ADR-001: Data Security and Privacy

Context

FinanceHero, as a responsible aggregator of sensitive financial data, and is committed to protecting user privacy and ensuring data security. This ADR outlines our approach to safeguarding user information.

Decision

To protect the user data, we will be implementing the following measures:

- **Encryption**: Using industry standard protocols like AES-256, all data must be encrypted at rest and in transit.
- **Authentication**: Implement robust user authentication protocols like OAuth-based multi-factor authentication (MFA) for secure logins.
- **Security Audits**: Penetration testing and regular security audits will be conducted periodically to identify and address potential vulnerabilities.
- **Compliance**: Adhere to data privacy regulations like CCPA or CPRA to protect user data.

Rationale

User trust is crucial for FinanceHero's success. Robust security measures:

- **Enhance trust**: User confidence is built by prioritizing data security.
- **Minimize risks**: Encryption safeguards data from unauthorized access in case of breaches.
- **Avoid compliance issues**: Adherence to regulations prevents fines and reputational damage.

Consequences

- **Positive**: User trust increases, regulatory compliance is achieved, and data breaches are mitigated.
- **Negative**: Implementing and maintaining security measures requires ongoing investment.

Status

Accepted

References

- https://en.wikipedia.org/wiki/California_Privacy_Rights_Act
- https://auth0.com/docs/secure/multi-factor-authentication/authenticate-using-ropg-flow-with-mfa

ADR-002: Machine Learning and Artificial Intelligence for Personalized Finance

Context

FinanceHero aims to personalize the user experience by analyzing financial data and providing tailored recommendations. This ADR outlines the approach to leverage Machine Learning (ML) and Artificial Intelligence (AI) for this purpose.

Decision

We will integrate ML and AI models to power the Personal Finance Assistant (PFA) and offer personalized financial insights. This include:

- **Specialized Learning Models**: Utilizes supervised learning models for:
  - Expenses categorization to automatically categorize transactions.
  - Transaction prediction to forecast future income and expenses.
  - Goal setting to suggest achievable financial goals based on user data.
- **Natural Language Processing(NLP)**: Implement NLP to:
  - Understand user queries in natural language for interation with PFA.
  - Generate coversational responses from the PFA for a more engaging experience.

Rationale

ML and AI offers:

- **Personalized Insights**: Analyze user data to provide recommendations on spending habits, budgeting strategies, and investiment opportunities
- **Predictive Capabilities**: Predict future financial trends to help users make informed decisions.
- **Enhanced User Experience**: Enable natural language interaction through PFA, making financial management more accessible.

Consequences

- **Positive**: Personalized recommendations, improved financial literacy, increased user engagement.
- **Negative**: Requires ongoing investment in data science expertise and model development. Potential for biases in model output if training data is skewed.

Status

Accepted

References

- Scikit-learn (Machine Learning library): https://scikit-learn.org/stable/
- TensorFlow (Machine Learning framework): https://www.tensorflow.org/

ADR-003: Cloud-Based Receipt Storage with Security Considerations

Context

FinanceHero aims to offer a receipt tracking feature where users can store receipts securely. This ADR explores leveraging existing cloud storage platforms (e.g., Google Drive, Dropbox, iCloud) for receipt storage while considering security implications.

Decision

We will not directly store receipts within the FinanceHero application. Instead, we will integrate with existing cloud storage platforms to allow users to:

- **Link Cloud Storage Accounts**: Users can securely connect their preferred cloud storage provider (e.g., Google Drive, Dropbox, iCloud) to FinanceHero.
- **Upload Receipts**: Users can upload receipt images or PDFs directly from their devices or linked cloud storage accounts.
- **Access and Manage Receipts**: FinanceHero will provide functionalities to view, search, and organize receipts stored within the linked cloud storage platform.

Rationale

Leveraging existing cloud storage offers several advantages:

- **Security**: Cloud storage providers typically employ robust security measures like encryption and access controls,mitigating the risk of data breaches within the FinanceHero app itself.
- **User Choice and Familiarity**: Users can choose their preferred cloud storage platform, leveraging existing security settings and access controls they're already familiar with.
-
  - **Reduced Storage Burden**: FinanceHero avoids the burden of managing user data storage and associated costs.

