Avoid Fraudulant Activities In Netbanking Transaction Using Ai And Blockchain Technology

Mr . D. Sivaramakrishnan[1], Mr .S. Kabilan[2], Mr . S. Suresh[3], Mr . V. Sanjay[4]
[1, 2, 3, 4] Dept of Cyber Security Engineering
[1, 2, 3. 4] Paavai Engineering College, Namakkal, Tamil Nadu, India

Abstract- *Biometric traits can be used to confirm a person's identification because password authentication is prone to dangers such as hacking. The face is a secure feature and protected front portion of the head, with a random texture that is distinctive and very stable throughout life. It can operate as a sort of living passport or password that does not need to be remembered but is always present. As a result, one successful means of securing online transactions is face recognition. A facial recognition system provides a user-friendly authentication solution that is accurate, robust, fast, and secure. It Obtains, processes, analyses, and compares facial patterns from users' iris images to ensure their personal identity. The purpose of the system is to improve online banking security by adopting a facial biometric technique for safe authentication. The purpose of the proposed system is to construct an application that will ask for the user's username, password, and an iris image, which the user should supply using his or her device's camera. The application will pre-process the iris image before checking it against the database. The user is considered an authorized person if his or her username, password, and iris image match those in the database. Blockchain technology provides high levels of data security, as well as an open and transparent network infrastructure, decentralization, and low operational expenses. Banking activities are inextricably linked to deposits and loans. Because the deposits are not controlled by a single company, a distributed system for loans and deposits based on ledger technology is decentralized and cannot go bankrupt.*

I. INTRODUCTION

During the enrolment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. Selection of biometrics for any practical application depends on the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption. The project aims to develop an application that will ask for the username, password as well as a face image of the user, which the user should provide through his respective device camera. Also implement cued click point selection for face recognition approach. The application will pre-process the iris image and scan through the database for authentication. If the username, password and face image matches with that in database then the user is authenticated

II. PROBLEM IDENTIFICATION

Face is a protected internal organ whose random texture is complex, unique, and very stable throughout life, it can serve as a kind of living password that one need not to be remembered but can always be present. So here implement face recognition with transaction OTP verification is efficient way of securing online transactions. During face registration user should select click point on face image to improve authentication. The first time an individual uses a biometric system is called enrolment. During the enrolment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrolment. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the role.

III. FEASIBILITY STUDY

Feasibility study examines the viability or sustainability of an idea, project, or business. The study examines whether there are enough resources to implement it, and the concept has the potential to generate reasonable profits. In addition, it will demonstrate the benefits received in return for taking the risk of investing in the idea. These studies analyze strengths, weaknesses, opportunities, and threats to determine whether the proposals are cost-effective and beneficial to a company’s long-term success. Furthermore,

investors can benefit from evaluating the problems and solutions listed in the study and determine whether a proposed project is the right choice for a company

- **TECHNICAL FEASIBILITY**

This assessment is based on an outline design of system requirements, to determine whether the company has the technical expertise to handle completion of the project. When writing a feasibility report, the following should be taken to consideration: • A brief description of the business to assess more possible factors which could affect the study • The part of the business being examined • The human and economic factor • The possible solutions to the problem At this level, the concern is whether the proposal is both technically and legally feasible (assuming moderate cost).[citation needed. The technical feasibility assessment is focused on gaining an understanding of the present technical resources of the organization and their applicability to the expected needs of the proposed system.

- **OPERATIONAL FEASIBILITY**

Operational feasibility is the measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development. The operational feasibility assessment focuses on the degree to which the proposed development project fits in with the existing business environment and objectives with regard to development schedule, delivery date, corporate culture and existing business processes.

- **ECONOMICAL FEASIBILITY**

Economic evaluation is a vital part of investment appraisal, dealing with factors that can be quantified, measured, and compared in monetary terms (Chen 1996). The results of an economic evaluation are considered with other aspects to make the project investment decision as the proper investment appraisal helps to ensure that the right project is undertaken in a manner that gives it the best chances of success. Project investments involve the expenditure of capital funds and other resources to generate future benefits, whether in the form of profits, cost savings, or social benefits. For an investment to be worthwhile, the future benefit should compare with the prior expenditure of resources need to achieve them

