IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907151 |

One Touch Multi Banking Transaction ATM System Using Biometric and GSM Authentication

S.Hariharan, Ranjith Kumar.R, Hariprasath.B, Nivetha.K

Assitant Professor, Department of Electronics and Communication Engineering, Knowledge Institute of Technology, Kakapalayam, Salem, India

UG Student, Department of Electronics and Communication Engineering, Knowledge Institute of Technology, Kakapalayam, Salem, India

UG Student, Department of Electronics and Communication Engineering, Knowledge Institute of Technology, Kakapalayam, Salem, India

UG Student, Department of Electronics and Communication Engineering, Knowledge Institute of Technology, Kakapalayam, Salem, India

ABSTRACT: People need to carry numerous ATM cards for transactions because they have various bank accounts with different banks, and each account may have a separate PIN. Traditional ATM terminal customer recognition systems rely solely on bank cards, security pin numbers, and other identity verification methods, which are not perfect and have too few functions, and there are times when we forget our security PIN numbers, lose our cards, have our cards stolen, or have our PIN numbers stolen. To address the flaws in traditional ATM systems, a new customer recognition technology for ATM terminals called "One Touch" was introduced. Biometric and GSM Authentication for Multi-banking Transactions". Unauthorized access is prohibited because fingerprints are unique identifier for everyone. Biometric based fingerprint authentication technology is one of the most secure systems. This technology also ensures a secure GSM transaction (OTP-One Time Password). In comparison to the existing ATM system, the suggested system has minimal risk overhead in managing numerous account transactions and achieves excellent security. Human identification from face pictures, on the other hand, does not require it. As a result, face recognition plays an important part in determining a person's identification since it does not require human collaboration, which is a distinct benefit of face recognition over other biometric approaches.

I.INTRODUCTION

An ATM (Automated Teller Machine) is a machine that allows bank account holders to perform transactions without the need for human involvement at any time. Customers authenticate themselves in an ATM system by using an ATM card, which is a plastic card with a magnetic stripe on it. The magnetic stripe contains information about the consumer. Data on magnetic stripes can be readily erased by high magnetic fields on occasion. When it comes to PINs (Personal Identification Numbers), each account has its own PIN. In a typical ATM system, we may forget our PINs or become confused. As a result, the ATM card has a variety of downsides, such as damaging the card, losing the card, having it stolen, losing the PIN, forgetting the PIN, and so on, all of which increase the risk of fraud. All ATM users are always trying to keep their every transaction under secure observation, but in the case of money, security is still a big issue. When it comes to ATM machines, the most important consideration is physical security, which focuses on guaranteeing access limitation, recognition, and validation. The traditional PIN-based technique to user identification in banking transactions is increasingly scarce these days. The biometric approach is based on a user's bodily characteristic, which is unique and permanent for each individual. Because each person's fingerprint is unique, fingerprint recognition is the most secure system. This prohibits unauthorised access to a customer's bank account. It functions as a latch that only unlocks if the right key, i.e. an approved fingerprint, is located. Because the skin of our hands and feet shows a stream arrangement of hills on every tip of the finger, biometric authentication has been proven to be accurate. In the field of biometrics, face identification from pictures is a prominent topic of study. Due to such difficulties, one of the most valuable uses of face recognition has the highest risk of fraud. The ATM system offers customers with services 24 hours a day, seven days a week for simple transactions, but as the usage of ATMs grows, so do fraudulent assaults on

