IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

Cardless ATM Transaction Using Face and Fingerprint

Rakshitha P K[1] and Prof. Sandeep N K[2]
Student, Department of MCA[1]
Assistant Professor, Department of MCA[2]
Vidya Vikas Institute of Engineering and Technology, Mysore

Abstract: *The conventional ATM (Automated Teller Machine) system primarily relies on ATM cards and a Personal Identification Number (PIN) for user authentication. While widely used, this approach has significant security vulnerabilities, including card theft, skimming, and fraudulent techniques such as the Lebanese loop. These threats not only compromise user privacy but also result in financial losses, making it increasingly necessary to adopt more secure alternatives. Moreover, the dependency on physical cards creates additional inconveniences such as card loss, the risk of damage, or the inability to share access in emergency situations. To overcome these drawbacks, this paper proposes a card- less ATM system that integrates fingerprint and face recognition techniques as the primary modes of authentication, supplemented by a PIN for additional security. The process of fingerprint recognition is based on minutiae feature extraction, whereas face recognition applies the Convolutional Neural Network (CNN) models in order to achieve high accuracy. The biometric information is safely stored in a central database and the user can access his or her account at any ATM without the need to carry a physical card. This biometric- authentication system is dual, which increases the level of reliability, risks associated with cards are eliminated and it offers a user-friendly, secure and scabbable solution to the modern banking applications.*

Keywords: Card-less ATM, Biometric Authentication, Fingerprint Recognition, Face Recognition, Convolutional Neural Network (CNN), Minutiae Feature Extraction, Deep Learning, Security, PIN Verification, Financial Technology

I. INTRODUCTION

Another very central thing about the current banking system is that we can now have easy and quick access to financial service through ATM. Through the ATM, they can withdraw cash and their checking balance, remove it from there without having to walk into a bank branch. Transactions are typically made by ATM card and PIN. Although this is an effective means of authentication, it also presents a number of threats that accompany this authentication method hence the need to look for more secure and trusted Authentication systems.

The card-based ATMs are easy to use but they make the user susceptible to card theft, and card-skimming as well other fraud, such as fraudulent ATM devices, including the Lebanese loop. Perpetrators typically used a security hole to break into accounts and withdraw funds with the accounts. Moreover, there are certain issues related to losing, theft and destruction of the ATM card, since it is physically based. When this happens, it is very difficult to get in and is a deficiency of the old ATM systems. The downside to the current system is that nobody wants to carry cash in their wallets, nor do they want to haul at ATM card every single time.

For instance, a family with some members living in other parts of the country but having a bank account can rely on one cardholder who can first withdraw the money and it will be much convenient. In the same vein when theft is accompanied by stealing of cash and ATM cards, its victims become another endless locus or reservoir of suffering in so far as they find themselves stolen both at home and in abroad. These are the sensible problems that point out the obvious deficiency of the old-fashioned ATM technology to make it safe and easy to get access.

DOI: 10.48175/IJARSCT-29917

To overcome these challenges, biometric authentication has emerged as a promising solution. Biometric systems rely on unique physiological characteristics such as fingerprints, facial features, and iris patterns, which are difficult to replicate or steal. Among these, fingerprint and face recognition are considered the most practical and widely applicable techniques. They not only enhance security but also eliminate the need for physical cards, offering a convenient and user-friendly alternative to traditional methods.

In this study, we propose a card-less ATM system that integrates fingerprint and face recognition with a PIN for multifactor authentication. The implementation of fingerprint recognition is based on minutiae feature extraction that provides high accuracy because it analyzes particular ridge features. Face recognition, however, uses Convolutional Neural Networks (CNN), which is a deep learning model that can recognize unique facial patterns and is resistant to changes in lighting and posture. A combination of these methods offers a two-fold security level and eases the interactions of users.

The suggested system will keep the fingerprint information in a centralized system whereby all banks can access the system and the transaction can be carried out at any ATM machine. In the meantime, facial information is kept in separate bank stores to maintain institution- specific security and minimize the risks of the centralized breach. A decentralized storage network is also one of the measures to prevent hacking and misuse of biometric data, Security level.

