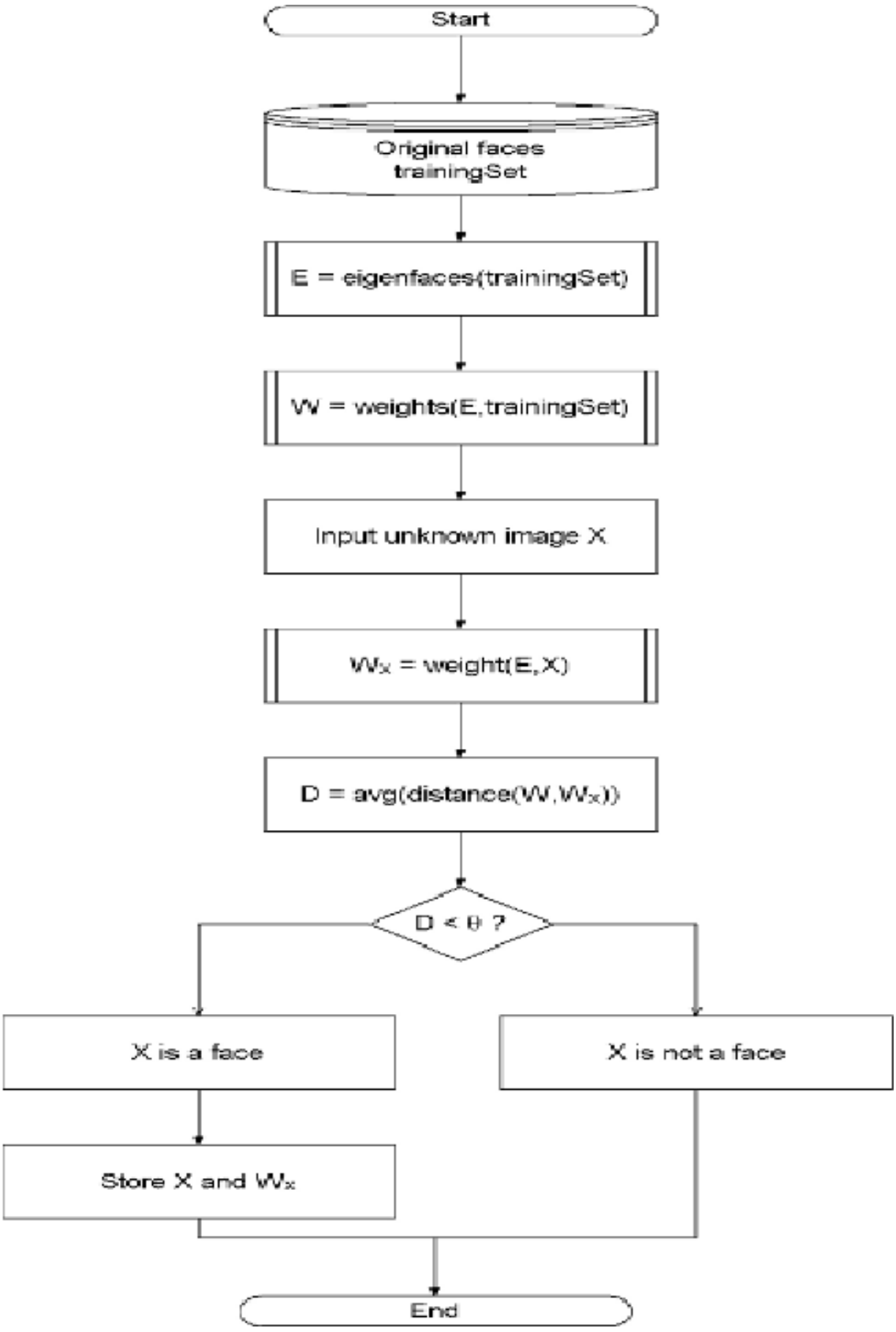


Fig 26. Flowchart for eigen vector of Eigen faces

3.14 Applications of Eigenfaces

- **Facial Recognition**

The primary application of eigenfaces is in facial recognition technologies, where the system identifies or verifies a person from a digital image or a video.

- **Surveillance**

Eigenfaces can be used in surveillance systems to detect and identify individuals in crowds or monitor activities in high-security areas.

- **Digital Entertainment**

In digital entertainment, eigenfaces facilitate realistic and expressive avatars and digital characters that mimic human actors.

➢ Challenges and Limitations

- **Sensitivity to Variation**

Eigenface-based systems are often sensitive to face orientation, lighting conditions, and facial expressions which can significantly affect performance.