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907151 |

the ATM system. As a result of these difficulties, there are more opportunities for fraud. The ATM system offers customers with services 24 hours a day, seven days a week for simple transactions; nevertheless, as the usage of ATMs grows, so do fraudulent attacks on the system. All ATM users are always trying to keep their every transaction under secure observation, but in the case of money, security is still a big issue. When it comes to ATM machines, the most important consideration is physical security, which focuses on guaranteeing access limitation, recognition, and validation. As the current ATM system in the market has various drawbacks because ATM cards are made up of plastic cards on which a magnetic strip is mounted for storing data such as user details, it is possible that the magnetic strip will become neutral due to strong magnetic fields. There are also other drawbacks such as forgetting our PINs and losing our ATM cards. Our cards are taken on a regular basis. To get the codes, robbers utilise illegal card readers rather than approved card readers. Hackers also utilise duplicate devices to get unauthorised access to users' bank accounts. The usual method, because such difficulties increase the risk of fraud. The ATM system offers customers with services 24 hours a day, seven days a week for 11 simple transactions; but, as the usage of ATMs grows, so do fraudulent assaults on the system. When it comes to ATM machines, the main issue is physical security, which focuses on guaranteeing limitation of access, recognition, and validation. In the case of finance, however, security may sometimes become a big problem. Because ATM cards are made up of plastic cards on which a magnetic strip is mounted for storing data such as user details, it is possible that the magnetic strip will become neutral due to strong magnetic fields. There are also other drawbacks such as forgetting our PINs, losing our cards, and having our cards stolen. To get the codes, robbers utilise illegal card readers rather than approved card readers. Hackers also utilise duplicate devices to get unauthorised access to users' bank accounts. The traditional PIN-based technique to user identification in banking transactions is increasingly scarce these days. The biometric approach is based on a user's bodily characteristic, which is unique and permanent for each individual. In This necessitates the integration of biometric technologies into regular ATMs. Fingerprint-based biometric authentication systems are becoming increasingly widespread across the world. In Because each person's fingerprint is unique, fingerprint recognition is the most secure system. This prohibits unauthorised access to a customer's bank account. It functions as a latch that only unlocks if the right key, i.e. an approved fingerprint, is located. Because the skin of our hands and feet shows a stream arrangement of hills on every tip of the finger, biometric authentication has been proven to be accurate.

II.LITERATURE SURVEY

A Self-Banking Biometric M/C featuring Fake Detection for Fingerprints and Iris, as well as GSM Technology for OTP:

The rising number of direct or spoofing fraudulent assaults by thieves has prompted us to place a higher priority on money transaction security. Biometrics' precision in identifying is causing a surge in its use. The approach described in this article focuses on how money transactions in an ATM machine will be protected by evaluating biometrics such as fingerprints and iris patterns, which are recognised for their consistency and diversity. The use of biometrics allows for paperless banking as well as smart ATM access. In this method, the banker must take and record samples of the client's fingerprint and iris, as well as the customer's registered cellphone number, in the database before the consumer may use the ATM. The system's true operation begins when a consumer uses the ATM to execute a money transaction. The samples of fingerprints and iris will be taken and compared. By comparing it to the samples recorded in the database during registration, the system will be able to differentiate between genuine legitimate traits and false self-manufactured synthetic or rebuilt samples. After the system has found suitable samples, it creates a three-digit code that is sent to the customer's registered cellphone number. This procedure is carried out with the help of a GSM modem connected to the ARM7 processor. The inputted OTP will be verified; if it is determined to be genuine, the customer's account will be unlocked; otherwise, the account will be banned. A thermistor and a tilt sensor will be included in the system to protect the ATM terminal from fire and theft. The trials were carried out in real time, with two people first being enrolled and then being authenticated.

S Singh's A Constraint-based Biometric Scheme for ATMs and Swiping Machines:

In today's scientific world, technologies are continually evolving, but along with their convenience and comfort, they also carry with them a significant security issue. Considering the physical security of the system in order to provide access control and authentication of users, we decided to implement a new Biometric coupled with ATM PIN system, as PINs are readily guessed, stolen, and misused. Biometrics is being combined with current technology to increase security and minimise ATM fraud, but it has raised numerous concerns, including sensor durability and time consumption. This article addresses two questions: “Is it really worth it to go through the full biometric procedure only to debit a little amount?” and “Is it really worth it to go through the entire biometric process to simply debit a small amount?” and “What is the greatest amount that may be lost if one's card is used fraudulently?” As a solution, we

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907151 |

suggest a biometric limitation on ATM transactions to increase system efficiency and address the identified problems. The suggestion is split into two sections. The first part addresses sensor performance issues by imposing a limit on the amount of cash that can be withdrawn, as well as a limit on the number of transactions that can be made. This means that if a large amount must be withdrawn, or if multiple transactions must be made by withdrawing small amounts repeatedly, biometrics must be presented. Biometric presentation is not required if all that is required is a balance inquiry or if the cash is low and the number of transactions in a day is fewer than the set number of tries. Apart from preserving security, it may assist customers save time and retain sensor performance by not providing their biometric for a few hundred dollars. The second section of this paper explains how fingerprint verification is carried out if the claimant is allowed access to the system, as well as what measures could be taken to improve the performance of the fingerprint biometric system that could be added to our proposed system to improve overall system performance.

WA Shier's Biometrics in Human-Machine Interaction:

In applications such as decision making, interview support systems, and human-robot interfacing, the function of biometrics in human-machine interactions is examined. There are now biometrics initiatives that use "talking face" technology. Future technologies, we predict, will authenticate individuals using biometrics, evaluate facial expressions, temperature, and blood pressure, as well as develop and analyse cognitive questions. This paper gives an overview of relevant research as well as a forecast for future generations of sophisticated biometric-based human-machine systems and their applications.

