ADVANCED TECHNIQUES FOR STRENGTHENING CROSS-MEDIA BIOMETRIC AUTHENTICATION

[1]Kohila R, [2]Brightlin B C, [3]Muralidharan P, [4]Livanthan S, [5]Nitheesh Kumar B

[1]Assistant Professor, Department of CSE(Cyber Security), Muthayammal Engineering College.

[2]Associate Professor, Department of CSE(Cyber Security), Muthayammal Engineering College.

[3,4,5]Student, Department of CSE(Cyber Security), Muthayammal Engineering College.

[1]kohilamca@gmail.com, [2]brightlinsamvel@gmail.com, [3]muralisuri551@gmail.com, [4]leelivanthan@gmail.com, [5]nitheeshkumarb988@gmail.com

ABSTRACT - The rapid growth of digital banking has intensified security threats such as phishing, identity theft, shoulder surfing, and unauthorized access. Traditional authentication methods using passwords, PINs, and OTPs are increasingly vulnerable due to their static nature. This paper proposes a secure multi-layer authentication framework integrating behavioral biometrics, Illusion PIN mechanisms, facial biometric recognition, and blockchain-based data security. Keystroke dynamics are used for behavioral authentication, while Illusion PIN protects against observation attacks. Facial recognition using the Grassmann algorithm ensures accurate user verification, and blockchain technology provides tamper-proof transaction storage, enhancing trust and security in digital banking systems. The proposed approach improves resistance to both cyber and physical attacks while maintaining user convenience. This framework offers a reliable solution for next-generation secure digital financial platforms.

KEYWORDS - Digital Banking Security, Multi-Layer Authentication, Keystroke Dynamics, Illusion PIN, Facial Recognition, Blockchain.

1. INTRODUCTION

Digital banking has revolutionized financial services by enabling fast, remote, and user-friendly access to banking operations. However, this convenience has introduced serious cybersecurity risks, including phishing, malware injection, credential theft, and identity fraud. Traditional authentication systems primarily rely on static credentials such as passwords and PINs, which can be easily compromised through observation or social engineering attacks.

Recent studies indicate that single-factor and two-factor authentication mechanisms are insufficient to counter advanced cyber threats. Even OTP-based authentication is vulnerable to interception via SIM swapping and malware-based attacks. These weaknesses highlight the urgent need for intelligent, adaptive, and multi-layer authentication systems.

Biometric authentication has emerged as a promising alternative due to its ability to verify users based on unique behavioral and physiological traits. However, unimodal biometric systems suffer from spoofing and performance degradation under varying conditions. Therefore, this paper proposes a cross-media multi-layer biometric authentication system.

1. SCOPE OF THIS PROJECT

This project aims to:

- The project focuses on designing a multi-layer biometric authentication framework to enhance security in net banking and online financial systems.

- It incorporates behavioral biometrics (keystroke dynamics) to continuously and invisibly verify users based on their unique typing patterns.

- The system implements an Illusion PIN mechanism to protect against shoulder-surfing, screen recording, and observational attacks during PIN entry.

- It utilizes facial biometric authentication using the Grassmann algorithm to ensure accurate user verification under varying lighting and pose conditions.

- The project integrates blockchain technology to securely store transaction data, ensuring immutability, transparency, and resistance to data tampering.

The framework is designed to enhance security in online banking systems by providing robust, multi-layer biometric authentication to prevent unauthorized access and financial fraud.

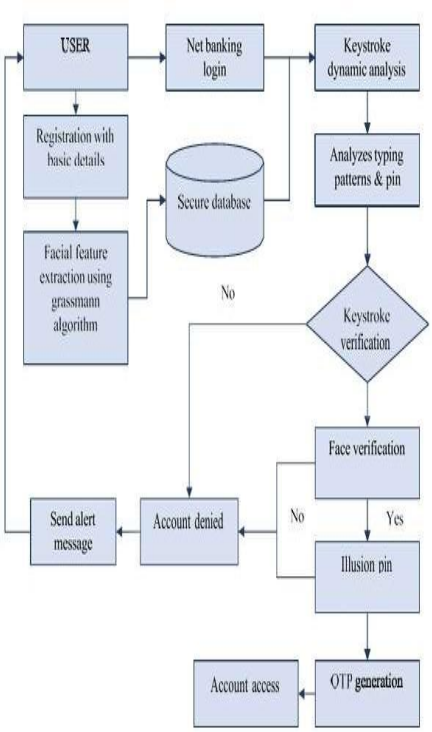
2. PROPOSED WORK

The proposed system introduces a robust multi-layer authentication framework designed to significantly enhance security in net banking applications. The first layer incorporates keystroke dynamics, a behavioral biometric technique that analyzes the user's typing rhythm while entering the PIN or password. This hidden verification step detects irregularities in typing behavior, preventing unauthorized users from proceeding even before they attempt the actual PIN.

