International Journal of Industrial Engineering
2023;7(2):50-56.
ISSN: 2456-8449

Biometric Fingerprint ATM System to Enhance Security Using Minutiae-Based Algorithm

C Malarvizhi[1*], P. Dass[2], P. Karthikeyani[3], Sasikar A[4]

[1]Department of Electronics and Communication Engineering, Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India.
[2]Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, Tamil Nadu, India.
[3]Department of Computer Science, Thanthai Hans Roever College (Autonomous), Perambalur, Tamil Nadu, India.
[4]Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India.

[*]Corresponding author: malarvizhi.c@ritchennai.edu.in

Abstract. One alternative to using a password for authentication is to use biometric information. Fingerprint-based identification is among the most created and reliable biometric techniques. There are several benefits associated with selecting Biometric Fingerprint automated teller machines (ATM) System for minutiae -based security, the main ones being increased authentication precision, strengthened security protocols, and a dependable and easy-to-use user interface. The main objective of an ATM system that uses biometric fingerprints and a minutiae-based algorithm is to improve security and provide users of ATMs with a reliable way to authenticate themselves. A high-resolution fingerprint scanner is used to capture fingerprint images now of the transactions at the ATM. When it comes to protecting bank clients from harm, security measures may be important. When discussing vulnerabilities and causes in a court of law, these precautions are crucial. To provide their consumer with a risk-free banking experience, banks should adhere to certain criteria. This paper examines ATMs, the primary target of thieves, because of the easy access to the cash they provide, as well as the vulnerabilities and rising tide of illegal activity at ATMs. Banking security may be improved using biometric measures for both customers and employees. While the real card user is unable to make purchases, it also offers a fingerprint identification mechanism for nominees to use in their stead. The result shows 90% accuracy and 94% security assurance.

Keywords: Security, Automatic Teller Machine, Biometric Fingerprint, Verification, E-Banking, Crime and Minutiae Based Algorithm

INTRODUCTION

These days, almost everyone makes use of ATM networks to make and receive financial transactions. The ATM System was used as the testing ground for this fingerprint approach. This line of work to help consumers feel more at ease during financial dealings by increasing their sense of security is gone. Everyone has their own set of fingerprints. There's no need to always have an ATM card on you, and no risk of losing it. When compared to other methods of ATM protection, fingerprint scanning is both more effective and safer. Because of these factors, this mechanism is a safe and convenient method to do business, and it helps to keep the relationship between customers and ATMs harmonious. This is the cutting edge in the field of electronic money transfers [1]. As the number of digital transactions rises, so does the need for reliable and quick user authentication. Biometric authentication has many uses in automated teller machines. Biometric authentication makes use of unique identifiers such as fingerprints and face mapping. The present technique of authenticating users at ATMs has the issue of requiring password-personal identifying number (PIN) combinations. Since PINs may be easily monitored and exploited. The system's goal is to make ATMs safer and put a stop to these kinds of illicit operations. Here, One Time Password (OTPs) generated at random and sent over the Internet of Things (IoT) take the role of PINs [2].

The project's ultimate objective is a world without cash machines and ATM cards. After the client has been authenticated using biometrics and an OTP pin, the transaction will proceed. After three unsuccessful login attempts, the account will be locked. The prevention of ATM fraud is also a focus of this effort. When the vibration

Received: 07.06.2023 Revised: 13.07.2023 Accepted: 03.08.2023

sensor detects anything out of the ordinary, it immediately locks the ATM and releases the gas while also sounding an alarm. This will stop the fraud before it happens by catching the criminal in the act. Millions of people all across the globe rely on ATMs, which are a fantastic piece of technology. Everyday transactions are simplified without stressing the financial infrastructure. They must, however, be protected against theft and other forms of harm. Both the PIN and the magnetic stripes on a smart card are used for authentication in today's modern ATM systems. Therefore, it ensures safety from the perspective of the user. However, much more effort is needed to secure ATMs at the bank's front. Security guards stationed at ATMs alone are insufficient [3].