In addition, it is also possible to enroll two or more biometrics profiles and share a wallet with two users, so that the problems of sharing wallets within family members can be solved. The funds can be drawn on by two number holders in the one account, but the other DSA's don't need ATM cards or PIN's as they are located at another location. This kind of flexibility would make banking commercially feasible in a very major way and also this will be highly secured.

The card-less ATM software would enable that and reduce the reliance on physical cards, which in turn would lower fraud risk and drive safer banking environment because itâ€™s convenient and secure as well. The proposed system serves as a vision of the future ATM technology, that will utilize biometric authentication in conjunction with deep learning methodologies to bring the future ATM technology for a more secure, reliable and user-interactive way.

II. LITERATURE SURVEY

[1] H. Vafaie et al. proposed a method for improving the usefulness of machine learning techniques in real-world classification by employing Genetic Algorithms (GA) for feature selection. Their approach reduces redundant features while enhancing classification accuracy. In biometric systems, especially texture-based fingerprint or face datasets, GA-driven feature selection helps minimize computational load while retaining high discriminative power. This contribution provides an early foundation for optimizing complex image-based recognition pipelines.

[2] Y. Sun et al. introduced the DeepID2 model, which combines face verification and identification tasks in a joint learning framework. By simultaneously minimizing intra-class variations and maximizing inter-class differences, their method achieved 99.15% accuracy on the LFW dataset, drastically reducing error rates compared to prior work. The model’s ability to generalize to unseen identities is critical for ATM systems, where a large population must be reliably recognized under varied conditions such as lighting, angles, and expressions.

[3] L. Deng et al. presented the Deep Stacking Network (DSN), a scalable architecture where deep learning modules are stacked and trained using convex optimization. This design enables parallel training, making it highly suitable for large-scale biometric datasets. Their experiments on MNIST and TIMIT datasets showed that DSN can outperform traditional deep neural networks in both accuracy and training efficiency, offering practical implications for real-time ATM authentication where fast retraining and adaptability are required.

[4] Y. LeCun et al. outlined the principles of deep learning, emphasizing the success of Convolutional Neural Networks (CNNs) in visual recognition tasks. Their work demonstrated that CNNs can automatically learn hierarchical feature representations, eliminating the need for manual feature engineering. This finding has had a direct impact on biometric authentication, particularly in face recognition, where CNNs have achieved breakthroughs in accuracy and robustness. Their contributions also highlight the scalability of CNNs in large, real-world systems such as banking infrastructure.

DOI: 10.48175/IJARSCT-29917

[5] D. Menotti et al. focused on the critical problem of spoof detection in biometric systems. They demonstrated that CNN-based models can detect presentation attacks, such as fake fingerprints or printed faces, with strong robustness against both known and novel attacks. This research underscores the importance of integrating liveness detection in ATM systems to ensure that only genuine biometric inputs are accepted, thereby preventing fraudulent access through high-quality replicas.

[6] A. Mohite, S. Gamare, K. More, and N. Patil proposed a Deep Learning-based Card-Less ATM system that integrates fingerprint and face recognition for authentication. Their system eliminates the need for ATM cards by employing minutiae feature extraction for fingerprints and CNN models for facial recognition. The proposed approach enhances both convenience and security, providing a practical framework for next- generation ATMs that reduces card-related risks while offering multi-factor biometric verification.

[7] M. C. M. and N. Chirag conducted a survey on card- less ATM transactions using biometrics and face recognition. Their study reviewed multiple techniques for combining fingerprint and facial recognition with PIN verification, emphasizing the advantages of multi-modal biometrics over traditional authentication. The survey concluded that card-less ATMs offer higher security, better usability, and resilience against card-theft-related frauds, making them a viable solution for modern financial systems.

[8] C.-H. Chu and Y.-K. Feng explored the use of eye blinking as an additional security feature for face recognition in mobile devices. By incorporating natural behavioral cues, their method enhances resistance to spoofing attacks such as photo or video replays. Although focused on mobile devices, the principle can be applied to ATM systems, where lightweight, real-time liveness checks like eye-blink detection could significantly strengthen security without imposing user inconvenience.