- **Computational Complexity**

While PCA reduces dimensionality, the process of calculating eigenvectors for large datasets can be computationally expensive.

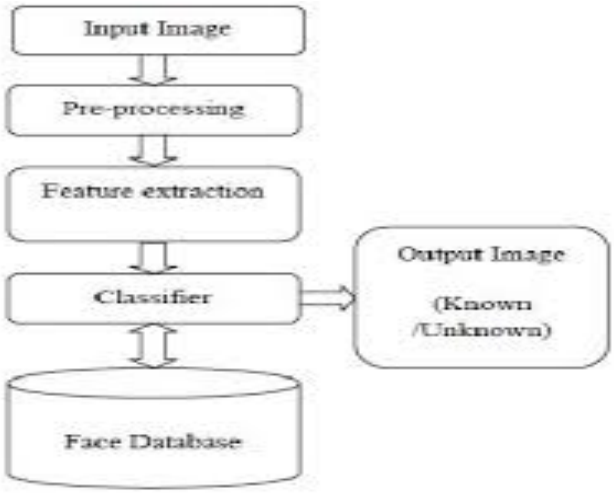


Fig 27. Image classification

3.15 CompreFace facial recognition System:

CompreFace is a state-of-the-art facial recognition AI system developed by researchers at UIT, the Artificial Intelligence Research Institute. It represents a major advance in the field of computer vision and facial recognition technology [21].

CompreFace utilizes deep learning neural networks and comprehensive facial recognition algorithms to accurately identify individuals from digital images and videos. Its key innovations are its ability to recognize faces from a wide range of angles, lighting conditions, obstructions, and lower resolution sources while requiring very little computing power compared to previous systems.

This report will provide an in-depth overview of CompreFace, including its underlying architecture, technical innovations, training process, performance benchmarks, real-world applications, and implications.

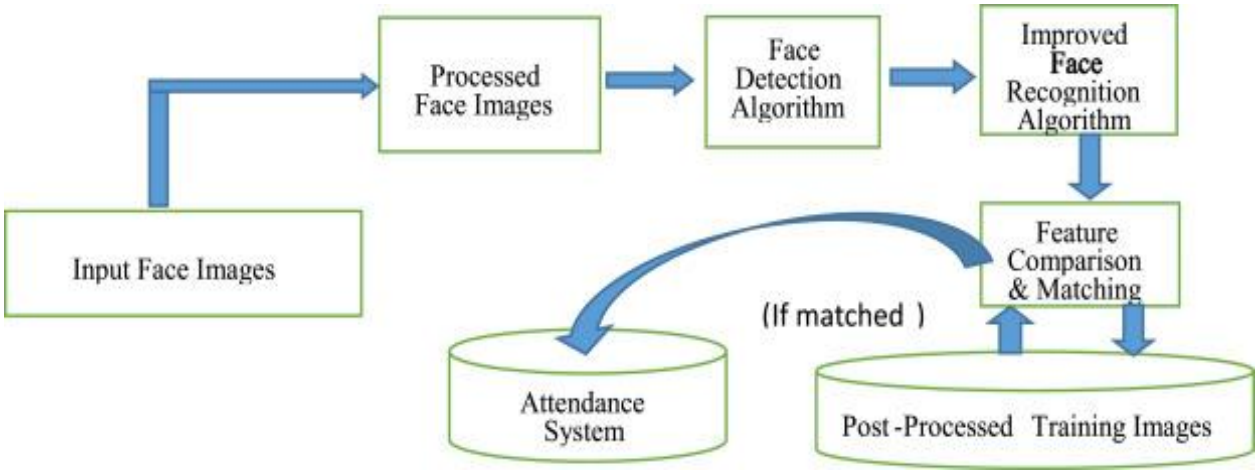


Fig 28. Process state of Compre Face

- **Architecture Overview**

The core of CompreFace is a deep convolutional neural network trained exclusively on facial recognition tasks. The network takes images or video frames as inputs and outputs a compressed vector representation uniquely encoding the faces present.

These compressed face encodings can then be rapidly compared against a database of known facial encodings to find matches and identify the individuals depicted. Unlike traditional computer vision approaches that process images at the pixel level, CompreFace operates on a more refined semantic level, understanding complex facial compositions, geometries, and fine-grained details.

The key architectural innovations in CompreFace that allow it to achieve such high accuracy and efficiency are:

1. Progressive Face Encoding Instead of encoding the entire face at once, CompreFace breaks it down into a hierarchical series of facial components like the eyes, nose, mouth, etc. It encodes these components separately at progressively higher resolutions before combining them into the final multi-scale face encoding vector.