In the event of a break-in or theft, this project's cutting-edge security system can keep tabs on the situation and spring into action. The ATM booth is protected from potential threats by this security system. The security system monitors many aspects of safety and reports any changes to the appropriate authorities. Reed Switch, an Ultrasonic Sensor, and Cameras are just a few of the sensors used. A reed switch opens the circuit whenever an unauthorized individual tries to move or open the ATM. An ultrasonic sensor is activated to detect an intruder. If one of these conditions changes, the security camera will capture a photo and send a Short Message Service (SMS) to alert the proper authorities, who may then use the Internet Protocol (IP) address to identify the intruder [4]. It's the twenty-first century, and success depends on the reliability and safety of cutting-edge technology. However, there are a lot of holes in this security mechanism, and that's why we keep running into problems. Millions of people throughout the globe utilize ATMs for financial transactions, making this method of payment one of the most important innovations of the modern era. However, many customers are wary about making large transactions at ATMs because of the security risks they face. This study contributes to a solution to this security issue. Two distinct methods of authentication are used in the proposed system. There are two types of security authentication: weak and powerful. There are two phases involved in basic authentication.

Bank-issued PINs and fingerprint scans are the first two options. There are three stages to authenticate with a high level of security. The first is a PIN issued by the bank, the second is Global Positioning System (GPS) tracking, and the third is a combination of Fingerprint and OTP. The 40-second OTP timer will be enforced. In fact, place a premium on robust authentication for security purposes. However, it will initially also provide the option to use weak security authentication so that users may get used to the more secure method. After the widespread use of robust security authentication, the weaker form of authentication will be phased out. The security concern with ATM transactions is resolved by following the procedure outlined [5]. Biometrics, which includes fingerprint technology, is cutting-edge science that uses an individual's unique physical or behavioral characteristics to confirm their identification. Despite the widespread interest in technology from both the public and business sectors owing to its potential advantages, consumer adoption has been sluggish. This research presents a methodology to investigate how consumers' perceptions of the pros and cons of using fingerprint ATMs influence their decisions to use this banking technology. Customers at banks in Jordan who use fingerprint technology at ATMs provided the empirical data. Potential users of the intended technology provided feedback on the suggested framework

The ATM was established in the 1960s to provide customers 24/7/365 access to a wide range of banking services, including cash withdrawal, deposit, account balance inquiries, and more. At first, customers needed bank-issued cards to utilize these services at ATMs. However, there are several drawbacks to employing plastic. As a result, numerous academics came up with other strategies for gaining access to these resources without using cards. To increase safety, some of them employed fingerprint recognition technology, while others relied on one-time passwords. This study presents a novel approach to obtaining cash from ATMs that enhances the security measures of the current approaches. In this setup, there are three distinct authentication methods that may be used to withdraw cash without a card [6]. The problem statement is discussed below. Nowadays, security breaches are a major concern in ATM systems since ATM cards are prone to theft or loss, which leads to miscellaneous transactions. A Minutiae-based algorithm was proposed to enhance security in the ATM system. So that secure authentication is marked by this algorithm for ATM physical cards.

Transactions using fingerprint minutiae are guaranteed to be biometrically un-repudiated. Because each user's Fingerprint is unique, it acts as a robust, verifiable, and non-re-audible credential, connecting them and their transactions. Users are better protected against identity theft thanks to technology. Because fingerprints are distinctive and difficult to counterfeit, fingerprint-based verification greatly reduces the ability of hostile actors to assume the identity of real people. For biometric templates, strong encryption and safe storage procedures are used to protect sensitive, detail-oriented data. By doing this, you may improve system security by preventing unauthorized access to saved templates. Because every transaction is linked to the user's unique Fingerprint, users benefit from increased transaction security. This guarantees the safety, traceability, and protection of financial transactions made at ATMs against unwanted access.

The following section of the literature survey is discussed in section 2, and the proposed system is discussed using a Minutiae-Based Algorithm for the Fingerprint ATM system in section 3. Then, the results and discussion of the given dataset to improve accuracy and security are discussed in section 4. Finally, the conclusion provides the overall performance of the healthcare system and future work.

LITERATURE SURVEY

The results indicate that those who are creative and open to new ideas are more likely to see the benefits of using fingerprint ATMs while banking. The perceived value of fingerprint ATMs is boosted by the advantages people associate with them, such as saving time and mental energy, feeling safer, and having more fun. Value is negatively affected by imagined dangers other than actual danger. Furthermore, it is acknowledged that value perception is a crucial facilitator of fingerprint ATM adoption intent. Banks in Jordan may use the research results to promote and encourage the adoption of fingerprint ATMs among local clients [7]. Thefts of cash from ATMs are widespread in several nations, including India. The most common method for stealing money from an ATM is to damage the machine and shatter the cash vault. Most cash withdrawals from ATMs in India are stolen because of carelessness and a lack of security safeguards. Because it is simpler and less risky than robbing a bank, many criminal organizations resort to robbing automated teller machines instead. Since less money in the hands of banks means less money in the hands of the public, the public is indirectly impacted by the amount lost in the ATM heist [8].