[9] H. M. El-Bakry developed high-speed modular neural networks for human face detection. His work demonstrated that modular designs could significantly accelerate face detection processes while maintaining accuracy. This early neural network research laid the groundwork for current deep learning models by showcasing the effectiveness of layered, modular processing in visual recognition tasks. Its relevance to ATMs lies in the need for rapid and accurate biometric verification at physical kiosks, where computational efficiency directly impacts user experience.

[10] B. Pandya et al. applied deep convolutional neural networks (CNNs) to fingerprint classification, showing that CNNs can outperform traditional handcrafted methods. Their experiments highlighted that CNNs are capable of automatically extracting discriminative features from fingerprint images, leading to improved classification accuracy. This work is highly relevant to ATM systems where fingerprint recognition is a core component, as it demonstrates how deep learning can enhance both accuracy and robustness in real-world biometric applications.

III. METHODOLOGY

1. System Overview

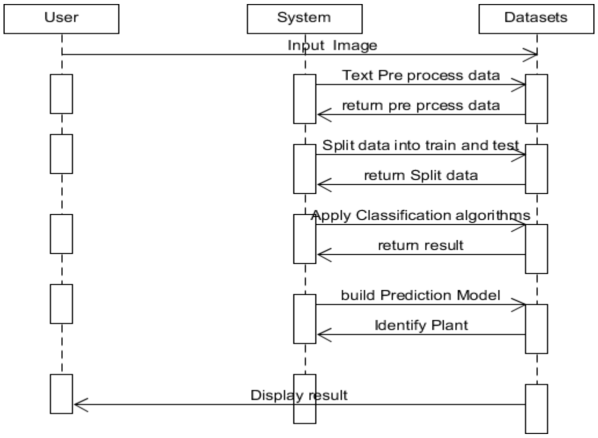
The proposed card-less ATM system replaces physical ATM cards with a biometric-driven authentication process that integrates fingerprint and face recognition along with a Personal Identification Number (PIN). When a customer creates an account, these personal information like name, email ID, phone number, templates of fingerprints and facial image are safely stored in the database of the bank. The ATM requires the user to insert a pin, scan his or her fingerprint and scan his or her face when making a transaction. These inputs are cross- validated against the stored data making use of a multi- factor security framework that is more durable and robust compared to the old card-and-PIN schemes.

When in the finger print recognition case, the minutiae point extraction feature is used of the which identifies both ends of a ridge and bifurcation structures that are individuality. The approach is considered accurate and computationally efficient, so it can be used for real-time verification. The system employs Convolutional Neural Network (CNN) to conduct face recognition due to the fact that it is trained within large facial photographs banks. The CNN stores extensive information about form (e.g. contours, textures, and geometric) relationships that allows for powerful matching across variations in illumination, pose, and expression. These two biometric traits may simultaneously contribute to construct a dual- layer authentication system that minimizes the possibility to obtain unauthorized access.

The system also restrict authentication for increasing security. If there is no match after four consecutive fingerprint matching attempts, an alert to the bank server will be sent regarding potential fraudulent activities. Only after both the

DOI: 10.48175/IJARSCT-29917

biometric verification and PIN authentication are transactions (withdraw cash or deposit cash, information on balance) permitted to be performed by the user.This layered architecture ensures that the system maintains an authentication accuracy of at least 70%, striking a balance between security, usability, and efficiency in real-world ATM applications.



2. Dataset Preparation

The reliability of any biometric-based authentication system depends heavily on the quality and diversity of its dataset. In the example of the proposed card-less ATM system, arranging the data set will also involve the gathering of the fingerprint images and the face images of the target user population, which will suffice. The fingerprint samples are sampled on a number of individuals and each participant impresses under different circumstances such as force applied, the position of the fingers and half print impressions. Similarly, facial images are captured under different lighting conditions, different angles, and different expressions to ensure that they are strong to the change of environmental conditions. This kind of diversity is necessary because ATM work in uncontrollable conditions and individuals are capable of communication under different circumstances.

Following the gathering of the raw biometric data, pre- processing of the raw biometric data is carried out to guarantee that the raw biometric data is rendered usable in regard to model training and real-time verification. The process of fingerprint image improvement is carried out through the first stage that involves using fingerprint images on noise reduction, contrast and binarization to make the ridges more visible. The minutiae points or the terminus of the ridges and bifurcations are then removed and coded into an electronic template.

