RESEARCH ARTICLE OPEN ACCESS

Enhancing Security of Automated Teller Machine Transaction using Biometric System with EMV Technology

Hema Blessy J[1], Thulasimani K[2]

[1] (P. *G. Student, Department of Computer Science and Engineering, Government College of Engineering, Tirunelveli*)
[2] (*Professor, Department of Computer Science and Engineering, Government College of Engineering, Tirunelveli*)

----------**********----------

Abstract:

Now-a-days Automated Teller Machine (ATM) system, most often only Personal Identification Number is used to verify authentic user which is not protected enough because it is very easy to copy. ATMs are a convenient way to meet user's banking needs. However, the use of debit card or other types of cards during ATM transactions has some problems like prone to ATM skimming, magnetic strips of card getting damaged, manufacturing and transportation cost of cards, longer time to authenticate users etc. The objective of this work is to provide a more secure transaction using Biometric features, Secure Hash Algorithm, and verification techniques. Therefore, a Biometric system can be a stable solution for this problem. This system refers to a cyber security process that verifies a user's identity using their unique biological characteristics, such as fingerprints, voice, and facial features. It stores the information to verify a user's identity when that user accesses their transaction. Europay, MasterCard, and Visa (EMV) technology refers to a global standard for secure payment card transactions, primarily using smart cards with embedded microchips. When applied to a biometric system, EMV technology integrates biometric authentication methods, such as fingerprint or facial recognition, to enhance the security of card-based transactions by ensuring that the person using the card is the authorized cardholder through their biometric data. This combination adds an extra layer of security to payment processes. Secure Hash Algorithm used to generate unique transaction authentication codes and protect against data tampering. So this proposed method will provide more security to users.

Keywords — **Automated Teller Machine, Biometric, Europay MasterCard and Visa, Magnetic Strips, Personal Identification Number, Secure Hash Algorithm**

----------**********----------

1. INTRODUCTION

Automated Teller Machine (ATM) plays a vital role for providing easy access to people for making transaction in banking activities. Automated Teller Machine was invented in 20th century by United Kingdom. The purpose of the system is to provide a convenient and automated way for the users to access their accounts at any time and also helps to reduce the manual transaction time and waiting time of transaction operation [1].

The current ATM model uses Europay, MasterCard, and Visa chip card, it makes more challenging for criminals to clone cards because the chip generates unique code for each transaction. The dynamic authentication process makes it difficult to create counterfeit cards [2]. Criminals

can still attempt to steal card data from magnetic stripe or chip to develop counterfeit cards. There is a more common in regions with mixed EMV and magnetic stripe card usage.

These issues can be overcome by the proposed system. Using Smart Debit card with Biometric features provide more secure transaction to users. The Secure Hash Algorithm can be used to secure data during transaction [3]. Biometric features are used to check out, the transaction holder fingerprint pattern from the bank database. Whether the user fingerprint matches with their bank database pattern, allow transaction otherwise decline it.

2. LITERATURE REVIEW

2.1. Biometric Features

Physical Biometric features are used to recognize and identify individuals. Commonly it plays a vital role in security systems, access control, and identity verification.

2.1.1. Fingerprint Recognition

Fingerprint biometrics relies on the minutia features present in an individual's fingerprints for identification and authentication. These features encompass ridge patterns, such as loops, whorls, and arches, forming the foundation of a fingerprint's distinctiveness. Ridge count, ridge shape variations, ridge path irregularities, and ridge crossovers all contribute to the complexity and individuality of fingerprints. Additionally, sweat pores and specific ridge characteristics like their thickness, width, and shape further enhance the uniqueness of each finger print [4]. The core and delta, situated at the centre and within the triangular region of a fingerprint pattern, respectively, assist in its classification and analysis. Minutiae points, which include ridge endings, bifurcations, and islands, serve as precise landmarks for matching fingerprints. These fingerprint biometric features collectively make fingerprint recognition systems highly reliable and widely used for security and identification purposes, encompassing everything from criminal investigations to secure access control on smart phones and other devices. Fingerprint minutia types are, Ridge ending, Bifurcation, Dot, Bridge and Crossover.