After a string of heists, criminals targeting ATMs have become more sophisticated and risk-taking. Modern methods and equipment, such as gas cutters, welding, and pneumatic breakers, are quicker and more powerful. The whole ATM has been known to be lifted. It is self-evident that no human being can personally ensure the security of every single ATM. The ATMs may be salvageable if they use the right technology. One constant across all methods of ATM heists is the destruction or alteration of the machine itself. The suggested worldview relies on this idea to identify any physical harm done to the automated teller machine containers [9]. This study reports the damage caused by using IoT technology that is available on a global scale. It's the best means of communication available right now. Using internet technology currently available in ATMs, IoT is the greatest potential way to report the incident to the authorities. The goal is accomplished by integrating the embedded systems with IoT. To identify and report ATM robberies, authorities may use ESP8266-based IoT systems coupled with vibration sensors and ATMEGA 328 microcontrollers. This article investigates the matter thoroughly and recommends what is believed to be the best course of action. This study also serves as a copy of the whole system [10].

ATMs are a convenient way for customers to handle their financial transactions. It takes longer to verify clients when they use a bank card or check card type of card during ATM cash transactions or withdraws, and the cards are more susceptible to being rigged at the ATM. This research explores two potential replacements for traditional currency cards: near-field communications (NFC) card-emulation modes and fingerprint technology. NFC is ideal for transactions involving sensitive information since just a small distance (often less than 4 cm) must separate the two devices. In addition to using an NFC tag and reader, a fingerprint sensor may be used to gather user data. The technique will be more secure than the existing method, which employs ATM cards, even if a cash card is not required for authentication. This provides a robust safety net for the authentication process [11].

Selecting a biometric framework that considers a person's unique traits and skills is useful for establishing their identity. Several forms of biometric identification are used for different reasons. Scanning a person's fingerprints or iris is only one example of a difficult but widely used technology that yields complex patterns. Considered the threats to security and decided to go forward with the system using biometrics like Fingerprint and iris scanning. A second chance is to validate the datasets with good scanning using inexpensive and widely accessible equipment [12]. The ATM systems may gain from using these frameworks in several ways. The PINs now used for ATM cards may be tracked and used fraudulently. Combining the PIN, fingerprint scanning, and iris scanning together may greatly improve ATM security, which is now lacking due to the reliance on written PINs. The bank would keep track of and sync everyone's biometric information with their bank accounts. In numerous parts of the globe, people are worried about the safety of ATM withdrawals. The current design of the numerous service sites is the root cause of these problems. The present ATM's reliance on the user's PIN for authentication and identity has led to security issues such as card chewing, lost or stolen PINs, and user forgetfulness. This research provides a theoretical foundation for fingerprint-authenticated automated teller machine software. The fingerprint enrollment, database administration, and authentication components make up the framework [13].

The verification module is broken down into three smaller modules that each use different mathematical models to complete their respective tasks (fingerprint improvement, feature extraction, and matching). The software also facilitates financial transactions like making withdrawals and checking account balances. The implementation was done in C# and Microsoft SQL servers as the frontend and backend engines, respectively, using a Windows 7 operating system. The suggested framework's suitability and usefulness for ATM user verification and authentication are shown by means of experiments measuring the False Rejection Rates (FRR), False Acceptance Rates (FAR), and Average Matching Times (AMT) [14]. These days, ATMs are ubiquitous, and their usage has only increased. People rely on ATMs because they make it easy to get the money they need to cover their regular expenses. Customers use ATMs to deposit and take cash from their bank accounts. Since there has been an uptick in the incidence of ATM-related crimes, it has become clear that these machines need heightened protection. ATMs employ a variety of security measures, including radio-frequency identification (RFID) technology, fingerprint readers, facial recognition cameras, iris scanners, OTPs, reference numbers, a random keypad, and more. A standard ATM system relies on a combination of a bank card and a PIN for verification, which raises a variety of security concerns. This study addresses these problems by exploring how replacing ATM cards and PINs with biometrics has improved the safety of these machines [15].