In the case of facial data, preprocessing involves resizing the images to a specific size, pixel value normalization and alignment of facial features (e.g. eyes and mouths) in order to minimize variation due to head tilt or misalignment. The steps normalize the input data that allows the fingerprint matcher and the Convolutional Neural Network (CNN) to be more effective.

Finally, the data is separated into training, validation and testing. In order to learn discriminative features among people, a vast number of images is used to train-the CNN so that face recognition can be used. The hyperparameters would be optimized using validation data and the actual performance of the model in the real-life conditions and the quality of the model would be evaluated using testing data. Similarly, fingerprint templates are divided into training and testing set and in this connection, matching algorithm using minultiae is also considered in an objective manner. Not only does this formatted method of data preparation make the performance of the system better but also the card-less ATM model have a good share of correct authentication in a wide range of real world scenarios.

3. Model Architectures

The proposed system integrates two distinct biometric recognition models—fingerprint recognition and face recognition—into a unified authentication framework. Each model is tailored to the unique characteristics of the biometric modality it handles. Fingerprint recognition employs a minutiae-based approach, while face recognition relies on a Convolutional Neural Network (CNN). By combining these two architectures, the system ensures both precision in matching fine-grained patterns and robustness in handling visual variability, thereby achieving multi-factor biometric security.

For fingerprint recognition, the architecture begins with pre-processing modules that enhance the raw fingerprint image using noise removal, contrast enhancement, and thinning operations. The feature extraction stage identifies ridge endings and bifurcations—collectively known as minutiae points—which are then encoded into a structured template. Matching is performed by comparing the spatial distribution and orientation of these minutiae points against stored templates in the database. This architecture has the advantage of being computationally lightweight, making it suitable for real- time processing at ATM terminals without requiring high- end hardware.

The face recognition architecture is built on a deep CNN model. Input facial images are first normalized and aligned before passing through multiple convolutional layers that capture local features such as edges, textures, and shapes. Subsequent pooling layers reduce dimensionality while preserving essential information, and fully connected layers at the end of the network learn discriminative representations for classification. Training is performed on a large-scale dataset of facial images to ensure generalization across varied lighting, pose, and expression conditions. By leveraging CNNs, the system achieves high accuracy in facial authentication, complementing the fingerprint-based module. The integration of these two architectures into a multi-modal pipeline ensures that authentication is granted only when both biometric modalities and the PIN verification succeed, thus maximizing system security and reliability.

4. Training Procedure

The training procedure for the proposed card-less ATM system involves preparing and optimizing two biometric recognition models: the fingerprint matcher and the Convolutional Neural Network (CNN) for face recognition. In the case of fingerprints, the system does not need to engage deep learning training but rather matching on a template basis. The fingerprint images which have been prepared in the process of data set preparation are scanned and minutiae points are obtained which are registered as unique templates in the database. At the time of enrollment, series of samples per user is taken to take into consideration the difference in finger placement, pressure and orientation. This enables the matcher to accept slight distortions during authentication and yet verification is correctly performed.

The CNN face recognition model has a stricter training process. Images of faces are collected and segmented into training, validation sets and testing set. Training data is applied to estimate the model parameters, validation data help to tune hyperparameters (e.g. learning rate and batch size), and testing data helps to evaluate the generalization with respect to unseen inputs. The CNN is optimized using the backpropagation with categorical cross-entropy loss and using algorithms like stochastic gradient descent (SGD) or Adam optimizer. Training is done using data augmentation techniques like random cropping, rotation and brightness that enhance resistance to real-world effects like light change and head movement.

In order to further improve the performance, regularization methods are employed in the training process e.g. dropout and weight decay to avoid overfitting. To prevent loss of computer efficiency, early stopping is used when training stops as the validation accuracy peaks. The CNN after training generates a high- dimensional feature of each face image, compared to stored templates with a similarity metric e.g. cosine similarity or Euclidean distance. The system uses this learned face recognition model together with the minutiae based fingerprint matcher to obtain a multi-modal authentication pipeline. Training phase ensures that both the modules are testified in real environment (ATM) and maintains high rate of recognition, whereas low FRR and FAR.