2.1.2. Iris Recognition

Iris recognition is a biometric technology that utilizes the characteristics of an individual's iris, the colored part of the eye, to confirm their identity with exceptional accuracy. Iris process involves capturing a detailed image of the iris using specialized cameras equipped with infrared or near-infrared light. The complex patterns present in the iris, including radial lines, crypts, and freckle-like spots, are extracted and converted into a digital model. This model is securely stored and serves as a reliable reference point for authentication. When authentication is required, a live iris scan is compared to the stored model, and if they match correctly, identity is verified [5]. Iris recognition is known for its remarkable accuracy, stability over time, and resistance to fraud, making it a preferred choice for applications demanding stringent security, such as border control, financial transactions, and secure facility access.

The advantage of iris recognition is its non-invasive and user-friendly nature. Individuals simply need to look into a camera for a brief moment, making it a convenient and comfortable biometric method. Additionally, its high level of accuracy ensures low false acceptance and false rejection rates, enhancing both security and user convenience. As a result, iris recognition has found applications not only in high-security environments but also in everyday scenarios like unlocking smart phones, demonstrating its versatility and reliability as a biometric technology.

2.1.3. Facial Recognition

A facial recognition system is a biometric technology designed to identify and authenticate individuals by analysing their unique facial features. It operates by capturing an individual's facial image through cameras or sensors, extracting distinct attributes like the arrangement of eyes, nose, mouth, and facial contours, and converting this information into a digital template or mathematical representation. This template is

securely stored and can be used for subsequent comparisons during authentication. When the system encounters an authentication request, it compares the live facial image to the stored template, and if there is a sufficient match, access is granted or the individual's identity is verified [6]. Facial recognition systems have found widespread application in diverse fields, including security, law enforcement, access control, and consumer electronics, due to their non-invasive and user-friendly nature.

The feature of facial recognition system is their real-time capability, allowing for swift and seamless identification. This technology can quickly process and match facial images in various scenarios, from unlocking smart phones and providing secure access to buildings to enhancing surveillance and airport security. However, it also raises concerns related to privacy, data security, and potential misuse, which has led to debates about ethical usage and the need for robust regulatory frameworks to protect individuals' rights and data. Despite these challenges, facial recognition systems continue to evolve, offering a powerful tool for identity verification in an increasingly digital and security-conscious world.

2.1.4. Palm Print Recognition

Palm print recognition is a biometric system that leverages the unique patterns present on an individual's palm for identification and authentication. The palm of the hand contains distinct ridges, wrinkles, and lines that are highly characteristic and stable over time. These features are captured using imaging techniques such as infrared or visible light scans, and the resulting palm print data is processed to create a template for matching and verification. The palm's surface area allows for a wide range of data points, enhancing the system's accuracy and reliability [7]. Palm print recognition is less intrusive than some other biometric methods and can be employed in various applications, from secure access control to financial transactions.

The advantage of palm print recognition is its versatility and resistance to environmental factors. Unlike some other biometrics, palm prints are less affected by changes in lighting conditions or minor injuries to the hand. This robustness makes palm print recognition suitable for outdoor and indoor environments alike. As technology continues to advance, palm print recognition is increasingly integrated into security systems and devices, contributing to enhanced security and user convenience. However, as with any biometric system, privacy and data protection considerations are essential in its deployment.

2.1.5. Hand Geometry Recognition

Hand geometry recognition is a biometric system that focuses on identifying individuals based on the physical characteristics of their hand. This technology primarily analyses the size and shape of the hand, along with the length and width of the fingers and the spaces between them. Users typically place their hand on a scanner or sensor, and the system captures these dimensions to create a unique template for comparison and verification. Hand geometry recognition is known for its ease of use and non-intrusiveness, as it requires minimal cooperation from individuals, making it suitable for applications such as time and attendance tracking and access control.

