American Express Makeathon 2024

👨‍👩‍👧 Team name and member details

- Team Name: OPAL
- Member 1: Vaishnavi Maheshwari
- Member 2: Muskan Sachan
- Member 3: Riya Gupta
- Member 4: Tanaya Mohanty

📝 **Theme Name:** Data Security in FinTech

🚩 Problem statement

- We aim to devise a feasible solution to safeguard users' sensitive data within their FinTech profiles (eg., Internet Banking applications) by integrating advanced encryption, authentication, and access control which also adhere to the regulatory standards.
- Encryption encodes the stored data to avoid unauthorized access, while authentication ensures only verified systems and individuals have access to the data, and access controls regulate permissions.
- In addition to this, we also plan to incorporate monitoring and incident response capabilities.
- Monitoring systems will continually scout for suspicious activities, enabling real-time detection of potential breaches.
- Effective incident response **protocols ensure swift action** in the event of a security incident, minimizing the impact on user data and privacy.
- Overall, the goal is to develop a comprehensive solution to avoid any data security mishap while also complying with regulations and maintaining customer trust.

Solution

We aim to provide internet banking services in the most user-friendly manner, while also upholding all the principles of data security and integrity. The methods mentioned earlier, involving the integration of encryption, authentication, and access control coupled with monitoring tools and security frameworks will help us achieve the safety for sensitive data, and identify any breach or cyber attack.
The data security architecture for our FinTech application helps to solve several critical problems and address the key challenges in safeguarding sensitive user data by implementing the following solutions -

- **User Authentication**: Apart from normal username and password We'll Integrate OAuth 2.0 and OpenID Connect for user authentication. so that multi-factor authentication can be implemented, where user will have to speak displayed characters on screen and then it will be cross-checked, to make sure any robot or software is not trying to access the banking website.

```
$("#predict-button").click(function() {
          let message = { image: base64Image };
          $.post("http://127.0.0.1:5000/predict", message, function(response) {
              $("#authentication").text("Results: " + response[0].label + " ( Confidence: " + response[0].authenticate.toFixed(2) + ")");
          });
      });
      try:
      for (() = {
          img_data = request.form['image']
          img_data = base64.b64decode(img_data)

          # Convert the image data to a NumPy array
          img_array = image.img_to_array(image.load_img(io.BytesIO(img_data), target_size=(224, 224)))

         # Get model authentication
          predictions = model.predict(img_array)
          decoded_predictions = decode_authneticate(auth, top=3)[0]

          # Return authentication as JSON
          result = [{'label': label, 'auth': float(prob)} for (_, label, prob) in decoded_predictions]
          return jsonify(result)

      except Exception as e:
          print("Error:", str(e))
          return jsonify(error=str(e)), 500
      })
```

💡 Solution

- **Data Encryption**- To utilize AES-256 encryption for data transmission and storage, coupled with the PBKDF2 (Password-Based Key Derivation Function 2) algorithm for secure key derivation and management.
  The application will integrate the encryption library's API such as OpenSSL into its codebase, allowing interaction with the AES-256 encryption functionality. This will involve wrapping the library's AES-256 encryption and decryption functions into the application's own data handling and storage processes. The application will pass the data to be encrypted/decrypted, along with the appropriate encryption keys, to the library's API calls.
- **Data Encryption Lifecycle** - For data at rest (e.g., database, file storage), the application will encrypt the sensitive information before storing it, using the AES-256 algorithm in GCM mode.
  For data in transit (e.g., API requests, service-to-service communication), the application will establish secure communication channels that leverage the AES-256 encryption.
- **Security Monitoring**- Our application will implement a comprehensive security monitoring infrastructure, using Splunk Enterprise SIEM for real-time event analysis and Zeek NSM for in-depth network traffic monitoring. Additionally, the application will establish incident response workflows based on the NIST Cybersecurity Framework to ensure a structured and efficient approach to detecting security incidents.
- **Access Control**- Implement role-based access control (RBAC) using the open-source Keycloak identity and access management solution. Explore attribute-based access control (ABAC) using the eXtensible Access Control Markup Language (XACML) standard and enforce the principle of least privilege for user permissions and data access.