S. Jathumithran, V. Thamilarasan, A. Piratheepan, P. Rushanthini, J. Mercy veniancya, P. Nirupa, and K. Thiruthanigesan have developed a novel approach to improve the security of ATMs using biometrics.

In today's society, ATM machines are utilised by everyone to withdraw and transfer cash. This study focused on incorporating a fingerprint method into an ATM system. We chose this region to enhance savings and security for all clients, making transactions simple. Each person's fingerprint has its own unique set of characteristics. There's no need to be concerned about losing your ATM card, and you don't have to have it with you at all times. When comparing the various methods used for ATM security, it is discovered that fingerprint technology works better and is safer than the others. Which involves making transactions simple and safe while also maintaining a user-friendly experience for both the customer and the ATM machine. This is the most promising electronic money transaction technology.

S Bharadwaj's Biometric Quality: A Review of Fingerprint, Iris, and Face :

Variability in data affects the acquisition, handling, and use of biometric samples in biometric systems. It is critical to evaluate the data first and then incorporate this knowledge into the recognition system, making biometric quality evaluation a crucial element of biometrics. Though there are numerous interpretations and definitions of quality, some of which are contradictory, a comprehensive definition of quality remains elusive. This study offers an overview of several biometric quality ideas and interpretations in order to provide a clear picture of the current status and future developments. Several variables that produce various forms of biometric sample degradations are described, as well as picture characteristics that attribute to the impacts of these degradations. The performance of quality measures for diverse applications is evaluated using evaluation methods. A overview of the characteristics, strengths, and limitations of existing fingerprint, iris, and face biometric quality evaluation methodologies is also provided. Finally, a representative collection of quality measures from all three modalities is assessed on a multimodal database of 2D pictures to better understand their behaviour in comparison to match scores derived from state-of-the-art recognition algorithms. The examination of the characteristic function of quality and match scores reveals that a carefully chosen complement of quality measurements can benefit a variety of biometric quality applications.

G Kayim's Short-Term Face Recognition for Automated Teller Machine (ATM) Users:

This article discusses a unique biometric situation in which a person is verified at an ATM and then has to be re-identified from a camera in a very short amount of time, under very difficult lighting and posture conditions, and using data from a single session. The application scenario is the automated retraction of a forgotten card or cash at an ATM, which occurs often and causes discomfort to customers as well as financial losses for banks. We propose a multimodal authentication system that works within the constraints imposed by this application scenario, and we use face recognition and color-based body appearance recognition to create a system that improves ATM behaviour in the event of a forgotten card or cash by re-identifying the user using an embedded ATM camera. We concentrate on the scenario and platform, and we present results from field tests using the suggested system under difficult conditions.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907151 |

The design of the ATM terminal is based on fingerprint recognition:

Customer identification systems for typical ATM terminals rely solely on bank cards, passwords, and other identity verification techniques, which are imperfect and have limited functionalities. The author creates a new ATM terminal customer recognition system to address the flaws of traditional ones. The S3C2440 chip is utilised as the microprocessor's core in ARM9, and an upgraded enhancement algorithm for fingerprint images increases the security of customers using ATM machines.

Biometric Technology is a type of identification technology that uses some part of a person's biology to identify them. Individuals can be identified using biometric technology such as facial recognition systems without their knowledge. Fingerprinting is one of the first and most well-known biometric technology that has been lumped together under the umbrella of digital forensics. Biometrics is the study of people's unique physical and behavioural traits via measurement and statistical analysis. The technology is mostly used for identification and access control, as well as identifying those who are being watched.

Iris Recognition is a technique for recognising a person's iris.

Iris recognition is a biometric identification approach that employs mathematical pattern recognition algorithms on video pictures of one or both of an individual's irises, which include complex patterns that are unique, stable, and visible from a distance.

Face Recognition: Facial recognition is a technique for recognising or validating an individual's identification by looking at their face. Face recognition software can identify persons in pictures, videos, or in real time. During police stops, officers may use utilise mobile devices to identify persons. However, facial recognition data is prone to errors, which can lead to persons being accused of crimes they did not commit. Software for facial recognition is extremely poor.

III.EXISTING SYSTEM

Every person has a variety of bank accounts at a variety of banks; consumers must carry several ATM cards for transaction deals, and each account may have multiple PINs.