The advantage of hand geometry recognition is its user-friendliness and speed. It offers a quick and straightforward means of authentication, where users simply place their hand on a sensor for rapid identification. Hand geometry features tend to be relatively stable over time, although they can be influenced by injuries or surgeries [8]. While it may not offer the same level of uniqueness as some other biometric methods like fingerprints or iris scans, hand geometry recognition strikes a balance between convenience and security, making it a practical choice for various applications where swift and non-intrusive verification is required.

2.1.6. Gait Recognition

Gait recognition is a biometric technology that identifies individuals based on the unique way they walk or move. It focuses on the distinctive features of a person's walking pattern, including their stride length, step duration, walking speed, and the angle

of their limbs during each step. These features are collected through various sensors or cameras that capture an individual's gait as they walk. Gait recognition systems then analyse this data to create a unique gait profile or template, which can be used for identification and authentication. Gait recognition is particularly valuable in scenarios where other biometric methods, such as facial recognition or fingerprint scanning, may not be suitable due to distance or low visibility.

Additionally, gait recognition can be combined with other biometric methods to enhance overall security and accuracy [9]. However, it's essential to consider that gait can be affected by factors like footwear, clothing, and temporary injuries, which may introduce variability into the recognition process. Despite these challenges, gait recognition continues to be an area of research and development for its potential applications in diverse fields, including security and healthcare.

2.2. Secure Hash Algorithm

A Secure Hash Algorithm is a cryptographic technique used to transform input data, such as messages, files, or passwords, into a fixed-length hash value. This hash value, often represented as a hexadecimal string, is a unique digital fingerprint of the input data. The key purpose of SHA is to ensure data integrity and security. The SHA process begins with the input data, which is typically padded to fit into fixed-size blocks. These blocks undergo a series of mathematical operations, including bitwise operations, modular arithmetic, and logical functions. These operations are performed in multiple rounds, and the result of each round is combined with the previous hash value, gradually transforming the data [10]. Once all blocks are processed, the final hash value is obtained. Even a minor change in the input data results in a significantly different hash value, making SHA useful for verifying data integrity during transmission or storage, as well as for securely storing passwords and creating digital signatures.

SHA algorithms come in various versions, such as SHA-1, SHA-256, and SHA-512, with differing levels of security and efficiency. SHA is widely used in file and software verification, network security, and biometric data protection, and cryptography, data duplication in storage systems, document integrity assurance, secure communications, and certificate authorities.

2.3. EMV Card Technology

EMV stands for Europay, MasterCard, and Visa, and it refers to a global standard for credit and debit card processing based on chip card technology [11]. EMV technology is designed to enhance the security of card-present transactions and reduce card fraud. EMV cards are equipped with a small microprocessor chip. Unlike traditional magnetic stripe cards, which store static data, EMV cards generate dynamic data for each transaction, making them more secure. EMV payment transaction security has three functionalities, Card authentication, Cardholder verification method and Transaction authorization. Card authentication involves the use of microprocessor chips embedded in payment cards, often referred to as "chip cards" or "smart cards." EMV cards generate a unique transaction code for each purchase, making it significantly more secure than traditional magnetic stripe cards. This dynamic authentication process helps protect against card counterfeiting and fraud, as the transaction data cannot be easily replicated for unauthorized use.

Cardholder verification method supports multiple methods for verifying the cardholder's identity. Chip and PIN: The cardholder enters a Personal Identification Number to authenticate the transaction. Chip and Signature: The cardholder signs a receipt to verify their identity. This method is still more secure than traditional magnetic stripe signatures [12]. Transaction Authorization: The terminal sends the transaction data, including the dynamic transaction data and cardholder verification method results, to the card issuer for authorization. The issuer evaluates the data and decides whether to approve or decline the transaction.