💡 Solution

We can consider the following impact metrics which are feasible to analyze the impact and effectiveness of the data security architecture. These impact metrics focus on measurable outcomes that can be realistically achieved and demonstrated within the constraints of a hackathon event -

- Encryption Overhead -
  - Measure CPU utilization and processing time during encryption.
  - To Showcase a comparison of system resource utilization before and after encryption implementation to demonstrate the efficiency gains achieved.
- Data Transmission Time -
  - Evaluate the impact of encryption on data transmission time over various network conditions.
  - To provide a comparison of data transfer speeds before and after encryption to highlight the impact on transmission time.
- Security Audit Findings -
  - Conduct vulnerability scanning and penetration testing to identify weaknesses in the encryption implementation.
- User Experience Impact -
  - Gather user feedback to assess the impact of encryption on application responsiveness and user experience.
  - Present user feedback and metrics that showcase the impact of encryption on user experience.
- Vulnerability Reduction -
  - Number of security vulnerabilities identified and remediated through assessments conducted.
  - Percentage decrease in the overall security risk profile of the application compared to a pre-defined baseline.

Solution

Key Technical Details and reason behind choosing a techstack

Encryption - AES-256 in GCM mode derived using PBKDF2-HMAC-SHA256.

- AES-256, with 256-bit keys, provides an exceptional level of data protection, meeting the stringent security requirements of the financial industry.
- The GCM (Galois/Counter Mode) block cipher mode of operation further enhances the encryption's confidentiality and authenticity

Authentication - OAuth 2.0 Authorization Code Grant flow with OIDC for user identity verification

- OAuth 2.0 is the industry-standard protocol for authorization, allowing users to grant limited access to their resources without sharing their credentials.
- OpenID Connect is an identity layer on top of OAuth 2.0, providing user authentication and profile information in addition to authorization.

MFA - TOTP-based one-time passwords, integrated with FIDO2 biometric authentication.

- multi-factor authentication (MFA) using TOTP-based one-time passwords and FIDO2 biometric authentication, such as fingerprint or facial recognition. This MFA solution provides an additional layer of user verification beyond just credentials, significantly enhancing the overall security

SIEM - Splunk Enterprise with custom dashboards and alerts for security incident detection

Network Monitoring - Zeek for deep packet inspection, anomaly detection, and threat hunting

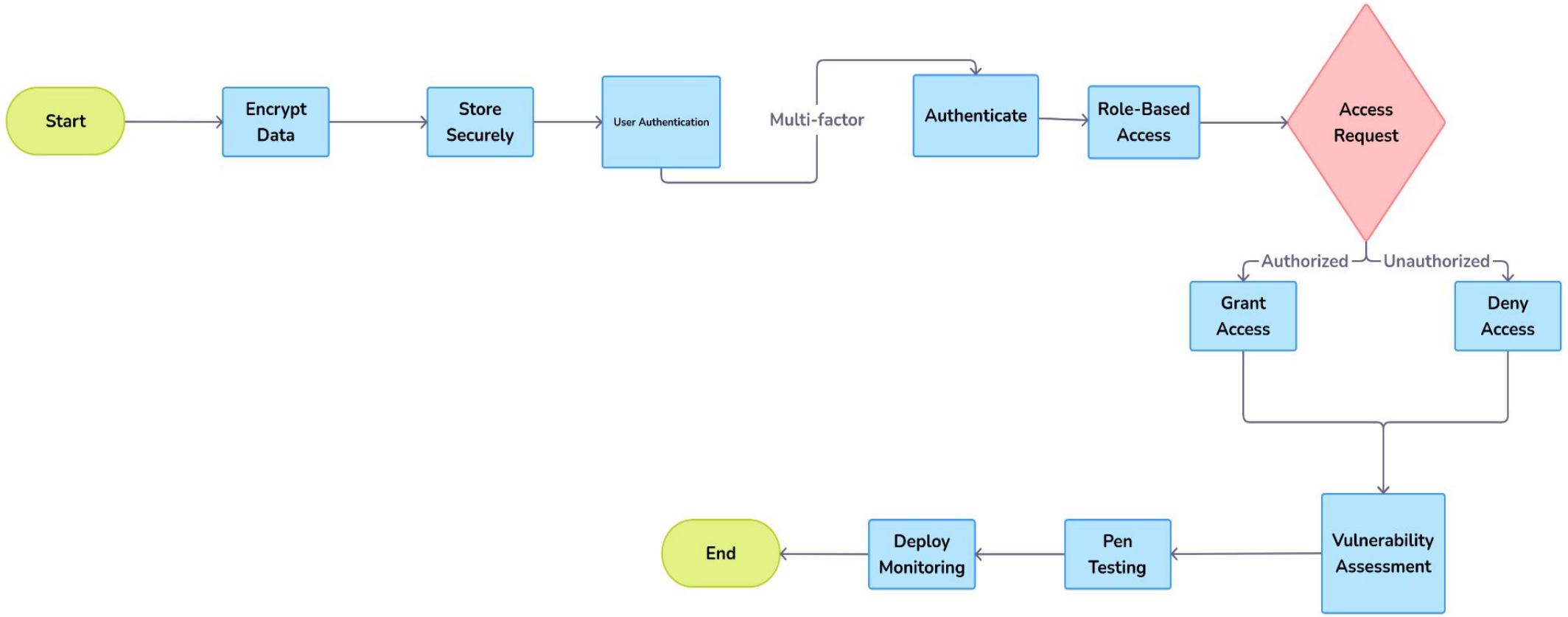
- The SIEM functionality provided by Splunk enables the FinTech application to centralize the collection, monitoring, and investigation of security-related events from various sources.