Security Considerations

While leveraging cloud storage offers benefits, security concerns need to be addressed:

- **User Responsibility**: Users are responsible for maintaining storage security practices within their chosen cloud storage platform(e.g., enabling two-factor authentication, using strong passwords).
- **Data Access**: FinanceHero will only access receipt metadata (filenames, timestamps) for organization purposes, not the actual receipt content.
- **Data Visibility**: Users should be aware that cloud storage providers may have access to stored data depending on their terms of service.

Consequences

- **Positive**: Leverages existing security infrastructure of cloud storage providers, reduces storage burden for FinanceHero, and offers user choice.
- **Negative**: Relies on user practices for cloud storage security, limited control over actual receipt content storage by FinanceHero.

Status

Proposed

Next Steps

- Conduct a security risk assessment of this approach, considering user data privacy and potential access by cloud storage providers.
- Explore potential API integrations with specific cloud storage platforms for seamless user experience.
- Develop clear communication to users regarding data storage practices and security considerations.

ADR-004: Open API Integration

Context

FinanceHero needs to connect with various financial institutions and platforms to seamlessly aggregate user data. This ADR outlines the approach to facilitate secure data exchange.

Decision

We will develop open APIs to enable secure data aggregation from various financial institutions and platforms. This includes:

- **Standardized API protocols**: Adhere to standardized API protocol like Open Banking APIs or Plaid to ensure compatibility.
- **Secure Authentication**: Implement secure authentication mechanism(e.g. OAuth) for data access authorization.
- **Partnerships**: Explore partnerships with financial institution for seamless data exchange and potential co-branding opportunities.

Rationale

Open APIs offer:

- **Ease of Integration**: Standardized protocols facilitate integration with a wide range of financial institutions.
- **Security**: Secure Authentication mechanism safeguard userdata during data exchange.
- **Enhanced User Experience**: Seamless data aggregation provides a holistic view of user finances.

Partnership with financial institutions:

- **Expand User Base**: Leverage partner network to reach a wider audience
- **Increase data Availability**: Gain access to additional financial data sources.
- **Potential Revenue Streams**: Explore co-branding and referral opportunities with partners.

Consequences

- **Positive**: Improved user experience, richer data insights. potential for additional revenue streams.
- **Negative**: Reliance on third-party APIs for data accessibility, potential integration challenges with specific institutions.

Status

Accepted

References

- https://plaid.com/resources/open-finance/open-banking-api/

ADR-005: Scalable and Cloud-based Infrastructure

Context

FinanceHero needs to handle a growing user base and vast amounts of data. This ADR outlines the approach to ensure a scalable and reliable infrastructure.

Decision

We will leverage a scalable cloud-based infrastructure to accommodate user growth and data storage demands. This includes:

- **Cloud Platform**:Utilize a reputable cloud platform like AWS, Azure, or Google Cloud Platform (GCP) for scalability and flexibility.
- **Microservices Architecture**: Implement a microservices architecture to allow for independent development, deployment, and scaling of functionalities.
- **Auto-Scaling**: Employ auto-scaling capabilities to handle fluctuations in user traffic and optimize resource utilization.

Rationale

A cloud-based infrastructure offers:

- **Scalability**: Effortlessly scale resources (storage, compute) to meet user demands.
- **Elasticity**: Pay only for the resources used, maximizing cost-efficiency.
- **Reliability**: Cloud platforms provide high availability and disaster recovery mechanisms.

Microservices architecture enables:

- **Modularity**: Independent development and deployment of feature simplifies update and maintenance.
- **Flexibility**: Individual services can be scaled independently based on usage and patterns.

Consequences

- **Positive**: Improved performance, scalability, and cost-efficiency.
- **Negative**: Reliance on third-party cloud provider introduces vendor lock-in and potential security concerns.

Status

Accepted

References

- https://www.cs.drexel.edu/~bsm23/pubs/CNSE-Preprint.pdf