3. METHODOLOGY

3.1. Block Diagram

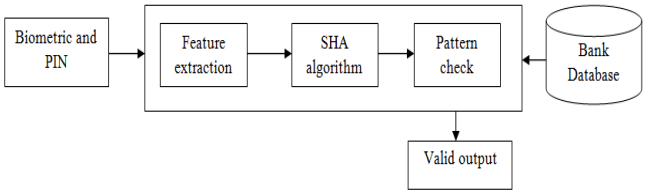

Fig1. Biometric System

First step involves user gives their Personal Identification Number (PIN) and fingerprint in an ATM transaction. User has to place their finger on the scanner which has a sensor. Optical and Solid state sensors are mainly used to capture a person's Finger impression. Optical fingerprint sensors capture fingerprint images using visible light. When user places their finger on the sensor's surface, the ridges and valleys of the fingerprint reflect or absorb light differently and creating a pattern. Each person's Fingerprint have a minutia features. Solid-state fingerprint sensors use various technologies to capture fingerprint data without relying on visual images. It generally offer higher accuracy and better resistance to spoofing, making them suitable for applications where security is a top priority [13]. The purpose of the feature extractor is to characterize the object to be detected by measurements. Secure Hash Algorithm (SHA) used to enhance security and data integrity. Bank databases contain a wide range of information about the bank's customers, fingerprint images, minutiae points, timestamps, accounts, loans, credit, and investments. Fingerprint Matching is done using Euclidean distance.

3.2. Feature Extraction

A fingerprint biometric system is a secure and identification technology that uses the patterns and features of an individual's fingerprint to verify their identity. The secure transaction fingerprint features are,

i) Ridge Endings
ii) Bifurcations
iii) Bridge
iv) Crossover
v) Enclosures

i) Ridge Endings

Ridge endings are a critical minutiae feature in secure transactions involving fingerprint biometrics. These points represent the terminations of ridges within a fingerprint pattern and are pivotal for accurate authentication. In a secure transaction, the presence and arrangement of ridge endings are meticulously analysed to ensure the identity of the individual attempting the transaction [14]. Ridge endings provide unique and distinguishing characteristics, and their precise positioning is essential for accurate matching against stored templates. During the verification process, the system evaluates the presence, location, and orientation of these ridge endings to ascertain the legitimacy of the fingerprint being presented. Any disparities or inconsistencies in the ridge endings can raise red flags and trigger additional security measures, making ridge endings a crucial component in the overall security of secure transactions reliant on fingerprint biometrics.

ii) Bifurcations

Bifurcations as a minutiae feature in secure transactions utilizing fingerprint biometrics play a pivotal role in verifying and securing sensitive transactions. These points represent locations where a single ridge splits into two branches, forming a distinct Y-shaped pattern. In a secure transaction context, bifurcations are of paramount importance because they offer unique and intricate details that contribute to the fingerprint's distinctiveness. The presence and precise arrangement of bifurcations are scrutinized during authentication to establish the authenticity of the individual involved [15]. These features are vital for matching the presented fingerprint against a stored reference template. The system assesses the consistency and alignment of bifurcations, ensuring that they are in agreement with the authorized user's fingerprint. Any anomalies or discrepancies in bifurcation patterns can trigger further security measures, making bifurcations a fundamental element in enhancing the security and reliability of secure transactions reliant on fingerprint biometrics.

iii) Bridge

A bridge refers to a specific point within a fingerprint pattern where a ridge connects or forms a bridge-like structure between two other ridges. These minutiae features, which also include ridge endings and bifurcations, serve as unique characteristics that distinguish one individual's fingerprint from another. During secure transactions, such as financial transactions or access control, the captured fingerprint is analysed for these minutiae features, including bridges [16]. By comparing the observed minutiae features to a pre-registered template, the system can verify the identity of the individual initiating the transaction. This biometric authentication method offers a high level of security, helping to prevent unauthorized access and fraud, as the uniqueness of an individual's fingerprint, and its minutiae features, ensures a robust and reliable means of identity verification.

