**System Design Report (SDR) for Data Breach Avoidance System**

**Document Revision:** 1.0  
**Date:** [Date]

**1. Introduction**

This SDR provides a comprehensive design overview for the Data Breach Avoidance System tailored for the MyBankCardsManager application. It details the architecture, components, data flow, and other essential elements to facilitate system development.

**2. System Architecture**

**2.1 High-Level Architecture**

* **Front-end Layer:** Handles user interaction and displays data to the user. Built using frameworks like React or Angular.
* **Application Layer:** Contains the business logic and the core functionalities of the system. Developed using Flask.
* **Database Layer:** Consists of the primary database and a sacrificial (honeypot) database. Implemented using MS Azure SQL Server.
* **Security Layer:** Incorporates the Adaptive Honeypot Behavior Algorithm, Intrusion Detection System, and User Entity Behavior Analytics.

**3. Component Design**

**3.1 Adaptive Honeypot Behavior Algorithm Component**

* **Honeypot Data Generator:** Generates and regenerates honeypot data.
* **Intrusion Logger:** Records intrusion attempts with timestamps.
* **Intrusion Analyzer:** Processes recorded data to identify intrusion patterns and adapt honeypot behavior.

**3.2 Intrusion Detection System Component**

* **Signature Detector:** Uses pre-defined signatures to detect unauthorized activities.
* **Anomaly Detector:** Uses machine learning to identify unusual patterns, suggesting potential threats.

**3.3 User Entity Behavior Analytics Component**

* **Behavior Database:** Stores known behaviors for system users.
* **Behavior Analyzer:** Processes user actions to match against the database and identify anomalies.

**3.4 BankCardManager Application Component**

* **User Interface:** Provides entry points and interactions for users.
* **Database Manager:** Interacts with the primary and honeypot databases for CRUD operations.
* **Email Alert System:** Sends notifications in case of suspicious activities.

**4. Data Flow Design**

1. The user accesses the BankCardManager application via the front-end interface.
2. User input is processed and sent to the application layer for authentication.
3. The behavior is analyzed using the User Entity Behavior Analytics component.
4. If behavior is suspicious, the Intrusion Detection System is triggered.
5. Depending on the results, the user might be redirected to genuine or honeypot data.
6. All interactions are logged and analyzed for continuous system adaptation.

**5. Database Design**

* **Original Database:** Stores genuine data, encrypted for security.
* **Honeypot Database:** Contains sacrificial data to distract attackers.

**6. Security Measures**

* **Encryption:** All sensitive data, including passwords, are encrypted using industry-standard methods.
* **Firewalls:** Deployed to prevent unauthorized external access.
* **Continuous Monitoring:** The system is monitored in real-time for potential threats.

**7. Scalability and Load Balancing**

* **Cloud Integration:** With MS Azure SQL Server, the system can scale based on demand.
* **Load Balancers:** These distribute incoming application traffic across multiple targets, ensuring high availability and fault tolerance.

**8. Backup and Recovery**

* **Backup Schedules:** Regular backups of the database are taken daily, weekly, and monthly.
* **Data Recovery:** A mechanism is in place to restore data in case of failures, ensuring data integrity and availability.

**9. Conclusion**

The System Design Report provides a blueprint for the development and deployment of the Data Breach Avoidance System. Proper implementation of this design will ensure an efficient and robust system that prioritizes user data security.