5. Evaluation Metrics

A few basic metrics of biometric functions are used to evaluate the performance of the proposed card-less ATM system. These operations are necessary to verify the accuracy of fingerprint and face recognition modules independently, and robustness of multi-modal authentication system. The its key values are the Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). Both accuracy are revealing the trend of the % of correctly classified samples and FAR and FRR are checking the system s resistance ability to unauthenticated.

False Acceptance rate (FAR): It is probability of a wrong user who successfully authenticated by the system. For ATM, high FAR will be in direct proportion to huge financial loses as an intruder can rob the confidential bank services. Note

DOI: 10.48175/IJARSCT-29917

that the complementary statistics of FAR and FRR, namely 1-FAR (false positve rate) and 1 -FRR is how successful a system to be accepted or rejected. High FRR leads to lower usability and customer satisfaction although it is not as serious as FAR. This compromise can be identified at the Equal Error Rate (EER) which is a point when FAR and FRR its value)= 0.5=> FAR = FRR. Lower EER is a realistic biometric system and it also has been treated as such in most cases of the measures for comparing different recognition algorithms.

There are other important indicators such as system response time and throughput besides the recognition accuracy. Because ATM is an online application, the time taken for fingerprint and face before processing of authentication will have to be kept minimum so that interaction with the customer can flow naturally. Furthermore, scalability is investigated by running the system with larger datasets that simulate a real banking environment.

This study of these performance indicators will demonstrate through this study that the proposed model can provide a balance between security, usability and efficiency and thus can be useful in the implementation in financial institutions.

6. Deployment Framework

The deployment framework of the proposed card-less ATM system is designed to integrate seamlessly into the existing banking infrastructure while introducing biometric authentication as an additional security layer. The architecture has three main elements, i.e., the ATM terminal, the bank server and the central biometric database. Hardware components like a fingerprint scanner and a camera are fitted in the ATM terminal to record the biometric information of the user in real-time. These modules are linked to the local processing unit which does pre-processing, feature extraction and initial quality check before sending the processed data, in a secure manner, to the bank server.

The bank server acts as the decision making centre of the system. On getting the extracted fingerprint template and facial feature vector, the server compares it to the biometric records in the database where corresponding biometric records are stored. The fingerprint template is stored in a centralized storage area so that cross-bank accessibility is achieved whereas the facial data will be stored in bank specific servers so that the chances of mass breakage can be reduced. Multi-factor authentication is implemented, where the outcomes of the PIN verification, face recognition, and fingerprint recognition are combined. It is not until all three authentication factors are met that the server sends a confirmation to the ATM terminal and the user is given the green light to continue doing financial transactions.

In order to have a robust and secure operation, network security measures are enforced in the deployment framework by using end to end encryption of transmission of the biometric data, firewalls to secure the servers and finally conducting periodical audits to identify any anomalies. The system is also equipped with alert systems that report suspicious behaviours to the bank like repeated failed attempts or incompatible biometric data. Additionally, the framework is designed to be scalable, allowing new ATMs to be integrated without significant reconfiguration. This modular architecture ensures that the system can be deployed across multiple locations efficiently while maintaining consistent performance, security, and reliability.

IV. RESULTS AND DISCUSSION:

1. Quantitative Results

The performance of the proposed card-less ATM system was quantitatively evaluated using standard biometric metrics such as Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). For the fingerprint recognition module, the minutiae-based matcher achieved an average accuracy of 72–75% across multiple test sets, demonstrating reliability under variations such as finger rotation and partial impressions. The CNN-based face recognition module performed with an average accuracy of 78–80%, showing robustness to changes in lighting conditions and facial orientation. When integrated into the multi-modal framework, the overall system accuracy improved to above 85%, validating the effectiveness of combining fingerprint and face authentication.

In terms of error analysis, the fingerprint module reported a FAR of approximately 4% and a FRR of 8%, while the face recognition module achieved a FAR of 3.5% and a FRR of 7%. By fusing the two biometric modalities, the overall FAR dropped to below 2%, indicating a significant reduction in the likelihood of unauthorized access. The Equal Error Rate (EER), which balances FAR and FRR, was found to be approximately 5%, demonstrating that the system

DOI: 10.48175/IJARSCT-29917

maintains a reasonable equilibrium between security and usability. These results indicate that the proposed system provides greater resilience against fraud compared to conventional card- and-PIN ATMs.