IV.PROBLEM STATEMENT

Every person has several bank accounts with various banks, requires multiple ATM cards for transactions, and may have separate PINs for each account. We forget our PINs, lose our cards, have our cards stolen, and have our PINs stolen. These scenarios occur in our everyday lives, and we must learn to deal with them.

V.PROPOSED SYSTEM

Designing a system that replaces traditional ATM transactions with biometric-based fingerprint identification and GSM-based authenticate transactions. The authentication procedure necessitates the use of a customer's fingerprint for identifying purposes. Every person has a distinct fingerprint. As a result, traditional ATM cards and PINs are being phased out in favour of human fingerprints. After successful authentication, it displays the customer's whole account list and grants permission to make transactions on those accounts. During the transaction process, control is passed to the GSM module, which performs an authentication transaction on behalf of the bank. With increased security, this technology addresses the disadvantages of the old traditional method.

The proposed system's goal is to give access to numerous accounts with a single touch, with high security transactions. It also includes features such as inter and intra bank transactions, and eliminates the need for several cards and PINs.

A fingerprint scanner is a form of technology that recognises and authenticates an individual's fingerprints in order to give or restrict access to a computer system or a physical location. Matrix keypads are the most popular input device in a wide range of applications, including digital circuits, telephone communications, calculators, and ATMs. A matrix keypad is made up of a series of push buttons or switches that are organised in rows and columns in a matrix pattern.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

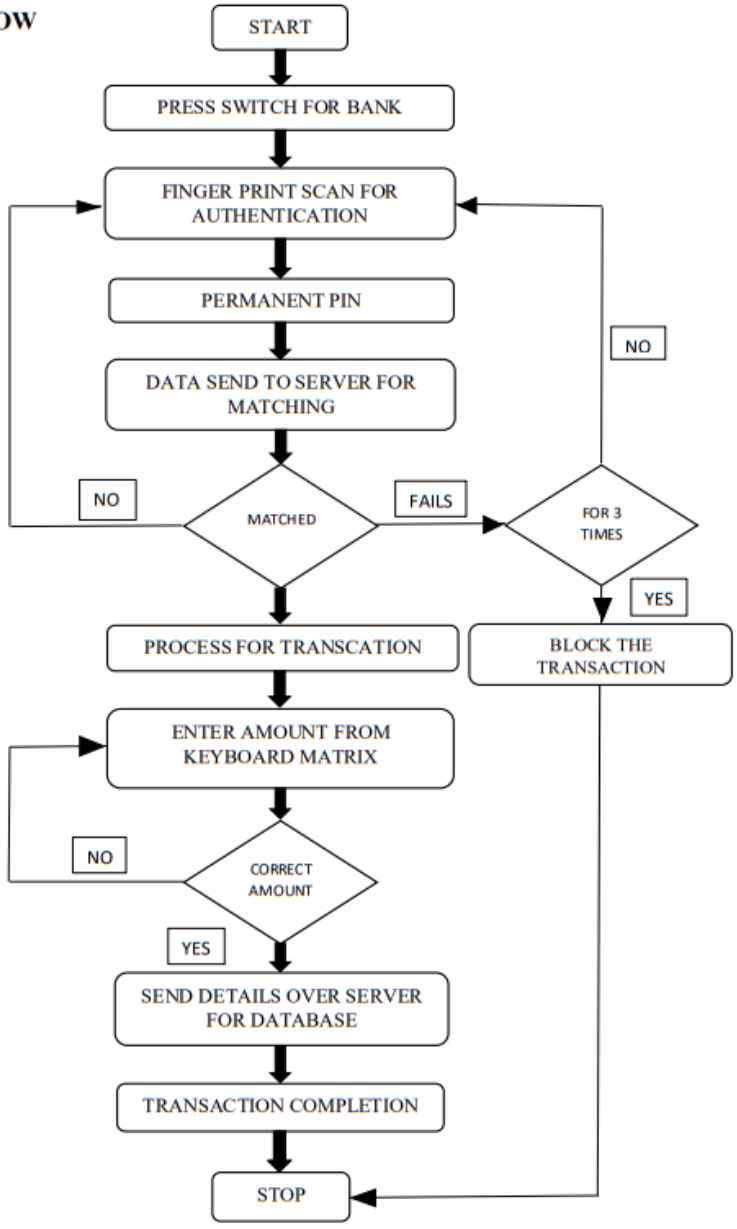
| DOI: 10.15680/IJIRCCE.2021.0907151 |

Transformers are most often employed in electric power applications to increase low AC voltages at high current (a step-up transformer) or decrease high AC voltages at low current (a step-down transformer), as well as to couple the stages of signal-processing circuits.