iv)Crossover

A crossover minutia feature refers to a specific point within a person's fingerprint where two ridge lines intersect or cross over each other. This unique fingerprint characteristic is vital for verifying an individual's identity during secure transactions. When someone initiates a secure transaction, their fingerprint is scanned and analyzed by a biometric system, which identifies and extracts minutiae features, including crossovers [17]. These crossovers are like distinct markers that help confirm the person's identity. By comparing these observed crossovers to a pre-registered template securely stored in the system, the biometric system can authenticate the user. This process adds an extra layer of security, ensuring that only authorized individuals can access secure systems or complete transactions, effectively reducing the risk of unauthorized access or fraudulent activities.

v) Enclosures

Enclosures a less common but still significant minutiae feature in secure transactions employing fingerprint biometrics, are distinct points where a single ridge divides into three branches, creating a characteristic triangular or enclosure pattern. These features, although less prevalent than ridge endings and bifurcations, contribute to the uniqueness of a fingerprint. In secure transactions, enclosures are carefully examined to bolster the security of the authentication process. The presence and precise arrangement of enclosures are analysed to verify the identity of the individual involved [13]. Enclosures provide an additional layer of authentication and can be used to increase the confidence in the fingerprint's authenticity. Any discrepancies or irregularities in enclosure patterns can trigger further security measures, enhancing the overall reliability and robustness of secure transactions relying on fingerprint biometrics. Although not as common as other minutiae types, enclosures add an extra dimension of scrutiny to ensure the accuracy and integrity of the authentication process in secure transactions.

3.3. Secure Hash Algorithm

Secure Hash Algorithm can play several important roles within biometric systems to enhance security and data integrity. SHAs work by taking a variable-length input and producing a fixed-length output, called a hash value [10]. The hash value is a unique identifier for the input data, and it is very difficult to find two different inputs that produce the same hash value. SHA-256 algorithm could be used in a biometric system.

- The user's fingerprint is captured using a fingerprint scanner.
- The fingerprint image is preprocessed to improve its quality and consistency. This may involve steps such as noise reduction and feature extraction.
- The preprocessed fingerprint image is hashed using the SHA-256 algorithm. This produces a 256-bit hash value.
- The hash value is stored in a database as the user's biometric template.
- When the user attempts to authenticate, their fingerprint is captured and preprocessed again.
- The preprocessed fingerprint image is hashed using the SHA-256 algorithm. The resulting hash value is then compared to the user's biometric template stored in the database.

- If the two hash values match, the user is authenticated. Otherwise, the authentication attempt fails.

3.4. Bank Database

Bank databases contain a wide range of information about the bank's customers, fingerprint images, minutiae points, timestamps, accounts, loans, credit, and investments. Bank databases are highly secure and are protected by a variety of security measures, such as encryption, firewalls, and intrusion detection systems.

- ***Customer information:*** This includes the customer's name, address, date of birth, phone number, email address, and Social Security number.
- ***Fingerprint Image:*** The fingerprint image itself, in a digital format.
- ***Minutiae points:*** The coordinates of the minutiae points in the fingerprint image. Minutiae points are unique features in a fingerprint, such as ridge endings and bifurcations.
- ***Timestamps:*** Timestamps or dates may be recorded to track when the fingerprint data was added or updated in the database.
- ***Account information:*** This includes the customer's account number, account type, account balance, and transaction history.
- ***Loan information:*** This includes the customer's loan amount, interest rate, repayment terms, and payment history.
- ***Credit information:*** This includes the customer's credit score, credit history, and outstanding debt.
- ***Investment information:*** This includes the customer's investment portfolio, investment goals, and risk tolerance.

3.5. Pattern Check Algorithm

Matching algorithms calculate the similarity between templates, typically using distance metrics like Euclidean distance or Hamming distance [18].

Step 1: Representation of Minutiae Points

Start with two fingerprint templates: one for the query fingerprint (authenticated) and another for the reference fingerprint (a stored template of the authorized user). Each template contains a set of minutiae points, which are unique features in the fingerprint, characterized by their (x, y) coordinates, minutiae type, and other relevant information.