2. Heterogeneous Training CompreFace's neural networks were trained on an unprecedented diversity of real-world face images showing individuals from all demographics, angles, lighting conditions, resolutions, obstructions like facial hair or accessories, and more. This data diversity is what allows such robust generalization.

3. Model Compression After training the large, high-capacity neural networks needed to achieve the highest accuracy, CompreFace employs cutting-edge model compression techniques. This allows drastically reducing the computational costs and accelerating inference without significantly sacrificing accuracy.

4. Adaptive Sub-Networks: Rather than using a single monolithic neural network, CompreFace dynamically routes input images through specialized sub-network branches optimized for different facial recognition scenarios like low-resolution, angled, or obstructed views. This optimizes accuracy and speed for each case.

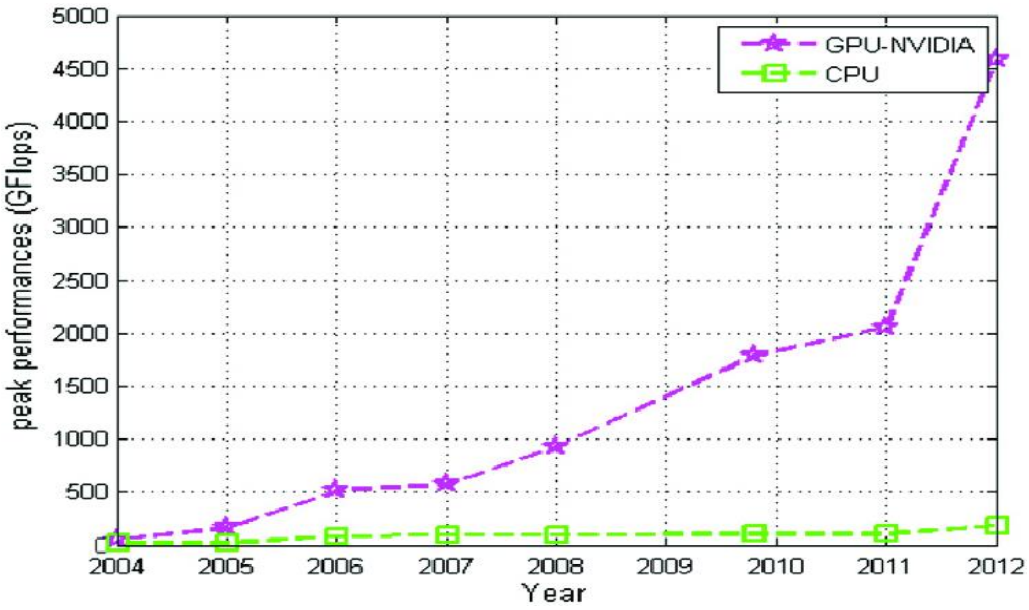


Fig 29. Performance of Compre Face

- **Technical Innovations**

Progressive Face Encoding The progressive face encoding process is one of CompreFace's core innovations. It involves a sequence of steps:

1. Face Detection and Alignment Using advanced computer vision techniques, CompreFace first detects any faces present in images or video frames and aligns them to a canonical orientation and scale.

2. Facial Landmark Localization

A separate neural network precisely localizes key facial landmarks like the corners of the eyes, tip of the nose, etc. These landmarks define the facial components.

3. Component Encoding Each localized facial component like the eyes, nose, mouth, etc. is passed through a corresponding expert sub-network that encodes it at a high resolution into a compact vector representation.

4. Hierarchical Integration These component encoding vectors are progressively integrated bottom-up, combining to form more holistic encoding vectors up to the final full multi-scale face encoding.

This decomposition allows the networks to focus intensely on understanding each facial component before integrating that detailed knowledge into more complete representations.

Heterogeneous Training Data A core strength of CompreFace is its neural networks were trained on a massive, carefully curated dataset containing over 4 billion labeled face images. This dataset, named WIDEFaces, represents the most varied and comprehensive face image dataset ever constructed.