GSM mobile phone authentication:

In the GSM system, authentication is accomplished by the Base Station transmitting a challenge to the mobile station. The MS sends back a response that is then validated using a key stored on its SIM. The MS is the only one who is authenticated, not the user..

SYSTEM FLOW



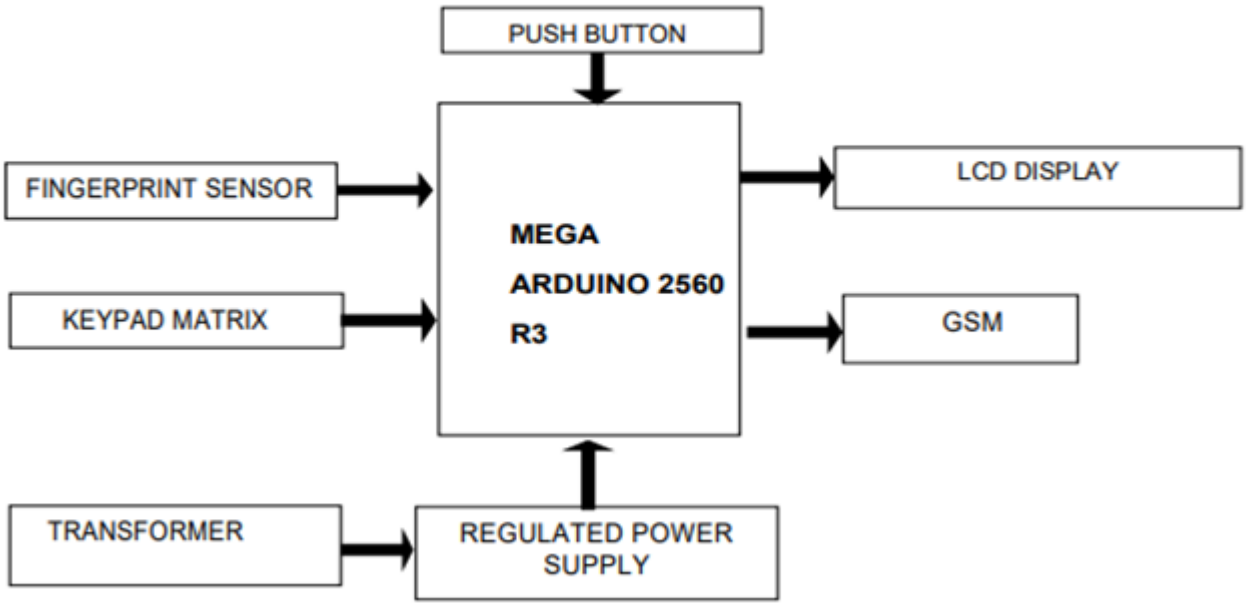
International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907151 |

BLOCK DIAGRAM FOR MULTIBANKING TRANSACTION



VI.WORKING PRINCIPLE

DESCRIPTION: The suggested system's design is shown in Figure 1. The system's operation begins with the user's input being read as a fingerprint. A fingerprint scanner will be used to read it. The data in the database will be used to verify the input, which will then be validated. The suggested system's design is separated into three main functioning modules: A) Fingerprint Module B) Web Services' Purpose C) The GSM module's operation.

HOW THE FINGERPRINT MODULE WORKS: The fingerprint scanner receives the data from the optical scanner sensor and compares it to the data stored in the cloud database. If authentication is successful, a UID is generated. The detail information from the bank database is retrieved using the UID. We may safely manage vital data on the cloud by using biometric fingerprints, which aids in the usage of cloud technology. The Minutiae Algorithm is used by many optical scanner equipment in author because it provides great precision. The optical 23 scanner was used to scan fingerprints. It mostly serves two purposes: Takes a picture of your fingerprint. Checks whether the new fingerprint picture's design matches the previously saved image. One of the most important aspects or main factors to consider is the quality of the fingerimage. The following factors have an impact on image quality: x Skin Conditions: - Dryness, wetness, dirtiness, cuts (temporary or permanent), bruises, and so on. x Sensor Settings: - Toxicity, Noise, Size, and User Cooperation After the fingerprint is confirmed, the system queries online services for the user's account information. For future transactions, the information of the user's bank accounts are presented. The table below contains extensive information on fingerprint scanners.