Access Control - Keycloak RBAC with fine-grained ABAC policies defined in XACML.

- Keycloak is an identity and access management solution that supports RBAC (Role-Based Access Control) and ABAC (Attribute-Based Access Control) models. Being open-source it is more available for reference and well documented.
- Integrating Keycloak allows the FinTech application to implement fine-grained access control policies, ensuring that users can only access the data and resources they are authorized to.

📊 Methodology / Architecture diagram

Here is the high-level approach of implementation of the solution with the help of flowchart. and architectural diagram



Backend Layer

User

API Gateway

Encryption

1) Encryption Library Integration
-Integrate encryption library, such as OpenSSL to utilize the optimized AES-256 implementation.

2) Key Management Workflows - When a user provides a password or passphrase for authentication, the key management service will apply the PBKDF2-HMAC-SHA256 algorithm to derive an encryption key.

3) Data Encryption Lifecycle -
For data at rest eg. database file storage)
(AES-256 algorithm in GCM mode)
For data in transit e.g., API requests, service-to-service communication (AES-256 encryption)

Authentication and Access control

User Authentication using MFA- Integrate OAuth 2.0 and OpenID Connect for user authentication. When a user attempts to log in, the IAM system will prompt them to provide their primary authentication factor.
The TOTP algorithm uses a shared secret (the TOTP secret key) and the current time to generate a one-time code.

Implementing Biometric Factors -
During the user's registration or account setup process, prompt them to provide their biometric data (e.g., fingerprint, facial scan).
Securely store the biometric credentials in the IAM platform's user profile or a dedicated biometric credential store.

Access Control - Keycloak identity and access management solution
Defining Roles and Permissions.
Assigning Roles to Users.
Enforcing RBAC in Applications.
Attribute-Based Access Control (ABAC) using XACML

Monitoring Tool

Splunk Enterprise (SIEM) Implementation - Configuration of data inputs to collect and index security-relevant logs from network devices, servers, and applications. Creation of custom dashboards and alerts for real-time security monitoring and threat detection.

Zeek as the NSM Tool - Configuration of Zeek scripts to extract metadata, detect anomalies, and generate network traffic logs.
Integration of Zeek with threat intelligence platforms to enrich network security monitoring with external threat feeds.

Vulnerability assessments and penetration testing - Implement regular vulnerability scanning using tools like Nessus, OpenVAS, or Qualys to identify known vulnerabilities in the FinTech application, underlying systems, and infrastructure.

