**Project designed phase – 1**

**Proposed Solution Template**

| | |
|---|---|
| Date | 2 September 2023 |
| Team Id | Team-591938 |
| Project Name | Online Payment Fraud detection |
| Maximum marks | 5 Marks |

**Proposed solution template:**

| S No. | Parameters | Description |
|---|---|---|
| **1.** | Problem statement(problem to be solved) | **The growth in internet and e-commerce appears to involve the use of online credit/debit card transactions. The increase in the use of credit / debit cards is causing an increase in fraud. The frauds can be detected through various approaches, yet they lag in their accuracy and its own specific drawbacks. If there are any changes in the conduct of the transaction, the frauds are predicted and taken for further process. Due to large amount of data credit / debit card fraud detection problem is rectified by the proposed method**<br>**We will be using classification algorithms such as Decision tree, Random forest, svm, and Extra tree classifier, xgboost Classifier.We will train and test the data with these algorithms. From this the best model is selected and saved in pkl format. We will be doing flask integration and IBM deployment.** |
| **2.** | Idea/ Solution description | **To address the rising credit/debit card fraud in the growing e-commerce sector, we propose a fraud detection system using classification algorithms like Decision Trees, Random Forest, SVM, Extra Tree, and XGBoost. By training and testing these models, we select the best-performing one, save it in .pkl format, and integrate it into a Flask-based web application. This application will be deployed on the IBM cloud, providing a practical and secure solution for real-time fraud detection in online transactions.** |
| **3.** | Novality/Uniqueness | **The novelty and uniqueness of the upper model lie in its comprehensive approach to tackling credit/debit card fraud in the context of e-commerce. It leverages a combination of well-established classification algorithms for fraud detection, specifically Decision Trees, Random** |

| | | |
|---|---|---|
| | | **Forest, SVM, Extra Tree, and XGBoost, allowing for a diverse and robust analysis of transaction data. The model selection process ensures that the best-performing algorithm is chosen for optimal accuracy. Additionally, the integration with Flask and deployment on the IBM cloud streamlines real-time fraud detection, providing a practical and secure solution for the ever-evolving e-commerce landscape.** |
| **4.** | Social Impact/ customer Saticfaction | **The upper model for credit/debit card fraud detection in e-commerce significantly enhances social impact by reducing financial losses, improving trust, lowering cybercrime rates, and promoting regulatory compliance. Simultaneously, it enhances customer satisfaction by offering heightened security, transaction convenience, fewer false positives, and peace of mind, ultimately creating a safer and more user-friendly environment for online transactions while positively impacting the broader financial ecosystem.** |
| **5.** | Business Model (Revenue model) | **The business model for the upper case of credit/debit card fraud detection in e-commerce primarily revolves around a subscription-based revenue model. E-commerce businesses and financial institutions can subscribe to the fraud detection service, paying a recurring fee based on the volume of transactions and the level of service required. Additionally, revenue can be generated through customized consulting services for optimizing fraud detection algorithms and system integration. The deployment on the IBM cloud platform could also involve pay-as-you-go pricing, further tailoring the revenue model to the specific needs and scale of the clients. This model ensures a steady stream of income while offering flexibility to cater to the diverse needs of businesses in the e-commerce sector.** |
| **6.** | Scalability of the Solution | **The upper case solution for credit/debit card fraud detection in e-commerce is highly scalable. It can handle growing data volumes and transaction rates by leveraging cloud-based deployment on the IBM cloud platform, which offers resources that can be easily scaled** |

| | | |
|---|---|---|
| | | **up or down to meet demand. The multi-algorithm approach, dynamic model selection, and real-time fraud detection also ensure that the system can adapt to evolving fraud patterns and increasing transaction loads. This scalability is vital for accommodating the rapid growth in e-commerce and online transactions, making it a robust and future-proof solution for addressing credit/debit card fraud.** |