IV. DESIGN

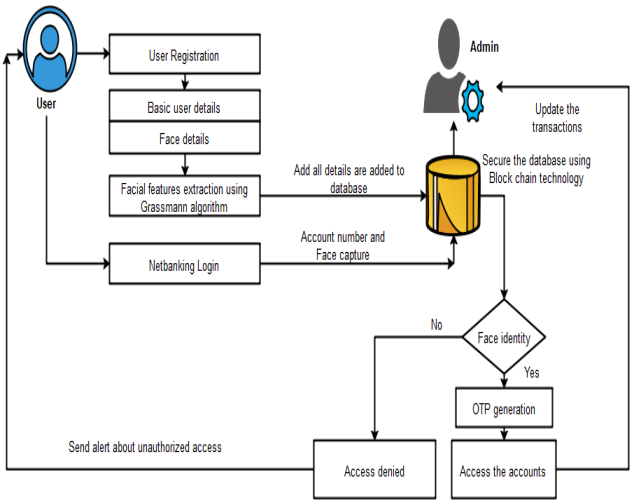

Figure: Architecture of the software

V. ELECTRONICS COMPONENT

HARDWARE REQUIREMENTS

- Processor : Dual core processor 2.6.0 GHZ
- RAM : 4 GB
- Hard disk : 320 GB
- Compact Disk : 650 Mb
- Keyboard : Standard keyboard
- Monitor : 15 inch color monitor

SOFTWARE REQUIREMENTS

- Operating system : Windows OS
- Front End : Python
- Back End : MySQL SERVER
- IDLE : Python 2.7 IDLE

VI. BANKING PROCESS

- Bank Interface Creation

Traditional techniques such as password or tokens are no match to their attacks. User Interface is an important component of every computing system. This is particularly true in Internet Banking, where the users are customers, who access the banking services online, from different locations of the world. These customers when dissatisfied with the banking services could take drastic actions, such as spreading service failure related rumors, withdrawal of patronage, and so on. Since customers access Internet Banking services through the user interfaces via the websites, it means that such interface designs should follow best practices and highest standards.

Though no singular Internet Banking System may be termed as superior over the rest of the others in the world, it is necessary that system designers should be contemporary, innovative and customer-centric. To overcome, these attacks, we can design the interface for online transactions in banking system. In this module, admin and user interface created. Admin can be view the details of users, accounts details and so on. The user can be performing various operations such as net banking, credit card transactions, and debit card transactions and on.

- User Registration Process

The Face Recognition is the study of physical or characteristics of human being used for the identification of person. These physical characteristics of a person include the various features like fingerprints, face, hand geometry, voice, and iris biometric device. These Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking-based account security systems. Face recognition presents a challenging problem in the field of image analysis and computer vision. The security of information is becoming very significant and difficult. In this module, we can implement 12 features-based method to detect the facial parts such as nose, lips, eyes, cheeks using iterative closest point algorithm.

- User PIN Verification

In this module, perform the verification of multiple users using classification algorithm named as Convolutional neural network algorithm. With the development of convolutional neural networks, the achievements made in various competitions are getting better and better, making it the focus of research. In order to improve the training performance of the forward BP algorithm, an effective method is to reduce the number of learning parameters. This can be done by convolution of the spatial relationship of the neural network. Convolutional neural network, the network structure is proposed, it minimizes the input data pre-treatment. In the structure of convolution neural network, the input data is input from the initial input layer, through each layer processing, and then into the other hierarchy, each layer has a convolution kernel to obtain the most significant data characteristics.

- Face Image Verification

One time password can be generated using random algorithm. Hash algorithms are fundament to many cryptographic applications. Although widely associated with digital signature technology, the hash algorithm has a range of other uses. A secure hash algorithm, often known simply as an "SHA," is a hashing algorithm that is considered cryptographically secure. In general, hashing functions are used to sort and organize digital data into smaller, more categorized packets for password. And transfer the OTP to Server. Server can compare OTP and Allow access to the system. In the secondary access, OTP can be transfer to main user and also secondary users. A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

- Online Transaction

SMS Notifications are out-of-band text messages sent in response to events or transactions which occur somewhere else. While often used as a marketing tool to increase the percentage of returning visitors, SMS notifications are very useful for organization and public safety purposes as well. Finally provide SMS alert to primary users about the transactions. The details of the transactions have user name of account access, timing details, amount details, mode of payments and so on. Based on these details, primary user easily knows the transactions details up to date.

- Blockchain based Transaction Data Storage

Blockchain technology produces a structure of data with inherent security qualities. It's based on principles of cryptography, decentralization and consensus, which ensure trust in transactions. In most blockchains or distributed ledger technologies (DLT), the data is structured into blocks and each block contains a transaction or bundle of transactions. Each new block connects to all the blocks before it in a cryptographic chain in such a way that it's nearly impossible to tamper with. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is true and correct.