Step 2: Matching Minutiae Points

Match corresponding minutiae points between the query and reference templates. This pairing is based on their type (ridge ending or bifurcation) and proximity [14,15]. Each minutiae point in the query fingerprint is paired with the closest matching minutiae point in the reference fingerprint.

Step 3: Calculating Euclidean Distance for Each Pair

The algorithm calculates the Euclidean distance for each pair of corresponding minutiae points. The Euclidean distance formula is applied to determine the spatial separation between these points

$$Euclidean\ Distance = sqrt((x1 - x2)^2 + (y1 - y2)^2) \quad (1)$$

Where (x1, y1) and (x2, y2) are the coordinates of the minutiae points being compared.

Step 4: Summing Distances

The calculated Euclidean distances for all corresponding minutiae point pairs are summed to obtain a single numerical value representing the overall difference or similarity between the two fingerprint templates.

Step 5: Threshold Comparison

Compare the total sum of distances to a predefined threshold value, which is set based on the desired security level of the system. If the total distance is less than or equal to the threshold, proceed to the next step. If the total distance exceeds the threshold, reject the query fingerprint, as it is considered not to match the reference fingerprint.

Step 6: Decision

Based on the threshold comparison, if the total distance is below the threshold, the fingerprints are considered a match, and the authentication or transaction is approved. If the total distance

exceeds the threshold, the fingerprints are considered not to match, and access is denied.

4. PROPOSED SYSTEM

Current ATM Transaction doesn't have a biometric based system. So criminals are easy to steal card data from magnetic stripe or chip to develop counterfeit cards. It is one of the most common problems in mixed EMV and magnetic stripe card usage. These issues are overcome by the proposed system. Using EMV chip card with Biometric features provide more secure transaction to users.

4.1. Working Principle

Initially each user gives their personal information and fingerprint impressions at bank database. After verification by bank, each user will get the EMV based Smart Debit card it is also called as EMV chip card. It contains details of the user's information and their biometric impressions. When user insert the EMV chip card, the reader reads data from card and display the verification message on LCD screen. Then user scans their fingerprint impression on the biometric system [3]. Biometric features are used to check out, the transaction holder fingerprint pattern from the bank database. Whether the user pattern matches with their bank database pattern, allow transaction otherwise decline it.

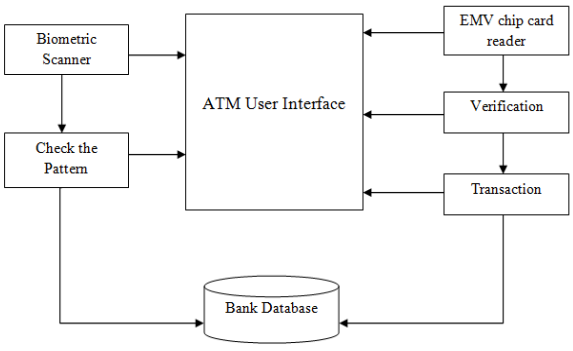

Fig2. Architecture diagram for ATM transaction

4.2. Algorithm

Input: Card Insertion or Contactless Tap with Fingerprint Scan

The input phase begins when a cardholder inserts their EMV chip card into a card reader or taps their contactless EMV card on a compatible device. Simultaneously, the fingerprint system scans the cardholder's fingerprint for authentication.

Process: Data Capture and Verification

The system captures transaction data from the card's chip, including the card number and transaction amount. It also verifies the scanned fingerprint against a stored template. Both the card data and fingerprint must match for verification.

Output: Transaction Approval or Decline

The combined data, along with the fingerprint verification result, is sent for authorization. If both the card data and fingerprint match, the transaction is approved. In case of any mismatch, the transaction is declined, ensuring secure and accurate payment authorization.