PROPOSED SYSTEM

The financial services industry is rapidly adopting biometric authentication. The fingerprint notion isn't only for security; it's also meant to help customers who don't quite grasp how ATMs work. Since many clients have savings accounts and need access to their funds outside of normal banking hours, we Suggested equipping ATMs with biometrics and fingerprint security technology. Smart cards and fingerprint scanners are the primary input methods; hence, the devices are very secure for cardholders. If a consumer loses their card, the digital Fingerprint makes it harder for a stranger to use it. When clients see that their fingerprints are required to access their accounts, even if they lose their ATM card, they feel more at ease with the concept of keeping their money in the bank. When it comes to biometric authentications, fingerprint-based identifications are by far the most widely used and well-established technology. Biometrics has the potential for more efficient, user-friendly, accurate, trustworthy, and cost-effective authentication in the financial sector using minutia-based algorithms.

Customers enroll their fingerprints on high-resolution scanners during the transaction process. A secure connection is used to send the fingerprint picture to the main server. At the ATM, a customer's fingerprint image is scanned and compared to the bank's database to ensure it belongs to the customer. If the details match, the authentication is sealed by a signature. The suggested method has the added benefit of being quick. There are typically five major parts to every biometric authentication system. Figure 1 shows the system architecture of the proposed system.

A sensor, feature extractors, fingerprints/template databases, and matches and decision modules are all necessary components. The sensor reads the user's biometric information. The module's job is to take the scanned biometric property and turn it into a usable feature set. Then, the template database is updated with this set of features. The matcher's modules compare the similarity between two inputs, the template database's feature sets and the user's feature set used to authenticate him. Decisions on the compatibility of the two feature sets are made by the last module, known as the verification module. Biometrics is a fast-developing technology with several potential civilian applications. It is already being used in forensics for purposes like criminal identification and jail security. Financial transaction machines, mobile phones, smart cards, desktops, computers, workstations, and computer networks may all benefit from biometrics security measures. The client/server architecture was used to provide the security features for the Indian banking ATMs.

The bank's (server's) records and the customer's accounts will be linked via the customer's identifying data. The network is built to accommodate many users and does so with the help of a dedicated server. Client/Server architecture was selected because it offers the necessary level of protection for the application's resources, which is especially important for financial services. Use case models, activity diagrams, sequence diagrams, and other tools are used to provide a descriptive conceptual approach. Visual Basic 6.0 is the primary tool for developing the ATM's user interface and cardholder interaction. With the advent of electronic banking, customers may manage their finances online from almost anywhere in the globe. Several new developments are met by the electronic banking system, including the need to serve customers at all hours, the need to get products to market quickly, and the complexity of back-office integration. Customers may do things like reorder checks and read bank rates and product information, as well as access their accounts and see recent transactions and requests for statements. The term "e-banking" refers to the delivery of financial services and products to end users over the Internet and other digital networks.

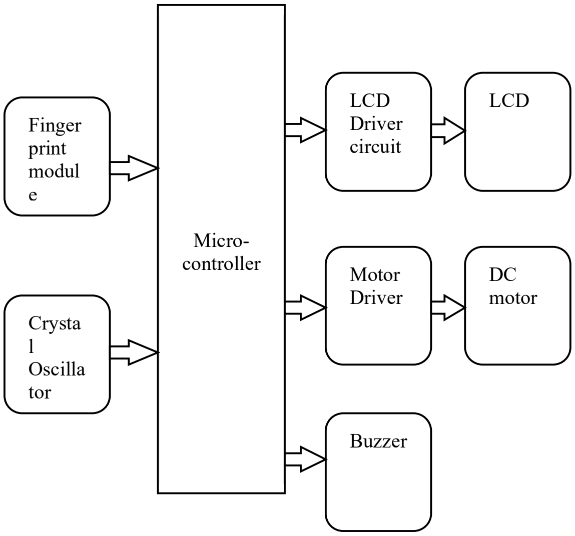

FIGURE 1. System architecture of the proposed system

RESULTS AND DISCUSSIONS

The study's main objective is to develop a measure for authenticating cardholders and nominees using three different factors: the ATM IDs, the PINs, and the biometrics characteristic (fingerprints). Customers are required to have an ATM card, know and remember their PIN, and enroll their fingerprints into the system via a fingerprint device/reader adapter. The consumer provides a live fingerprint sample, which is then compared to a stored template to see whether a match can be made. The suggested verification method ensures the truthfulness of the customer's information before granting them access to the ATM network. It has also offered the idea of a customer's nominee, who would be responsible for completing transactions in their place if the client themselves were unable to. The proposed system's architecture makes use of the Unified Modeling language's (UML) use case modeling, activity diagrams, and sequence diagrams tools to depict the user's (the bank customer) interactions with the systems. System needs may be better understood with the help of use cases.A use-case model may be helpful for projects, plans, and requirements documentation. A use case is a scenario in which users engage with a system; it describes the users' needs and the role of the system in meeting those needs. It defines what occurs in a system and outlines how the system may be put to use, outlining possible actions and sequences of occurrences. In essence, the use case model is aimed at the users or the "actors" of the system rather than its implementers and attempts to systematically discover applications of the systems by providing an external perspective of the systems or applications using a minutiae-based algorithm.