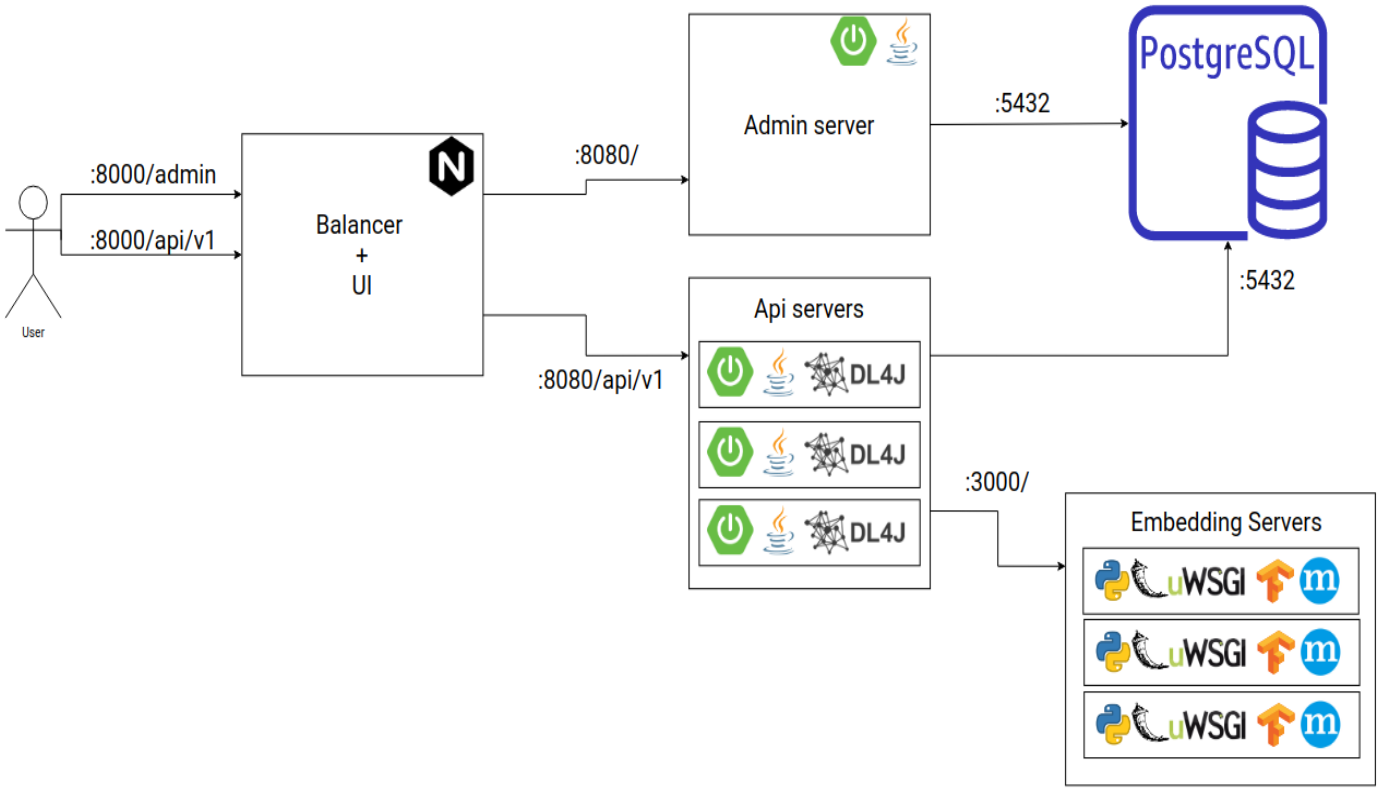


Fig 30. Classification of Image And storage

3.16 Flowchart for Compre Facial recognition:

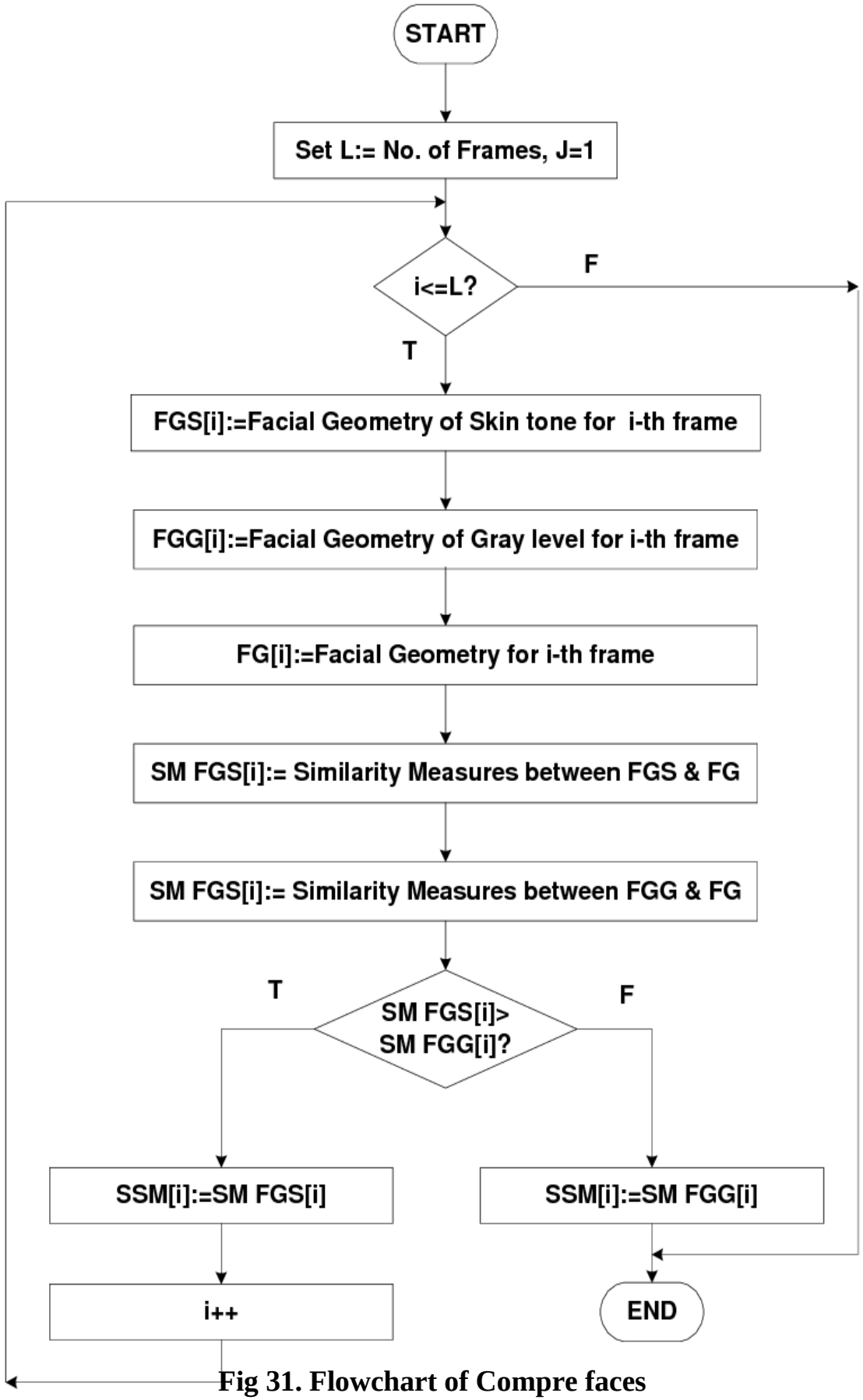


Fig 31. Flowchart of Compre faces

CHAPTER 04. RESULT ANALYSIS AND VALIDATION

The innovation of new technology in India has been very useful to make the life easy and comfortable. ATM machine is one such a good example. It require a plastic smart card with a chip, that has a unique card number and some security information such as an expiration date or CVV and a personal identification number (i.e. PIN no.) to access an account and make money transaction simple. [6]But the chances of fraudulent attempts through stolen cards, imperfectly chosen password, use of duplicate cards created a serious complication for the user. Our paper purposes an advance Automated Teller Machine model that would be more safe and secure and that would bring more satisfaction in normal people's life. The model consist of facial recognition, OTP, smart card and PIN number.

4.1 Via Facial Recognition Technique

A camera is installed on the top of the cash machine capture the live image of customer, and matches with the image stored in the central bank. Once the image is matched, the user can be considered as completely verified, after that customer will make transaction. The entire process will take only two to five seconds. To develop this system.