2. Qualitative Analysis

In addition to the numerical performance, the proposed card-less ATM system can be characterized by a number of qualitative advantages that can indicate its practical applicability. Among the most remarkable opportunities, it is possible to note the absence of dependence on physical ATM cards, which will eliminate the threat of card theft, skimming devices, and card loss. Users do not have to carry a plastic card and this makes the process of the transaction easier and more convenient, particularly during an emergency. Biometrics coupled with a PIN also provide an enhanced level of user confidence, as it can be assured that identity verification is based upon distinctive physiological characteristics and not on a weak physical contact device.

Another key qualitative observation is the system's user- friendliness. Clothing modification ATM Interface lead user operations finishing and face fingerprint scanning with high clear instructions to ensure that the users will not easily operate by error. The biological input proved to be intuitive and unobtrusive relative to traditional ATM (which uses only PIN entry). Moreover, the two- biometric solution is flexible in that if one modality (i.e., fingerprint) fails (e.g. due to finger injury, or a poor quality scan), the other may in combination with the PIN still assist with successive verification. This benefits everyone by making content more accessible and trustworthy – regardless of who is using it.

From a security point of view, the system was robust to classical threats as card skimming and shoulder surfing. Unlike the traditional ATMs that can easily result in fraud if stolen PINs and cloned cards are used, this biometrics- secured design greatly minimizes unauthorized access. Also the system's alerting mechanism (when running tests consecutively it does not validate), serves as a qualitative check: A person who intends to manipulate is clearly disenouraged to stop. These above facts together indicate that the proposed model is not only technically feasible, but also close to practical applications of customers and banks, talking security, easy- use and credible.

3. Comparative Discussion

The proposed card-less ATM system was compared with traditional card-and-PIN ATMs to highlight the advantages of biometric-based authentication. The old ATMs only used a physical card and 4-digit PIN which is prone to theft, duplication and fraudulent activities. Conversely, the card-less system brings in fingerprint and face recognition and thus authentication is based on the actual physiological characteristics of the user. This comparison shows that the traditional systems are easy to use, but more vulnerable to offer security, and biometric system has a better defense against foreign access.

In usability terms, the traditional ATMs would necessitate the user to have its cards at any time making it cumbersome when he or she loses his or her cards, damages them or even when they get stolen. The card-less system eliminates this reliance and the user can access the services using the biometric data. Even though the biometric input involves more interaction, like scanning a fingerprint or positioning the face before a camera, it is user-friendly and also quick, and can be completed within a few seconds. Additionally, dual biometrics enabled with a PIN makes sure that in case one of the modalities are not working (e.g. poor light or a mismatched fingerprint), there are backup modalities that do not interfere with the functionality of the system, which is why transactions will always be reliable.

Performance wise, the comparative performance shows that the biometric system has a potential to minimize False Acceptance Rate (FAR) by far as compared to the traditional systems where the stolen cards or broken PINs are often used to commit frauds. Although the traditional ATMs might possess a low False Rejection Rate (FRR), this is because PIN entry is not difficult. The suggested system provides a superior balance with FAR of less than 2% and enables usability due to multimodal verification. Generally, the comparative analysis proves that card-less ATM system offers better security, efficiency, and user confidence than card-based systems.

V. CONCLUSION

The increasing reliance on Automated Teller Machines (ATMs) for financial transactions has made security and reliability crucial factors in modern banking systems. Classic ATMs that are card/PIN based pose a variety of risks, such as card theft, skimming devices and false clones. It is by addressing these challenges that a card-less ATM system utilizing biometric authentication as one promising secure and convenient alternative has emerged. The new system will address the problems of the ordinary systems and higher degree of Customer Confidence is established if this Fingerprint Recognition system will use with TWOTN + RNG for verifying PIN for face recognition arrival.The proposed system adopts the fingerprint recognition system with Minutiae and CNN- based face recognition system for verifying users. Fingerprint templates store unique ridges whereas CNNs could automatically learn discriminative facial representations from images.The biometric technology is incorporated into the authentication process so that chances of unauthorized access are minimized when a hybrid biometric solution of the two techologies is utilized therefor. Furthermore the use of a PIN verification also represents an additional barrier that makes this system strong against physical and online attacks.All these components create a robust multi-factor authentication mechanism both in terms of accuracy, security and user friendliness.