THE PURPOSE OF WEB SERVICES: Web services play an essential role in transporting data between the cloud and the bank database and delivering it to the computer that serves as a user interface.

Working of Biometric Fingerprints: The fingerprint scanner receives the data from the optical scanner sensor and compares it to the data stored in the cloud database. If authentication is successful, a UID is generated. The detail information from the bank database is retrieved using the UID. We may safely manage vital data on the cloud by using biometric fingerprints, according to author [8], which aids in the usage of cloud technology. The author uses an optical scanner to scan his fingerprints. It mostly serves two purposes:

Takes a fingerprint image and checks to see if the new fingerprint picture's design matches the previously saved image. The quality of the finger picture is one of the most important aspects or main factors to consider. x Skin Conditions: - Dryness, Wetness, Dirtiness, Temporary or Permanent Cuts, Bruises, and other factors that impact image quality x Sensor Settings: - Uncleanliness, Noise, Size, and User Collaboration After the fingerprint is confirmed, the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907151 |

system queries online services for the user's account information. For future transactions, the information of the user's bank accounts are presented.

Principles of Operation Fingerprint enrollment and fingerprint matching are the two elements of fingerprint processing (the matching can be 1:1 or 1:N). The user must input the finger twice while registering. The system will analyse the two-time finger pictures, create a finger template based on the processing findings, and save the template. When a user inserts a finger using an optical sensor, the system creates a finger template and compares it to templates in the finger library. For 1:1 matching, the system compares the live finger to a template specified in the Module; for 1:N matching, or searching, the system searches the whole finger library for the matched finger. In both cases, the matched result failure will be returned by the system.

GSM

The GSM system is the world's most extensively utilised cellular technology today. It has been a particularly successful cellular phone technology for a variety of reasons, including the ability to roam internationally with the assurance of being able to function on GSM networks in the same way - as long as payment arrangements are in place. GSM stood for Groupe Speciale Mobile at first, but when it became obvious that cellular technology was being used all over the world, the definition of GSM was altered to Global System for Mobile Communications. Since its introduction in 1991, GSM has gradually risen in popularity, and it is currently the most commonly used cell phone system on the planet. GSM passed the one billion subscriber threshold in February 2004, and is currently well over the three billion subscriber mark, with growth continuing to remain steady.

GSM BASICS: When the GSM cellular technology was first developed, it had a variety of design goals:

• It should have a cheap phone or terminal cost • Terminals should be able to be portable • It should enable international roaming • It should have excellent spectral efficiency • It should be ISDN compatible.

All of these were addressed by the GSM cellular technology that was created. GSM's overall system definition include both the air interface and network or infrastructure technology. It is possible to specify the functioning of the entire network in this way, allowing international roaming as well as network parts from various manufacturers to work together, however this last feature isn't always true, especially with older devices. RF channels with a frequency of 200 kHz are used in GSM cellular technology. Each carrier is time division multiplexed to allow up to eight people to access it. It's a TDMA/FDMA system in this sense. The base transceiver stations (BTS) are grouped together and managed by a base station controller (BSC), which is usually co-located with one of the BTSs. The base station subsystem refers to the BSC and its related BTSs (BSS). The primary switching area is located further into the core network. The mobile switching centre is what it's called (MSC). The home location registration (HLR) and the visitor location register (VLR), which track the position of mobile phones and allow calls to be directed to them, are linked to it. There's also the Authentication Centre (AuC) and the Equipment Identify Register (EIR), which are used to authenticate the phone before it's permitted on the network and for billing purposes. These are discussed in detail in the following pages. Last but not least, there's the phone. This is the thing that the end user sees, sometimes referred to as the ME or mobile equipment. The usage of a Subscriber Identity Module was one of the first features to be deployed on GSM. This card included the user's identification and other information, allowing the user to quickly update a phone while maintaining their network identity. It might also be used to hold additional data, such as a "phone book" or other objects. This item alone has made it incredibly easy for users to switch phones, which has fueled the phone manufacturing business and allowed new phones with extra capabilities to be released. This has helped mobile carriers to boost their average revenue per user (ARPU) by guaranteeing that consumers can take use of any new network capabilities that need more advanced phones.

GSM's future development: The GSM mobile telecommunications system was a huge success. It was originally designed for usage inside Europe, but within a short period of time, it had spread well beyond Europe's boundaries, becoming a globally acknowledged standard. It was extended beyond the basic speech capabilities to be able to transport data, in addition to its success as a voice communications system. GSM was created to give a packet data capability as the Internet became more extensively utilised. The GPRS system was the first important advancement.