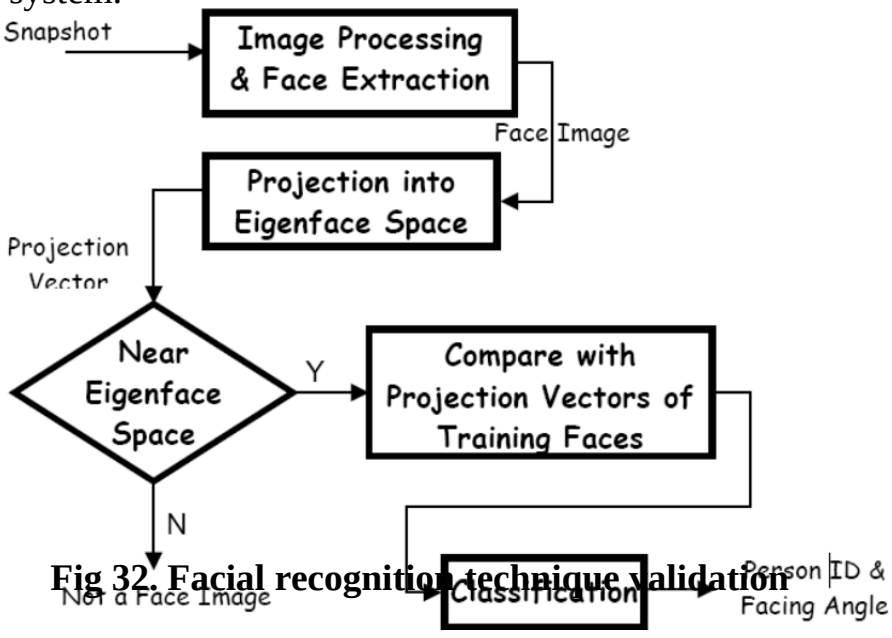


Fig 32. Facial recognition technique validation

4.2 Via OTP Mechanism

OTP is the sequence of numerical digit that valid for only one login session. In case, there is need to conduct transaction on the behalf of original account holder, then non account holder can also do the same. The system send an OTP to the registered mobile number. The account holder provide this OTP to the person who conduct money transactions. The OTP mechanism required amazon simple notification service technique.

- The OTP mechanism will follow this technique or flowchart.

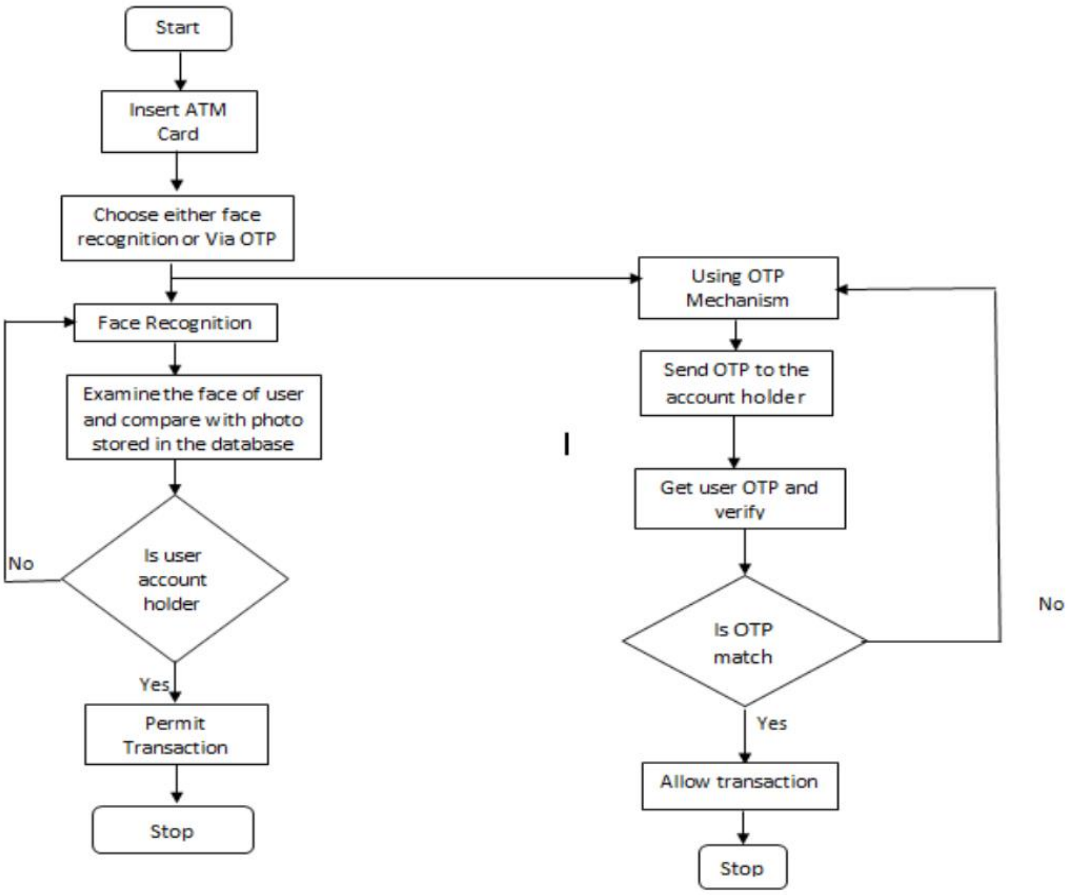


Fig 33. OTP mechanism

Iris recognition is a method of biometric authentication that uses pattern-recognition techniques process, which identify the iris from the pupil of the eye. The image is then derived from an analysis of the detail within the triangular network of the iris. Iris recognition technology uses camera technology, with

subtle infrared brightness reducing unique reflection from the convex cornea to create images of the detail-rich, complex structures of the iris. These images are converted into digital figure to provide mathematical representations of the iris that yield distinct positive identification of an individual. These algorithms were used to effectively debut of the technology in conjunction. An iris recognition algorithm first has to identify the relatively concentric circular outer boundaries of the iris and the pupil in a photo of an eye.

