Seamless Banking: Innovations In Card-Less ATM Systems Utilizing Biometric Authentication Through Fingerprint And Facial Recognition

Shruthi K
Assistant Professor, Dept of Master of Computer Application

Abstract- *Users now have a simple and safe option to access their bank accounts without using actual cards thanks to the rise of cardless ATM operations. In this research, we used machine learning classification methods to build a strong authentication system using datasets of images of the finger and face. To prevent illegal access and improve user experience, it is important to guarantee a trustworthy and accurate verification procedure. Machine learning algorithms are being trained for the project on the gathered face and finger picture datasets. The algorithms may identify trends and create classification models by sifting through the photos and collecting pertinent characteristics. SVM has demonstrated greater accuracy in separating between real and imposter users among the studied algorithms, making it the algorithm of choice for this application. If the user's face and finger photos match, access to their account is allowed, allowing for safe and effective cardless ATM transactions. The outcomes of this experiment show how useful SVM is for precise authentication during cardless ATM transactions.*

I. INTRODUCTION

ATM (Automated Teller Machine) is generally used for withdrawal of money from our Bank account without going to the bank. Using an ATM which is used as an agent through which we can access our bank account remotely by providing ATM card details with a proper PIN, one can withdraw, deposit, or check the account balance. But in today's ATM technology, there is always a chance of stealing money. The money can easily be stolen if one gets access to an ATM card and security PIN rather there is always a chance of losing an ATM card and during that period withdrawal of money gets difficult. In addition to that, we always have to carry ATM cards everywhere we go and only one person can have access to the card which sometimes can get pretty difficult when members of the same family want to withdraw cash, who are at different locations.

In addition, if you are new in an area or country and the purse you are carrying in which all of your cash and ATM card are kept gets stolen then undoubtedly it will be the worst situation to survive.

To overcome such drawbacks the idea of a card-less ATM that uses fingerprint and face recognition for authorization and authentication of users seems quite useful and reliable. For instance, if two members of the same family are at different locations in a country then both of them can have access to the same account anywhere and anytime, they want without carrying an ATM card. In this technology, we take the user's fingerprint and face-print as a replacement for ATM cards which data is stored in a separate server to provide a common ground for accessing fingerprints through any bank's ATM, and with face recognition we add a double layer of security of which data is stored in particular bank's server By providing the data of Fingerprint and face ID of two members for a particular account a single account can be accessed by two persons.

II. PROPOSED SYSTEM

We propose a system that uses fingerprint and face recognition authentication (not ATM cards) for accessing user accounts which is more secure and reliable than the existing system. Here we are using the CNN model for face recognition and Minutiae feature extraction for fingerprint recognition.

III. LITERATURE SURVEY

3.1.Haleh Vafaie et al. provides us with a way to improve the usefulness of machine learning techniques for generating classification rules for complex, real-world data. This approach reduces the number of features necessary for texture classification and simultaneously makes improvements in recognition rates. The approach involves the use of genetic algorithms (GA) as a front end to traditional rule induction systems to detect and select the best subset of features to be used by the rule induction system. This technique has been implemented and tested on difficult texture classification problems.

3.2.Yi Sun et also that the difficulties with face recognition can be well solved with deep learning and using both face verification and identification signals as supervision. The challenge of face recognition is to build effective feature representations for lowering intrapersonal variations while enlarging interpersonal differences. The face identification task increases the interpersonal variations by drawing DeepID2 features obtained from various identities apart, while the face verification task lowers the intra-personal variations by pulling DeepID2 features obtained from the same identity together, both of which are essential to face recognition. The learned DeepID2 features can be well generalized to new identities unnoticed in the training data. On the challenging LFW dataset, 99.15% face verification accuracy is maintained. Compared with the previous deep learning result on LFW, the error rate has been drastically reduced by 67%. Deep Learning Face Representation by Joint Identification-Verification reduces intra-personal variations while enlarging inter-personal differences. Scalable stacking and learning for building deep architectures Deep Neural Networks(DNNs) has shown remarkable success in pattern recognition tasks.

3.3.The DNN provides a method of stacking simple processing modules in building deep architectures, with a convex learning problem in each module. Additional fine tuning further improves DSN, while introducing minor non-convexity. In the DNN full learning is batch mode, making it amenable to parallel training over many machines and thus be scalable over the potentially huge size of the training data. Experimental outcomes on both the MNIST (image) and TIMIT (speech) classification tasks demonstrate that the DSN learning algorithm developed in this work is not only parallelizable in implementation but also attains higher classification accuracy than the Deep Neural Network as proposed by Li Deng et al.

3.4.Yann LeCun et al Reff. in the finding of the paper "Deep learning" show us that deep learning discovers intricate structures in large data sets by using the backpropagation algorithm to indicate how the machine should change its internal parameters that are used to compute the representation in each layer from the representation in the previous layer. It allows computational models which are composed of multiple processing her archery to learn representations of data with multiple levels of abstraction. These methods have drastically improved the state-of-the-art in speech recognition, visual object recognition, object detection, and many other domains such as drug discovery and genomics. The Deep convolution nets have brought about breakthroughs in processing images, video, speech, and audio, whereas recurrent nets have shone a light on sequential data such as text and speech. It also helps to Reduce the need for feature engineering Quality and accurate results.