OTP (One-Time Password)

The MFA application will also employ the OTP-based authentication method as one of the phases in the multi-factor authentication system. During the login step, the user is required to provide a 6-digit one-time passcode (OTP)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907151 |

that was sent to their phone number. This module may only be used during the login process. This module also gives the MFA application an API to verify whether or not the OTP authentication was successful. At a later point, this API will be used to provide access to the prototype application.

Notification by SMS

After a succession of authentications, the user receives an SMS notice. Every successful transaction is reported to the user. In the event of a fraudulent attempt to log into a legitimate user's account, the user will be notified via multiple messages.

VII.RESULTS

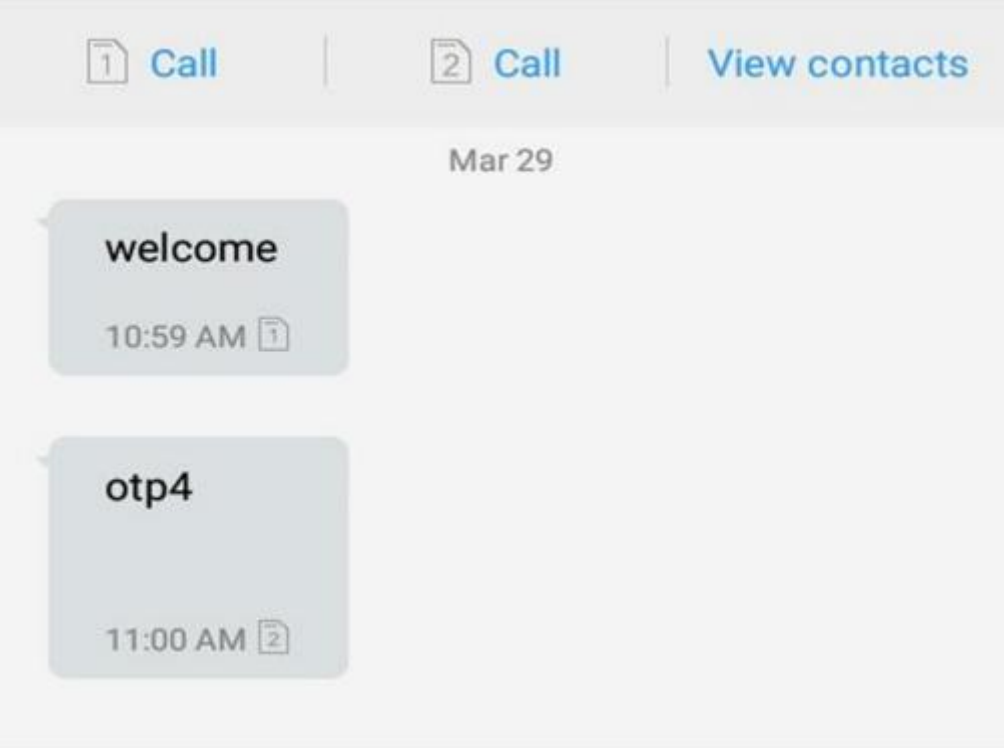
Only the account holder (not the nominee) has access to the account due to biometrics. Multiple authentications are time demanding at first, and such a system requires quick and efficient technology to administer. There is no need to carry numerous cards or remember their passwords because all bank accounts are controlled with a single finger touch. Problems such as fraud, unauthorised entry, and stolen cards with forgotten PINs are avoided. For validation, the system uses biometrics rather than a PIN. As a result, transactions become more secure. It pauses the fraud alerts linked to ATM card verification and other issues.

GSM OUTPUT

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907151 |



VIII.CONCLUSION

The planned one-touch Multi-banking Transaction ATM system will take the place of existing ATMs. It has benefits such as lowering card manufacturing costs and overcoming traditional system drawbacks such as carrying multiple cards, losing cards, losing PINs, remembering multiple PINs, fraud calls related to ATM cards, and so on. It also provides high security by utilising authentication methods such as fingerprint, face recognition, and OTP systems, making it simple to conduct multiple bank account transactions. The use of biometrics has improved the reliability and security of ATM transactions. The addition of the OTP and facial recognition concepts to the system improves security and eliminates the need to memorise passwords. Furthermore, the system is based on embedded technology, making it user-friendly and non-intrusive. In comparison to the previous method, the time it takes for each user to complete an ATM transaction is lowered.