The bank client is conceived of as the application's "actor" in the design of the ATM banking system. With the bank's app, customers may add funds to and take funds from their accounts at will, up to the account's maximum withdrawal limit. The system’s case graphics show how users may complete transactions by inserting their ATM cards and then completing the approval processes by inputting their PIN numbers and confirming their fingerprints. The customer requests the kind of transaction (deposits or withdrawals) after approval, and the transaction is processed appropriately. The fingerprint dataset is shown in Table 1. Figure 2 and Figure 3 show the accuracy performance and security assurance, respectively.

TABLE 1: ATM Fingerprint Datasets

Database	Sensor Type	Image size	Number	Resolution
DB1(FVC 2000)	Optical sensor	300*300	100*8	500dpi
DB2(FVC 2000)	Capacitive sensor	256*354	100*8	500dpi

$$Accuracy = \frac{Total\ correct\ predictions}{Total\ number\ of\ predictions} \quad (1)$$

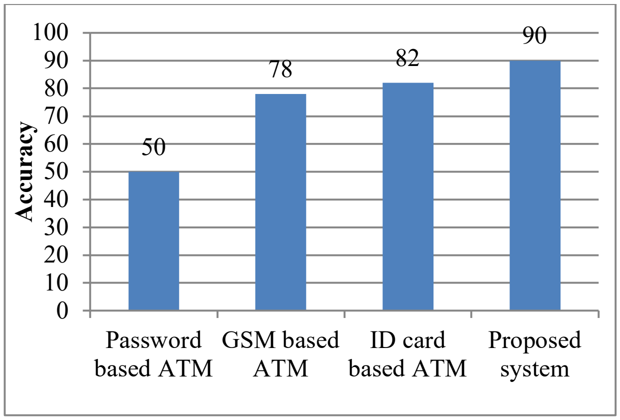

FIGURE 2. Accuracy performance of the proposed system

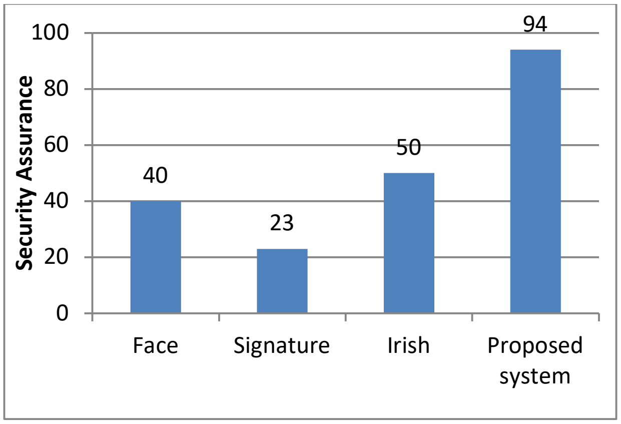

FIGURE 3. Security assurance of the proposed system

Interface Design for Customers and Cardholders: To process inputs and generate outputs, a system requires a Customer/Cardholder interface that is both user- and machine-friendly. It's a way for the user to interact with the computer and get information out of it, using input and output devices and related software. The nine interfaces that make up this ATM app are as follows: 1) ATM Login Interfaces -1 (PIN CODE Interfaces); 2) ATM Login Interfaces -2 (Enroll Fingerprints Interfaces); 3) Banking Transactions Type Interfaces; 4) Withdrawal Interfaces; 5) Deposit Interfaces; 6) Mini statement Interfaces; and 7) Status Interface.