5. CONCLUSION

ATM is a convenient way to meet the banking needs of the users. ATM machines are deployed worldwide and used by a very large population of the world. The use of debit card or other types of cards during ATM transactions has some problems like prone to ATM skimming, magnetic strips of card getting damaged, manufacturing and transportation cost of cards, longer time to authenticate users etc. The proposed system uses biometric technique for fingerprint scanning using Secure Hash Algorithm. EMV technology is an advanced transaction method that combines the security of EMV chip cards with biometric authentication [11]. It requires the cardholder to verify their identity by scanning their fingerprint before authorizing a transaction and reducing the risk of unauthorized card use. So the proposed system will provide more security by identifying and reducing the forgery.

The future work, the plan is to focus on the security aspects of the User authentication safety app to be installed on the smart phone.

REFERENCES

[1] Divyans Mahansaria and Uttam kumar roy, " Secureauthentication for ATM transactions using NFC technology" , International Carnahan Conference on security Technology.

[2] Shubhra Jain, "ATM frauds-detection & prevention", International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835.

[3] Sweta Singh, Akhilesh Singh and Rakesh Kumar, "A constraint-based biometric scheme on ATM and swiping machine", 2016 International Conference on Computational Techniquies in Information and Communication Technologies (ICCTICT).

[4] Abdullah Saud1 , Nazar Elfadil, "Biometric Authentication by Using Fingerprint Recognition System", International Journal of Scientific Engineering and Science, Volume 4, Issue 5.

[5] K. Laxmi Narshima Rao, Vikram.Kulkarni, C.Krishna Reddy, "Recognition Technique for ATM based on IRIS Technology", International Journal of Engineering Research and Development, volume 3, Issue 11(September 2012).

[6] Omoyiola, Bayo Olushola, "Overview of Biometric and Facial Recognition Techniques", IOSR Journal of Computer Engineering, Volume 20, Issue 4.

[7] Kanchana .A, Stanly Jayaprakash .J, " Introduction To Palmprint Recognition", International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 11 | Nov -2017.

[8] Odgerel Ayurzana, Bumduuren Pumbuurei, Hiesik Kim, "A Study of Hand-Geometry Recognition System", IEEE.

[9] Nishtha Gupta, "Biometric System using Gait Feature Analysis and Comparison", International Journal of Engineering Research & Technology (IJERT), Vol. 6 Issue 05, May – 2017.

[10] Iti Malviya, Prof. Tejasvini Chetty, " Performance and Limitation Review of Secure Hash Function Algorithm", International Journal on Recent and Innovation Trends in Computing and Communication , Volume: 7 Issue: 6.

[11] Ahmed O. Ibrahim , Yaseen Hikmat Ismael, " EMV Electronic Payment System and its Attacks: A Review", Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM), Vol. 16, No. 1, 2022 (23-29).

[12] Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, Ross Anderson, "Chip and Skim: cloning EMV cards with the pre-play attack", IEEE Symposium on Security and Privacy.

[13] Wencheng Yang , Song Wang , Jiankun Hu , Guanglou Zheng and Craig Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review" , Symmetry.

[14] Roli Bansal , Priti Sehgal and Punam Bedi, "Minutiae Extraction from Fingerprint Images - a Review", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.

[15] Neeraj Bhargava, Ritu Bhargava, Manish Mathuria, Minaxi Cotia, "Fingerprint Matching using Ridge-End and Bifurcation Points", International Conference in Recent Trends in Information Technology and Computer Science.

[16] Ziad Alqadi , Mohammad Abuzalata , Yousf Eltous , Ghazi M. Qaryouti, " Analysis of Fingerprint Minutiae to Form Fingerprint Identifier", International Journal On Informatics Visualization, VOL 4 (2020) NO 1.

[17] Harminder Kaur, Poonam Dabas, "Minutiae Based Fingerprint Recognition", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 6, June – 2014.

[18] K. Martin Sagayam, D. Narain Ponraj, Jenkin Winston, Yaspy J C, Esther Jeba D, Antony Clara, "Authentication of Biometric System using Fingerprint Recognition with Euclidean Distance and Neural Network Classifier", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-4, February 2019.