VII .CONCLUSION

Biometric technology offers enhanced security while being convenient to use. It guarantees that information is accessed only by authorized persons. It is robust solution to meet the stringent requirements of restricted access for top secret information. When biometric technology goes main-stream, banks can use biometrics in every transaction requiring the authentication of identity. The system can implement face recognition system to online net banking application. Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking based security systems. The ID can be stolen; passwords can be forgotten or cracked but the physical characteristics of a person cannot be stolen or hacked. The Face Recognition with click point identification overcomes all the above. And also provide multi-person access control to provide access privileges to users with improved security. This provides real time alert system about unauthorized access and multi person access.It can extend the framework to implement an ATM security by utilizing the stability and reliability of fingerprint characteristics the individual can enhance the framework by incorporating ATM security features through fingerprint recognition and leveraging GSM MODEM. Additionally, the system also contains the original verifying methods which were inputting owner's password which is send by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use.

REFERENCES

[1] Habib Ullah Khan , Muhammad Zain Malik , Shah Nazir and Faheem Khan in “Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: `A Systematic Analysis”. July 2023.

[2] Garg, Yashika, And Kanika Sachdeva. "Artificial Intelligence In Indian Banking Sector: A Game Changer." DogoRangsang Research Journal, Vol-12 Issue-08 No. 05 August 2022.

[3] Jobair Hossain Faruk, Md, et al. "Malware Detection and Prevention using Artificial Intelligence Techniques." arXiv e-prints (2022): arXiv-2206.

[4] Priya, G. Jaculine, and S. Saradha. "Fraud detection and prevention using machine learning algorithms: a review." 2021 7th International Conference on Electrical Energy Systems (ICEES). IEEE, 2021.

[5] Kang, Dongwoo, Jaewook Jung, Hyoungshick Kim, Youngsook Lee, and Dongho Won. "Efficient and secure biometric-based user authenticated key agreement scheme with anonymity." Security and Communication Networks 2018 (2018).

[6] Xia, Zhihua, Chengsheng Yuan, Rui Lv, Xingming Sun, Neal N. Xiong, and Yun-Qing Shi. "A novel weber local binary descriptor for fingerprint liveness detection." IEEE Transactions on Systems, Man, and Cybernetics: Systems 50, no. 4 (2018): 1526- 1536.

[7] Ajish, S., and K. S. Anil Kumar. "Secure Mobile Internet Banking System Using QR Code and Biometric Authentication." In Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021, pp. 791-807. Singapore: Springer Nature Singapore, 2022.

[8] Shanmugapriyan, J., R. Parthasarathy, S. Sathish, and S. Prasanth. "Secure Electronic Transaction Using AADHAAR Based QR Code and Biometric Authentication." In 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), pp. 1-4. IEEE, 2022.

[9] Estrela, Priscila Morais Argôlo Bonfim, Robson de Oliveira Albuquerque, Dino Macedo Amaral, William Ferreira Giozza, and Rafael Timóteo de Sousa Júnior. "A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications." Sensors 21, no. 12 (2021): 4212. 62

[10] Muflih, ‘‘The link between corporate social responsibility and customer loyalty: Empirical evidence from the Islamic banking industry,’’ J. Retailing Consum. Services, vol. 61, Jul. 2021, Art. no. 102558

[11] A. Jan, M. Marimuthu, and M. P. B. M. M. Isa, ‘‘The nexus of sustainability practices and financial performance: From the perspective of Islamic banking,’’ J. Cleaner Prod., vol. 228, pp. 703–717, Aug. 2019.

[12] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, ‘‘Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation,’’ Cogent Econ. Finance, vol. 11, no. 1, Dec. 2023, Art. no. 2153412.

[13] S. M. Hussain, A. Wahid, M. A. Shah, A. Akhunzada, F. Khan, N. U. Amin, S. Arshad, and I. Ali, ‘‘Seven pillars to achieve energy efficiency in high-performance computing data centers,’’ in Recent Trends and Advances in Wireless and IoT-enabled Networks. London, U.K.: Springer, 2019, pp. 93–105.

[14] M. S. Al-kahtani, F. Khan, and W. Taekeun, ‘‘Application of Internet of Things and Sensor in healthcare,’’ Sensors, vol. 22, no. 15, p. 5738, Jul. 2022.

[15] Surekha, Nayak, et al. "Leveraging Blockchain Technology for Internet of Things powered Banking Sector." Blockchain based Internet of Things. Springer, Singapore, 2022. 181-207