IX.FUTURE WORK

Software changes are required. Changes might be made to improve the system's performance. All undertakings are constrained by time and resources, yet they are all possible if given limitless time and resources. The features that may be added to our system are as follows: - Performance in terms of speed and memory can be improved. This may be accomplished by utilising a different SMS gateway. There is a problem with the SMS gateway. Additional improvements can be made by concentrating on the speed with which communications are sent and received. An illegal individual visiting the ATM can be detected via a spoken voice alarm. It is necessary to provide a warning to anyone who is not permitted. A spoken voice alert in the security sector outside the ATM might be used as a warning.

REFERENCES

[1] Ranjit P. Khatmode and Ramchandra V. Kulkarni, "ARM7 Based Smart ATM Access and Security System Using Fingerprint Recognition and GSM Technology," International Journal of Emerging Technology and Advanced Engineering, Vol. 4, Issue 2, February 2014.

[2] G.Udaya Shree and M. Vinusha, "Real-Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Terminals," International Journal of Scientific Engineering and Technology Research, Vol. 2 Issue 12, Sep.2013.

[3] Ritu Jindal and Gagandeep Kaur, "Biometric Identification System Based on Iris, Palm, and Fingerprint for 4. Security Enhancements," International Journal of Engineering Research and Technology, Vol. 1, No. 4, June 2012.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907151 |

[4] Deepa Malviya, "Enhanced Safety Approach for ATM Using Face Recognition Technique," International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014.

[5] Matsoso Samuel Monaheng and Padmaja Kuruba, "Iris Recognition Using Circular Hough Transform," International Journal of 413 Innovative Research in Science, Engineering, and Technology, Volume 2, Issue 8, August 2013.

[6] Fakir Sharif Hossian, Ali Nawaz, and Khan Md. Grihan, "Biometric Authentication Scheme for ATM Banking System Using AES Processor," International Journal of Information and Computer Science Volume 2 Issue 4 (May 2013).

[7] Mohsin Karovaliya, Saifali Karedia, Sharad Oza, and Dr.D.R. Kalbande, "Enhanced Security for ATM Machines with OTP and Facial Recognition Features," International Conference on Advanced Computing Technologies and Applications (I CATA-2015).

[8] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, and S. McBride, "A system for automatic iris recognition," Sarasota, FL, IEEE Workshop on Applications of Computer Vision, pp. 121- 128, 2011.

[9] Ravi.J. et al., "Fingerprint Recognition Using Minutiae Score Matching," International Journal of Engineering Science and Technology, Vol. 1(2), 35-42, 2009.

[10] 978-1-4673-9098-9/15/$31.00 JinXin Xu, "An Online Biometric Identification System Based on Two Dimensional Fisher Linear Discriminant," ©2015IEEE

[11]Abdul Razaque, Fathi H. Amsaad, Chaitanya Kumar Nerella, Musbah Abdulgader, Harsha Saranu, "MultiBiometric System Using Fuzzy Vault," 978-1-4673-9985-2/16/$31.00, 978-1-4673-9985-2/16/$31.00, 978-1-4673-9985-2/16/$31.00, 978-1-4673-9985-2/16/$31 IEEE, 2016. 39

[12] H. Lasisi and A. Ajisafe, "Development of Stripe Biometric-Based Fingerprint Authentication Systems in Automated Teller Machines," IEEE, ISBN 978-1-4673-2488-5, pp. 1 72-l75, 2012.

[13] K. K. Nair, Albert Helberg, Johannes van der Merwe, K. K. Nair, Albert Helberg, Johannes van der Merwe, K. K. Nair, Albert ISBN:978-1-4673-9609-7, "An Approach to Improving the Match-on-Card Fingerprint Authentication System Security." IEEE, 2016.

[14] Yun Yang, JiaMi, "ATM terminal design is based on fingerprint recognition," 978-1-4244-6349 7/10/$26.00 201 0 IEEE, 978-1-4244-6349 7/10/$26.00 201 0 IEEE, 978-1-4244-6349 7/10/$26.00 201 0 IEEE.

[15] Albert Ali Salah*, Ekberjan Derman#1, Y. Koray Gecici#2, 2013IEEE. "SHORT TERM FACE RECOGNITION FOR AUTOMATIC TELLER MACHINE (ATM) USERS," 978-1-4799-3343-3/13/$31.00 2013IEEE,

16. R.M. Bolle, K. Ratha, S. Chikkerur, J.H. Connell, and K. Ratha. IEEE Transaction on Pattern Analysis and Machine Intelligence, Bolle, "Generating Cancelable Fingerprint Templates." vol. 29, no. 4, 2007.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details