**Data Breach Avoidance System: A Proactive Security Measure Based on the Honeypot Strategy**

**Abstract:**

Data breaches have become one of the most pressing concerns for businesses and individuals in the digital age. With the continuous advancement of cyber-attack techniques, traditional security measures often fall short. This calls for a proactive approach to data protection. One such method that has gained traction is the honeypot strategy, which serves as a decoy to attract and detect cyber threats. The proposed Data Breach Avoidance System leverages the Honeypot Strategy to provide a proactive cybersecurity framework specifically designed for the MyBankCardsManager app. By deploying a sacrificial database alongside the original one, the system distracts would-be attackers, effectively monitoring and mitigating cyber threats. The architecture is built on MS Azure SQL Server and employs machine learning algorithms, Intrusion Detection Systems (IDS), and User and Entity Behavior Analytics (UEBA) to offer a robust security solution.

**Algorithms**

* **Adaptive Honeypot Behavior Algorithm**: Utilizes machine learning techniques to adapt and improve the honeypot’s effectiveness over time.
* **Intrusion Detection System (IDS)**: Employs either signature-based or anomaly-based detection methods to identify unauthorized activities.
* **User and Entity Behavior Analytics (UEBA)**: Identifies unusual patterns in user behavior, which could be indicative of a security breach.

**Tech Stack**

* **Backend Development**: Python
* **Database**: MS Azure SQL Server
* **Machine Learning**: TensorFlow or PyTorch
* **Web Application & API**: Flask
* **Frontend Development**: React or Angular
* **Version Control**: Git

**Existing System**

* **Centralized Database**: The MyBankCardsManager app relies on a centralized database for storing sensitive information.
* **Basic Security Measures**: Likely uses traditional firewalls and encryption but lacks proactive threat detection.
* **Manual Monitoring**: Mostly reliant on manual monitoring and auditing of the system for security breaches.
* **Static Defenses**: Utilizes static security measures that don’t adapt to emerging threats.

**Proposed System**

* **Sacrificial Database (Honeypot)**: Deploys a honeypot database alongside the original database to distract potential attackers.
* **Adaptive Algorithms**: Implements machine learning algorithms to improve honeypot functionality and adapt to new types of attacks.
* **Advanced Threat Detection**: Integrates Intrusion Detection Systems (IDS) and User and Entity Behavior Analytics (UEBA) for a multi-layered security approach.
* **Cloud-based Architecture**: Utilizes MS Azure SQL Server for a scalable and secure database solution.
* **User-Friendly Interface**: Incorporates a web application front end to enhance user experience without compromising on security.
* **Collaborative Development**: Utilizes Git for version control and to facilitate effective team collaboration.