**Review 2: Data Breach Avoidance System for MyBankCardsManager App**

1. NEED FOR THE STUDY

The necessity of this study arises from the increasing prevalence and sophistication of cyber threats, particularly against financial applications like MyBankCardsManager. With the growing reliance on digital banking, the security of such apps is paramount. This study is undertaken to develop a proactive cybersecurity solution that not only defends against data breaches but also adapts to evolving cyber threats.

2. OBJECTIVES

**2.1 PRIMARY OBJECTIVE**

The primary objective of this study is to design and implement the Data Breach Avoidance System, a comprehensive cybersecurity framework for the MyBankCardsManager app. This system aims to enhance data security through a multi-faceted approach, including a honeypot strategy, advanced threat detection, and adaptive learning algorithms. The objective may evolve to include finer aspects of cybersecurity based on initial findings and technological advancements.

**2.2 SECONDARY OBJECTIVES**

* **Honeypot Implementation**: To successfully deploy and integrate a sacrificial database alongside the primary database.
* **Algorithm Optimization**: To utilize machine learning for improving the honeypot's effectiveness and adaptability over time.
* **Threat Detection and Analysis**: To implement and refine Intrusion Detection Systems (IDS) and User and Entity Behavior Analytics (UEBA).
* **User Experience**: To ensure that security enhancements do not compromise the app's usability and performance.

3. METHODOLOGY

The methodology includes:

* **Data Requirement**: Identification of necessary data types, such as intrusion attempts, user behavior patterns, and system logs.
* **Research Instruments**: Development of algorithms and deployment of IDS and UEBA tools.
* **Sampling Framework**: Utilizing real-time data from the MyBankCardsManager app for analysis and simulation.
* **Sample Size**: Comprehensive inclusion of all relevant data within the app's operational scope.
* **Hypothesis Testing**: Testing hypotheses related to the effectiveness of the honeypot strategy and adaptive algorithms.
* **Analysis Tools**: Utilization of statistical and machine learning tools for data analysis.

4. DATA COLLECTED

Data collection will encompass both primary and secondary data:

* **Primary Data**: Real-time monitoring data, user access logs, and honeypot interaction records.
* **Secondary Data**: Historical breach reports, cybersecurity research findings, and existing security protocol assessments.
* **Documentation**: Maintenance of filled questionnaires, system logs, and algorithm performance records in both hard and soft copies.

5. DATA ANALYSIS

Data analysis involves:

* **Statistical Testing**: Employing statistical methods to analyze user behavior and intrusion patterns.
* **Machine Learning Analysis**: Using TensorFlow or PyTorch for pattern recognition and predictive modeling.
* **Hypothesis Testing**: Evaluating the effectiveness of the honeypot system and the adaptive behavior of the IDS and UEBA.
* **Results Interpretation**: Correlating the findings with the objectives to assess the success of the implemented strategies.

6. WORK TO BE DONE

The remaining work includes:

* **System Refinement**: Fine-tuning the algorithms and security measures based on initial data analysis.
* **Extended Data Collection**: Expanding the data pool to include more varied scenarios and threat models.
* **Advanced Analysis**: Implementing deeper machine learning and statistical techniques for more nuanced insights.
* **Integration and Testing**: Fully integrating the system with MyBankCardsManager and conducting extensive testing.
* **Final Review and Documentation**: Preparing comprehensive reports and documentation for the final review and viva-voce presentations.