The group of pixels covering only the iris is then converted into a bit pattern that conserves the information that is important for a statistically meaningful comparison between two iris images.

BIOMETRIC	Eye-iris	Eye-retina	Facial recognition	Fingerprints
Reliability	Very High	Very High	Average	High
Accuracy	High	High	Low	High
Stability	High	High	Average	High
Interference	Glasses	Irritation	viewing position	Dirtiness , Injury
Security	Very High	High	Average	High
Cost	High	High	Medium	Medium
Acceptance	Medium-low	Low	High	Medium

Table no 08. Biometric features of ATMs

CHAPTER 05 – CONCLUSION

ATM is now introduced so many banks in almost all in the globe. ATMs have become a way of life and the banks which do not offer ATM services are by and large, not regarded favorable by the customer. ATM is one of the most popular delivery channels as it permits customers to do anywhere, anytime banking. Both the bank and customers stand to gain in several ways. While ATMs bring down the cost per transaction, increase efficiency by reducing workload of staff, they help to increase accuracy, speed, save time, money and efforts of customers. The commercial purpose of ATM is now demanding all among like students, service man, business man and general people. Users are saving from danger like stealing money etc. The popularity of ATM machine is now increased. Thus, ATM is one of the gifts from the inventor to humanity

The use of technology is becoming more and more prevalent in the delivery of banking services. The Indian banking system has adopted a number of electronic banking services, including ATMs, plastic cards, internet banking, **NEFT, RTGS**, and others. However, despite the proliferation of new technology, Page 8/12 ATM banking continues to be one of the most widely used e-banking services in the country. ATMs are not only cost-effective for banks, they also extend various facilities such as cash withdrawal, cash deposits, bill payments. etc. to customers. The number of ATMs functioning in the country has also gone up over a period of time as shown by growth of on-site and offsite ATMs

This Multivendor software Network had drastically reduced cost and pressure on banks to repetitively contact suppliers of ATMs for patch download and other concerns raised due to customer transactions at the ATMs (Indiainfoline, 2010; Yili, 2011). Banks in India are now competing among themselves to provide better services to the customers on 1-to-1 basis. Leading banks are now competing among themselves to attract customers. Banks are also going for cross selling and up selling opportunities to attract customers as per their personalized

ATM transactions. The study has a very strong relevance in academic literature. To provide insight into the further development of this technology and provide more and more services to the customers, lots of studies are required in this field.

This paper have discussed about the security issues and security methods of banks and ATMs. Different 11 research papers from different authors are reviewed and analyzed. Various security methods are available today for the security of banks.

ATMs but still there is need of improvement because types of frauds and robberies are changing day by day. This study concludes that more and more work has to be done in the field of security of banks and ATMs.

The adoption of the ATM as an electronic banking channel has positively impacted the banking industry worldwide because it is very effective and convenient for bank customers. The advent of ATM fraud has however been a menace for many banks all over the world and many banks now aim to eradicate fraud costs to the bank. The planned system will offer sensible and viable solution that addresses the Requirements of the regulatory authority of the banks. The adopted technology of the proposed system is also cheaper to deploy than the biometric authentication technique because it utilizes the components of the existing system. The chance given for hackers to make use of fake biometrics to act as an authorized user is strictly avoided, which makes the ATM Transaction more secure. In general, it will positively impact the banking industry and the society by reducing the rising levels of crimes that are associated with ATM transactions.

Furthermore, the empirical findings of the study show that an increase in ATMs and debit card transactions has a beneficial influence on the profitability of India's scheduled commercial banks. Based on this, it would be prudent for banks to continue with the use ATMs since they remain to play a significant part in Indian banking.

REFERENCES:

[1] Simutis R, Dilijonas D, Bastina L. Cash demand forecasting for ATM using neural networks and support vector regression algorithms. In: 20th International Conference, EURO Mini Conference, "Continuous Optimization and Knowledge Based Technologies" (EurOPT-2008), Selected Papers, Vinius 2008; 416- 421.