CONCLUSIONS

ATMs have developed into a reliable method of providing banking services to a growing number of people in a variety of nations. The use of biometrics in general and fingerprint scanning in particular as a trustworthy method of safeguarding access via identification and verification procedures is growing in popularity. In this research, determine a high-level framework for integrating PIN and biometric fingerprint strategies into the current ATM infrastructure. To improve the safety of financial transactions in India's electronic banking system, implemented a fingerprint method as a biometric safeguard. Based on the prototype's responsiveness to client fingerprint identification as stored in the database, the built application shows promise. When completely implemented, this method will ensure that only the card's registered owner has access to the bank account, drastically lowering the incidence of ATM fraud. Additionally, the Customers/cardholders' interfaces and/or cardholder interactions with the ATMs were designed using the software tool Visual Basic 6.0. An increased degree of security for ATM transactions is the main outcome. By lowering the possibility of unauthorized access, card-related fraud, and identity theft, the minutiae-based algorithm helps to make the verification process more precise and dependable. Spend money on research to improve minutiae-based algorithms' accuracy and efficiency even further. To enhance the overall performance of fingerprint identification, investigate feature extraction approaches, neural networks, and advanced machine learning techniques

REFERENCES

[1]. T. Sangeetha, M. Kumaraguru, S. Akshay, and M. Kanishka, 2021, "Biometric-based fingerprint verification system for ATM machines," *In Journal of Physics: Conference Series, IOP Publishing*, **1916(1)**, pp. 1-9.

[2]. M.N. Kumar, S. Raghul, K.N. Prasad, and P.N. Kumar, 2021, "Biometrically secured ATM vigilance system," *In 7th International Conference on Advanced Computing and Communication Systems*,**1**, pp. 1-9.

[3]. S.S. Pradhan, 2021, "Fingerprint Based Atm System" (Doctoral dissertation, Srm University)," pp. 1-8.

[4]. S. Takkar, M. Rakhra, A. Ratnani, DS. Protyay, P. Pandey, M. Arora, 2021, "Advanced ATM security system using Arduino Uno," *In 9th International Conference on Reliability, Infocom Technologies and Optimization, (Trends and Future Directions)*, pp. 1-5.

[5]. A. Farzana, N. Mohammad, S. Ahmed, J.A. Mim, J.A. Noshin, 2021, "Trifecta Approach to ATM Transaction Security," *International Journal of Computer Applications*, **975(1)**, pp. 1-9.

[6]. A.A. Trawnih, A.S. Al-Adwan, H. Yaseen, and W.M. Al-Rahmi, 2023, "Determining perceptions of banking customers regarding fingerprint ATMs," *Information Development*," pp. 1-5.

[7]. D. Thirumoorthy, U. Rastogi, B.B. Sundaram, M.K. Mishra, B. Pattanaik, and P. Karthika, 2021, "An IoT implementation to ATM safety system," *In Third International Conference on Inventive Research in Computing Applications*, pp. 744-749.

[8]. K. Renuka, R.P. Janani, K. Lakshmi Narayanan, P. Kannan, R. Santhana Krishnan, and Y. Harold Robinson, "Use of Near-field Communication (NFC) and Fingerprint Technology for Authentication of ATM Transactions," *Intelligent Sustainable Systems: Proceedings of ICISS, Singapore: Springer Nature Singapore*, pp. 415-426.

[9]. M. Doultani, R. Khole, N. Rohra, M. Rashid, and N. Joag, 2021, "Encrypted Biometric Authenticated ATM System–An Overview," pp. 1-7.

[10]. S. Koli, M. Patil, S. Thakare, 2021, "ATM Using Fingerprint," pp. 1-10.

[11]. A. Muley, A. Bendre, P. Maheshwari, S. Kumbhar, and B. Dhakulkar, 2021, "Survey on biometric-based ATMs," *International Journal of Scientific Research Scientific Research in Technology*," pp. 292-297.

[12]. V.D. Amareswari, and G.M. Vuyyuru, 2021, "Card less ATM using 3-level authentication system," *International Journal of Advanced Research in Computer and Communication Engineering*, **10(2)**, pp. 1-5.

[13]. H. Purohit, and P.K. Ajmera, 2021, "Optimal feature level fusion for secured human authentication in multimodal biometric system," *Machine Vision and Applications*, **32**, pp. 1-2.

[14]. D.M. Ahmed, S.Y. Ameen, N. Omar, S.F. Kak, Z.N. Rashid, H.M. Yasin, I.M. Ibrahim, A.A. Salih, N.O. Salim, and A.M. Ahmed, 2021, "A state of the art for a survey of combined iris and fingerprint recognition systems," *Asian Journal of Research in Computer Science*, **10(1)**, pp. 18-33.

[15]. Y. Kuckian, N. Bharambe, A. Sane, and E. Masih, 2021, "ATM Security System Using Gesture and Hand Vein Recognition," *International Conference on Information Systems and Management Science, Cham: Springer International Publishing*, pp. 330-341.