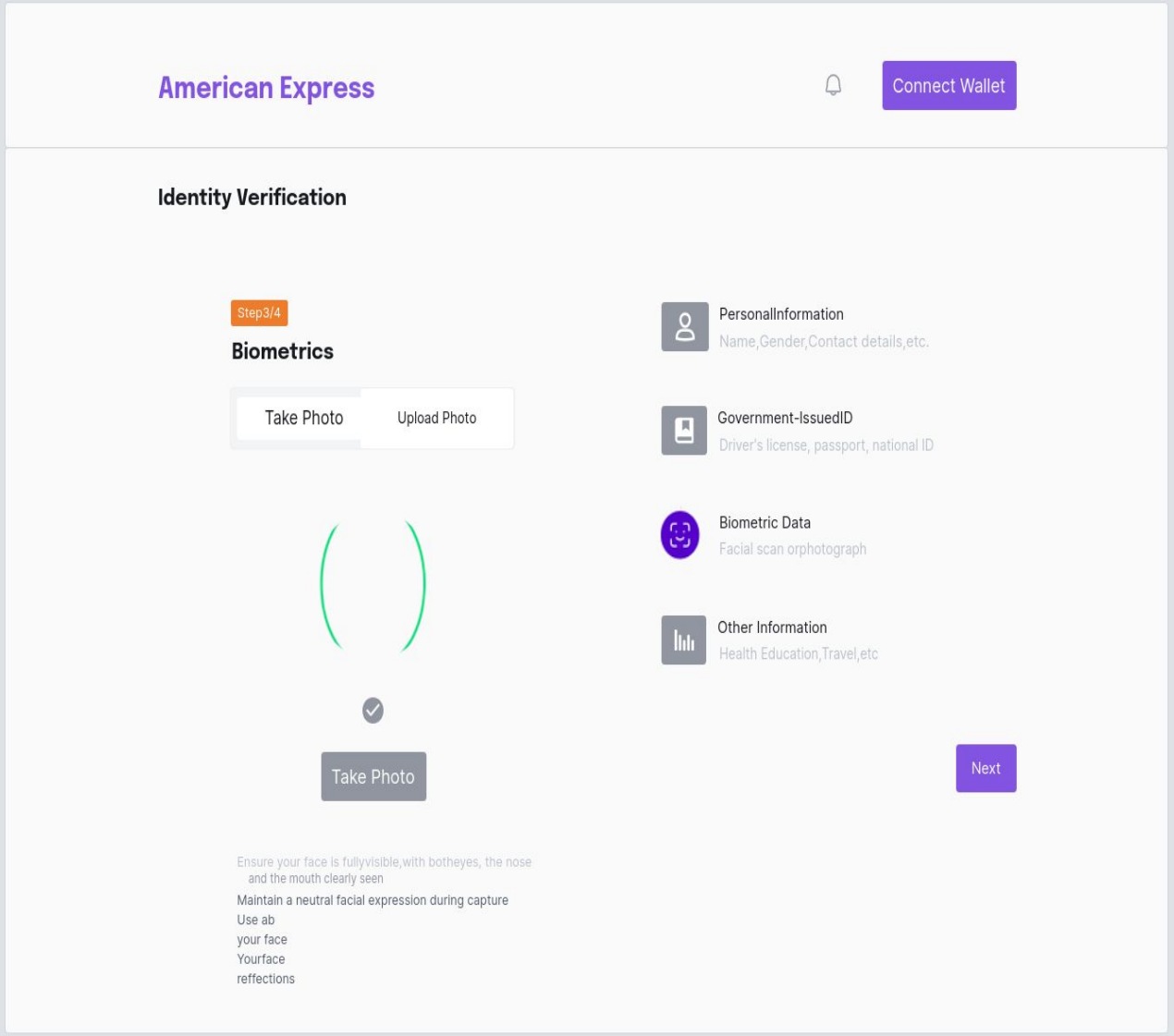
Develop a structured penetration testing strategy for the FinTech application, including the scope, frequency, and testing methodology (e.g., OWASP WSTG, PTES, NIST SP 800-115)

Incident responses - The security monitoring tools, such as the SIEM (Security Information and Event Management) system and the NSM (Network Security Monitoring) solution, would continuously monitor for suspicious activities, security alerts, and potential data breaches.
When the monitoring tools detect a security incident or anomaly, they would generate alerts and provide detailed information about the event, including the source, nature of the threat, and potential impact.

📊 Methodology / Architecture diagram

As we explored the possibilities of implementing the solution, we started with implementing the authentication protocols. On the right side, Multi Level Authentication and Biometric Auth can be seen. We successfully completed the interface and other details required for the user and currently working on integrating the Oauth and openID backend with the given frontend interface.

Implementation of the authentication ML model can be seen in this github link - Link



🚀 Future Scope

1. **Business Relevance:**
   - Addresses the critical need for data security in fintech.
   - Enhances regulatory compliance and customer trust.
2. **Optimization:**
   - Continuous improvement for better security.
   - Efficiency enhancements and scalability.
3. **Scope for Modification:**
   - Customization for different fintech use cases.
   - Integration with emerging technologies.

🎯 Impact / Novelty

1. Enhanced data security, reducing risks of breaches.
2. Compliance with regulations, mitigating legal risks.
3. Improved customer trust and loyalty.
4. Reduced financial risks from potential data loss.
5. Increased growth opportunities through positive reputation.

Thank You