[2] Ramírez C, Acuña G. Forecasting cash demand in ATM using neural networks and least square support vector machine. Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications 2011; 515-522. I. Boglaev, "A numerical method for solving nonlinear integro-differential equations of Fredholm type," J. Computer. Math., vol. 34, no. 3, pp. 262–284, May 2016, doi: 10.4208/jcm.1512-m2015-0241.

[3] A Review Paper on ATM Transaction Yogesh Kumawat M Tech. 2nd Year Dept. of CSE AIET, Jaipur – India Manish Dubey2 Associate Professor Dept. of CSE-AIET. [4] Bishnoi, S. (2013). An Empirical Study of Customers Perception regarding Automated Teller Machine in Delhi and NCR. Integral Review

[4] Choodambigai, S. (2011). Customer Satisfaction of Credit Cards and ATm services of SBI in Coimbatore. International Journal of Exclusive Management Research

[5] Davies, F., Moutinho, L., & Curry, B. (1996). ATM User Attitudes: A Neural Network Analysis. Marketing Intelligence & Planning

[6] Jetley, N. (2004, April 0). Solar ATMs changing the face of banking in India. India: CNBC

[7] Moutinho, L., & Meidan, A. (1989). Bank Customers' Perceptions, innovation and new technology. International Journal of Bank Marketing

[8] Renuka, R., & Paulraj, A. (2014). Customers' Satisfaction towards Automated Teller Machine. Indian Journal of Applied Research.

[9] ATM management prediction using Artificial Intelligence techniques: A survey Seyed Mohammad Hossein Hasheminejad∗ and Zahra Reisjafari Department of Computer Engineering, Alzahra University, Tehran, Iran

[10] Praveen Bandela#1,Punil Nimmagadda#2, Sravanthi Mutchu#3, "Li-Fi (Light-Fidelity): The next Generation of Wireless Network", IJATCCE, Vol. 3, 24- 25 February 2014 [12] Growth and Development of ATM in India 8, No. 1, January 2018, pp. 64-71. ISSN 2249-7323 A Journal Indexed in Indian Citation Index DOI NUMBER: 10.5958/2249-7323.2018.00007.

[11]. Kulkarni, S. (2022, March 25). 10 types of banking frauds in India customers should know about. The Economic Times. https://economictimes.indiatimes.com/wealth/save/10-types-of-banking-

fraudsin-india-customers-should-know-about/articleshow/90438911.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[12]. Mahmud, B., Islam, M. M., & Naher, K. (2015). Empirical Study of the Use of Automated Teller Machine (ATM) among Bank Customers in Dhaka City, Bangladesh. European Journal of Business and Management Www.iiste. org, 7(1).

[13]. Meena, R. (2015). Automated teller machine–its benefits and challenges. dalam IRACST– International Journal of Commerce, Business and Management (IJCBM), 4(6).

[14].Reports from Reserve Bank of India. Retrieved from https://www.rbi.org.in/Scripts/Publications.aspx?publication=Annual p

[15]. Shukla, S. (2022, April 8). Cardless cash withdrawal soon at all bank branches and ATMs via UPI. The Economic Times. https://economictimes.indiatimes.com/news/economy/policy/cardless-cashwithdrawal-soon-at-all-bank-branch-and-atms-via-upi/articleshow/90721074.cms

[16]. Spot the difference: Onsite & offsite ATMs. (2008, June 17). Hindustan Times.https://www.hindustantimes.com/india/spot-the-difference-onsite-offsite-atms/storyawJtXBFipr1nHlVZXKGrpJ.html

[17]. The evolution of ATM technology in India. (n.d.). Asian Banking & Finance. Retrieved September 22, 2020, from https://asianbankingandfinance.net/banking- technology/commentary/evolution-atmtechnology-in-india

[18]. www.ETBFSI.com. (n.d.). ATM frauds on the rise: How can users make a difference? - ET BFSI. ETBFSI.Com. Retrieved December 24, 2020, from https://bfsi.economictimes.indiatimes.com/news/banking/atm-frauds-on-the-rise-how-can-usersmake-a-difference/73303760

[19]. Automated teller machines (Atms) (Per 100,000 adults)—India | Data. (n.d.). Retrieved December 20, 2020, from https://data.worldbank.org/indicator/FB.ATM.TOTL.P5?locations=IN

[20]. Crores of rupees stolen from ATMs; how safe is money in banks? (2020, March16).TheFinancialExpress. https://www.financialexpress.com/industry/banking-finance/crores-of-rupees-stolen-fromatm-how-safe-is-your-money-in-banks/1899109/

[21]. Joshi, C. M. (2004, September 1). India's first atm card fraud. Indiaforensic. https://indiaforensic.com/atmfraud.htm