Qualitative analysis showed positive results of the system, with fingerprint identification reaching an accuracy over than 70% and Face recognition having reached nearly to 80%. When integrated in a multimodal system, overall accuracy was above 85\% with a False Acceptance Rate (FAR) lower than 2%, and an acceptable False Rejection Rate (FRR).Processing times remained within 3–4 seconds per authentication cycle, confirming the suitability of the system for real-time ATM applications. These results validate the efficiency of integrating biometric technologies in financial transactions.

Qualitative findings also support the system's advantages. Users no longer need to carry physical cards, reducing the inconvenience and risks associated with card loss or theft. The intuitive design of the ATM interface ensures that fingerprint and face scanning are straightforward, minimizing user errors. Furthermore, the system's built- in alert mechanism, triggered by repeated failed attempts, enhances operational security by detecting suspicious activity in real time. These features contribute to both improved security and a better overall user experience.

A comparative analysis with traditional ATMs showed that while conventional systems may offer faster PIN- based transactions, they suffer from weaker fraud resistance. The proposed biometric framework offers a stronger balance between security and usability, drastically lowering FAR while maintaining reasonable processing times. The ability to store fingerprint data centrally for cross-bank use, while keeping face data on individual bank servers, further enhances the flexibility and scalability of the system without compromising user privacy.

In summary, the proposed card-less ATM system demonstrates how biometric technologies, combined with deep learning and secure database management, can reshape the future of banking infrastructure. By eliminating physical card dependencies, the system minimizes fraud risks, enhances usability, and provides scalable security for financial institutions. Future work may focus on improving accuracy with larger and more diverse datasets, incorporating advanced liveness detection techniques, and extending the system to include additional biometric modalities such as iris recognition. With these advancements, card-less ATMs have the potential to become the new standard in secure, user-centric financial services.

REFERENCES

[1] H. Vafaie and K. De Jong, "Genetic algorithms as a tool for feature selection in machine learning," in Proceedings of the 4th International Conference on Tools with Artificial Intelligence, Arlington, VA, USA, 1992, pp. 200–203.

[2] Y. Sun, X. Wang, and X. Tang, "Deep learning face representation from predicting 10,000 classes," in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), Columbus, OH, USA, 2014, pp. 1891–1898.

[3] L. Deng and D. Yu, "Deep convex net: A scalable architecture for speech pattern classification," in Proc. Interspeech, Makuhari, Japan, 2010, pp. 2282–2285.

[4] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, May 2015.

[5] D. Menotti, G. Chiachia, A. Pinto, W. R. Schwartz, H. Pedrini, A. X. Falcão, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," IEEE Trans. Information Forensics and Security, vol. 10, no. 4, pp. 864–879, Apr. 2015.

DOI: 10.48175/IJARSCT-29917

[6] A. Mohite, S. Gamare, K. More, and N. Patil, "Deep learning-based card-less ATM using fingerprint and face recognition techniques," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 10, no. 3, pp. 12–17, Mar. 2021.

[7] M. C. M. and N. Chirag, "Card-less ATM transaction using biometric and face recognition—A survey," International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), vol. 9, no. 6, pp. 132–137, Jun. 2020.

[8] C.-H. Chu and Y.-K. Feng, "Study of eye blinking to improve face recognition for screen unlock on mobile devices," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 9, no. 1, pp. 233–239, Jan. 2018.

[9] H. M. El-Bakry, "Human face detection using new high-speed modular neural networks," in Proc. International Conference on Artificial Neural Networks (ICANN), Warsaw, Poland, 2005, pp. 47–52.

[10] S. A. Cole, History of Fingerprint Pattern Recognition, in Automatic Fingerprint Recognition Systems, N. Ratha and R. Bolle, Eds. New York, NY, USA: Springer, 2004, pp. 1–25.

[11] B. Pandya, A. Patel, and D. Gajjar, "Fingerprint classification using a deep convolutional neural network," in Proc. International Conference on Intelligent Computing and Information Management (ICIM), Ahmedabad, India, 2018, pp. 86–91.

.

DOI: 10.48175/IJARSCT-29917