To strengthen visual protection, the second layer integrates an Illusion PIN interface, which randomizes and disguises the PIN input pattern. This prevents attackers from identifying the correct PIN through shoulder-surfing, screen observation, or video recording, addressing one of the most common vulnerabilities in traditional systems.

Once the PIN is verified, the system performs real-time multi-biometric authentication using facial recognition based on the Grassmann algorithm. This algorithm accurately identifies the user even under variations in lighting, pose, or angle, ensuring that only the legitimate account holder gains access.

2.1 System Architecture



3.1 Data Processing & Preprocessing

User input data, including keystroke timing patterns and facial images, are collected and preprocessed to remove noise and inconsistencies

- **Data Collection:** User interaction data such as keystroke timings, PIN inputs, and facial images are securely collected during the authentication process.
- **Input Preprocessing:** Raw input data is filtered, noise is removed, and irrelevant variations are eliminated to improve data consistency.
- **Text Normalization:** Input text is normalized through case folding, removal of special characters, and standard formatting for uniform processing.
- **URL Preprocessing:** URLs are parsed and sanitized by removing redundant parameters and extracting relevant features to prevent malicious injections.
- **AI Model Interaction:** Preprocessed data is fed into trained AI models for behavioral and biometric analysis to perform accurate authentication.

3.2 MODULE DESCRIPTION:

3.2.1 Bank Interface Creation:

The Bank Interface Creation module provides a user-friendly and secure front-end platform for customers to interact with the net banking system. It includes the login screen, PIN input interface, and navigation menus required for performing banking operations.

3.2.2 User Registration Process:

The User Registration Process module is responsible for onboarding new users into the system securely. It collects essential user details such as name, account number, email, and mobile number.

3.3.3 User PIN Verification:

The User PIN Verification module ensures secure authentication by validating the user's PIN through multiple protective mechanisms. It first analyzes keystroke dynamics to verify the user's typing rhythm and detect anomalies before PIN entry