3.5.David Menotti et al show us that the results strongly indicate that spoofing detection systems based on CN can be robust to attacks already known and possibly adaptedwith little effort, to image-based attacks that are yet to come. Biometrics systems have significantly improved.
Person identification and authentication, play an important role in personal, national, and global security.

IV. SURVEY PAPERS

The survey papers collectively underscore the transformative impact of machine learning and deep learning techniques across various domains. They demonstrate how optimization methods and advanced neural network architectures can enhance performance, scalability, and security in tasks ranging from texture and face recognition to biometric authentication. The progress in these areas reflects the growing capabilities of these technologies to tackle complex, real-world problems and drive significant improvements in accuracy and efficiency.

V. METHODOLOGY

The System Cardless ATM uses fingerprint recognition and face recognition instead of an ATM card for authenticating the user. The user information is stored in the database while the user opens an account in the bank. The information such as name, email ID, mobile number, fingerprints, and face-print is registered into the database. The cardless ATM uses fingerprint recognition and face recognition techniques for authentication and authorization. Here we have implemented using the real-time database. Face recognition uses a CNN model for classification and fingerprint recognition uses minutiae features for extraction. Only 4 chances are provided for the user for fingerprint recognition if it doesn't match sends an alert message is sent to the bank server. Then the user needs to visit the bank to resolve the issues. The accuracy percentage to be mapped between both the recognition is 70% + for authentication. If the user is valid he/she can withdraw /deposit cash. Deep learning is part of machine learning methods based on learning data representations, as opposed to task-specific algorithms. Learning can be supervised, semi-supervised, or unsupervised [15]. Deep learning models are vaguely inspired by information processing and communication patterns in biological nervous systems yet have differences from the structural and functional properties of biological brains(especially human brains), which make them incompatible with neuroscience evidence[16].

VI. ALGORITHM

I'll take a look at the code in the uploaded file and then summarize the algorithm for you. Let me check it out.

The code appears to be a combination of a Flask application and various machine learning libraries, including TensorFlow/Kera's, OpenCV, and Scikit-learn, with additional modules for handling image processing, plotting, and file management. Below is a high-level overview of the likely algorithm structure based on the imported libraries and functions:

1) **Flask Setup: **
   a) Initialize a Flask application to handle HTTP requests.
   b) Define routes to render HTML templates and manage user interactions.

2) **File Upload & Handling: **
   a) Provide a mechanism for users to upload files (likely images or datasets).
   b) Secure the filename and save the uploaded files to a specified directory.

3) **Image Processing: **
   a) Use OpenCV to load, process, and analyze images.

   b) Convert images to a format suitable for machine learning models (e.g., using `img_to_array`).

4) **Model Loading & Prediction: **
   a) Load pre-trained machine learning models (e.g., TensorFlow/Kera's models).
   b) Use the loaded model to make predictions on processed input data.

5) **Data Visualization: **
   a) Utilize Matplotlib and Plotly to create visualizations, possibly displaying model predictions or input data characteristics.

6) **User Interaction: **
   a) Use Flask to manage user sessions, handle form submissions, and redirect users based on their actions.
   b) Use Tkinter for GUI elements, possibly for local applications outside of the Flask web interface.

7) **Email & Notifications: **
   a) Set up an SMTP client to send notifications or alerts via email, possibly based on model predictions or other triggers.

8) **Data Storage & Logging: **
   a) Save user input or model predictions to CSV files for logging purposes.
   b) Use Pandas for data manipulation and saving structured data.

This overview is based on the initial review of the imports and a portion of the file. If you need a more detailed algorithm or have specific sections of the code you want analyzed, let me know!

VII. CONCLUSION

In conclusion, the development of a Threat Detection Engine utilizing Machine Learning techniques presents a promising solution to combatting evolving cyber threats. By expanding threat coverage and employing advanced algorithms, the engine offers enhanced accuracy and efficiency in detecting phishing and BEC attacks. Through rigorous testing and validation, the system demonstrates its reliability and effectiveness in real-world scenarios. Furthermore, the project contributes to the ongoing advancement of cybersecurity by addressing critical challenges and proposing future research directions. Overall, the Threat Detection Engine stands as a proactive defense mechanism, empowering organizations to safeguard their digital assets and mitigate risks posed by malicious actors.

VIII. FUTURE WORK

Future enhancements for a machine learning-based cardless ATM system could focus on integrating multimodal biometrics, such as iris or voice recognition, to improve accuracy and security. Advanced anti-spoofing techniques and real-time fraud detection will enhance system integrity. Streamlining the user experience by optimizing authentication speed, incorporating accessibility features, and personalizing interfaces will improve convenience. Ensuring seamless integration with existing banking systems and compliance with privacy regulations will support broad adoption and ethical use. Additionally, ongoing updates and research will drive continuous improvements and innovation.

REFERENCES

[1] Manish vCard-Less ATM transaction using Biometric and Face Recognition— A Review ISSN: 2321-9653; IC

Value: 45.98; SJ Impact Factor: 7.429 July 2022- Available at www.ijraset.com

[2] Aysush Mohite Deep learning-based cardless ATM using fingerprint and face recognition technique March 2022,

[3] Ashwini Shashank's cardless banking atm system service using biometric and face recognition techniques in 2278-0181

[4] Aditya Lande cardless atm system February 2013 DOI: 10.48175/1JARSCT-8362

[5] Samuel Solomon CARDLESS ATM TRANSACTION USING BIOMETRIC AUTHENTICATION DOI:10.5281/zenodo.7137003 October 2022