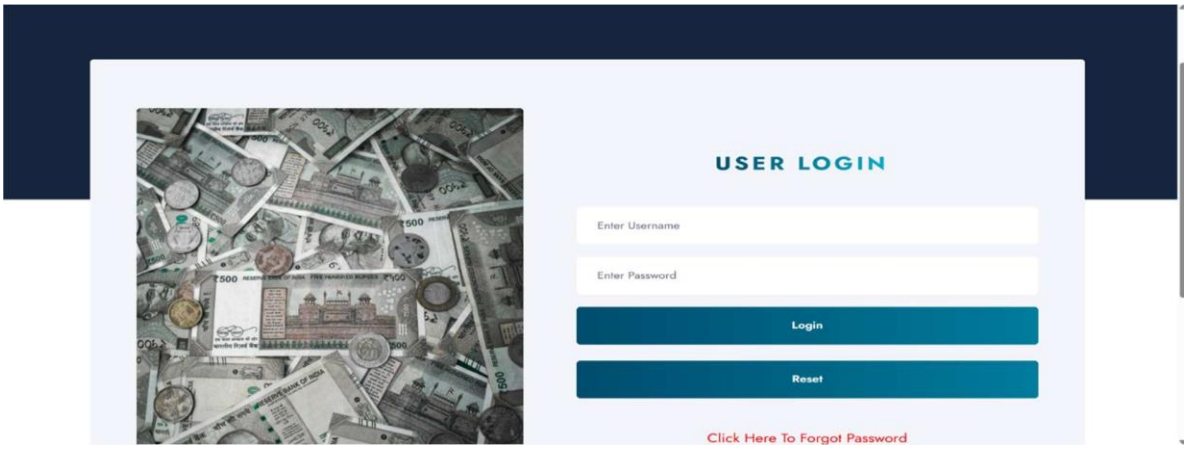
3.3 TOOLS AND LIBRARIES

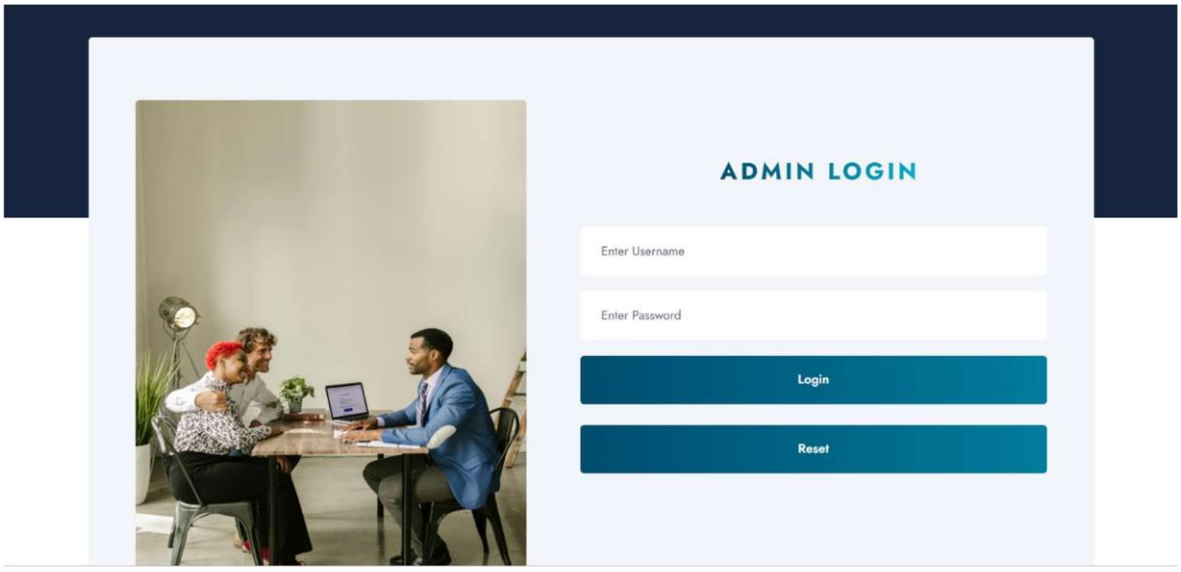
- **Python:** Python as the primary programming language due to its extensive support for cybersecurity, machine learning, and biometric processing.
- **MySQL:** integrated as the backend database for secure storage of user credentials and biometric data.
- **TensorFlow/Keras:** used for implementing deep learning-based facial recognition and liveness detection.
- **Libraries:** NumPy and Pandas are used for data handling and preprocessing of keystroke and biometric data

4. PROGRAM

```
from flask import Flask, render_template, flash, request, session
from flask import render_template, redirect, url_for, request
import sys, fsdk, math, ctypes, time
import mysql.connector

app = Flask(__name__)

app.config['DEBUG']
app.config['SECRET_KEY'] = 'san'


@app.route("/")
def homepage():
    return render_template('index.html')


@app.route("/AdminLogin")
def AdminLogin():
    return render_template('AdminLogin.html')


@app.route('/UserLogin', methods=['GET', 'POST'])
def UserLogin():
    return render_template('UserLogin.html')


@app.route("/NewUser")
def NewUser():
    return render_template('NewUser.html')


@app.route("/ForgotPassword")
def ForgotPassword():
    return render_template('ForgotPassword1.html')


@app.route("/AdminHome")
```

5. RESULTS AND OUTPUT





- **SQL Injection Scan Results:** SQL Injection (SQLi) scan results are essential for securing biometric databases by identifying vulnerabilities that allow malicious SQL queries through input forms or authentication requests.
- **XSS Scan Results:** Cross-Site Scripting (XSS) scan results identify whether malicious scripts can execute on biometric authentication webpages.
- **Anomaly Detection Reports:** Anomaly detection reports identify suspicious patterns indicating potential SQL injection or XSS attacks on biometric

6. CONCLUSION

The smart parking system presents a modern and efficient solution to the increasing challenges faced in urban mobility and parking management. By replacing traditional manual approaches with automation, real-time monitoring, and intelligent decision-making, the system significantly enhances user convenience and reduces operational inefficiencies. The integration of IoT devices, sensors, cloud computing, and machine learning ensures accurate detection of parking slot availability, minimizes human error, and improves overall resource utilization.

REFERENCES

1. Khan, Habib Ullah, et al. "Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis." IEEE Access (2023).
2. Karim, Nader Abdel, et al. "Online Banking User Authentication Methods: A Systematic Literature Review." IEEE Access (2023).
3. Darem, Abdulbasit A., et al. "Cyber threats classifications and countermeasures in banking and financial sector." IEEE Access 11 (2023): 125138-125158.
4. Sedik, Ahmed, et al. "Deep learning modalities for biometric alteration detection in 5G networks-based secure smart cities." IEEE Access 9 (2021): 94780-94788.
5. Hajiabbasi, Milad, Ehsan Akhtarkavan, and Babak Majidi. "Cyber-physical customer management for Internet of robotic things-enabled banking." IEEE Access 11 (2023): 34062-34079.
6. Parkinson, Simon, et al. "An empirical analysis of keystroke dynamics in passwords: A longitudinal study." IET Biometrics 12.1 (2023): 25-37.
7. Roy, Soumen, et al. "A systematic literature review on latest keystroke dynamics based models." IEEE Access 10 (2022): 92192-92236.
8. Abdrabou, Yasmeen, et al. "" Your Eyes Tell You Have Used This Password Before": Identifying Password Reuse from Gaze and Keystroke Dynamics." Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. 2022.