SC-402 - Introduction to Cryptography

Credit Card Fraud Detection Using Homomorphic Encryption in ML

Student ID	Name
202001267	Bhatt Meet Dhavalbhai
202003006	Vraj Chaudhari
202003019	Jay Patel
202003031	Shreyansh Kunjera

INDEX

1. Introduction:

1.1 Purpose:

- The purpose of privacy-preserving credit card fraud detection using homomorphic encryption is to provide a secure and effective way for financial institutions to detect fraudulent transactions while preserving the privacy of customer data.

- Every year, millions of people are victimised by credit card fraud. Individuals and financial organisations can suffer considerable financial losses as a result of fraudulent transactions. Detecting fraudulent transactions, on the other hand, frequently necessitates the analysis of sensitive client data, such as transaction history and personal information, which might jeopardise privacy and security.

- Homomorphic encryption solves this problem by enabling mathematical operations on encrypted material without the need to decode it. Financial organisations may now analyse transaction data without disclosing sensitive client information. Financial institutions can detect fraudulent transactions and avert financial losses by deploying a privacy-preserving credit card fraud detection system that protects the privacy and security of consumer data. This can assist to strengthen customer trust and the overall security of the financial system.

1.2 Scope:

- The goal of homomorphic encryption-based privacy-preserving credit card fraud detection is to give financial institutions a safe and reliable means to identify fraudulent transactions while protecting the confidentiality of consumer information. homomorphic encryption is used in the system to safeguard client data, which is made to interact with transaction data from credit card providers.

- The system is applicable to financial institutions, such as banks and credit card companies, that need to detect fraudulent transactions while maintaining the privacy of customer data. The system can be used alongside existing fraud detection methods and can be integrated with other systems to provide a comprehensive fraud detection solution.

- The privacy-preserving credit card fraud detection system can be designed to be scalable and able to handle large volumes of transaction data. It can also be designed to have a fast response time, with the ability to process a single transaction in less than 1 second. This makes it suitable for use by financial institutions of all sizes.

- Overall, the scope of privacy-preserving credit card fraud detection using homomorphic encryption is to provide a secure and effective solution to the problem of credit card fraud detection while preserving the privacy of customer data. This can help to prevent financial losses due to fraudulent transactions and improve the overall security of the financial system.

2. General Description:

2.1 Product Perspective:

- A homomorphic encryption-based system for privacy-preserving credit card fraud detection would primarily focus on offering a safe and effective way to identify fraudulent transactions while protecting user privacy.

- The system would, technically speaking, encrypt the credit card information using homomorphic encryption before passing it to the

detecting system. In this way, user privacy would not be jeopardised and the detection system could handle the encrypted data without ever seeing the real credit card information.

- From a commercial standpoint, the product would have a number of advantages. In the first place, it would aid in preventing credit card theft and safeguard users from monetary damages. The user's trust and confidence in the credit card issuer or merchant would also improve, which would result in a rise in customer loyalty and retention. Finally, it would assist the credit card issuer or merchant in adhering to data privacy laws like the GDPR or CCPA and avoiding possible fines.

- The product would, in general, be a beneficial addition to the fraud detection industry and would provide a special and cutting-edge solution to the issue of credit card fraud detection while protecting user privacy.

2.2 Product Features:

- **homomorphic Encryption:** The system will use homomorphic encryption to preserve the privacy of customer data while allowing financial institutions to detect fraudulent transactions.
- **Fraud Detection:** The system will be able to detect fraudulent transactions based on patterns and trends in transaction data.
- **Privacy Preservation:** The system will preserve the privacy of customer data by encrypting it before processing it.

2.3 User Classes and Characteristics:

- The privacy-preserving credit card fraud detection system will be used by financial institutions, including banks and credit card companies. Users of the system will have a basic understanding of fraud detection and data analysis.

2.4 Design and Implementation Constraints:

- The system will be developed using Python programming language and will use the CKKS library for homomorphic encryption. The system will be designed to be scalable and will use a distributed processing system to handle large volumes of transaction data.

3. Specific Requirements:

3.1 Functional Requirements:

- **Credit card data encryption:** The system should be able to encrypt the credit card data using homomorphic encryption to protect the user's privacy.

- **Fraud detection algorithms:** The system should include efficient and accurate algorithms to detect fraudulent credit card transactions based on various factors such as transaction amount, location, time, and user behavior.

- **Real-time processing:** The system should be able to process credit card transactions in real-time to detect any potential fraudulent activity and prevent losses.

- **Integration with existing systems:** The system should be compatible and easily integrated with the existing credit card processing and fraud detection systems used by the credit card issuer or merchant.
- **User notification:** The system should be able to notify the user of any suspicious activity detected on their credit card account through alerts or notifications.

- **User opt-out:** The system should provide users with the option to opt-out of the fraud detection system if they choose to do so.

3.2 Non-Functional Requirements:

- **Security:** Credit card information should be safe and protected against unauthorised access, hacking, and online assaults by the system.

- **Performance:**The system should accurately identify fraudulent behaviour, handle credit card transactions in real-time, and have low latency.

- **Reliability:** To avoid any potential data loss or fraud, the system needs to be dependable and accessible at all times.

- **Maintainability:** With the least amount of downtime or inconvenience to the credit card issuer or merchant, the system should be simple to maintain and upgrade.

- **Cost-effectiveness:** The system should be cost-effective and provide value for money to the credit card issuer or merchant.

4. System Architecture:

4.1 System Components:

- **Data Ingestion Component:** The component will ingest transaction data from credit card companies.
- **Homomorphic Encryption Component:** The component will encrypt customer data using homomorphic encryption.
- **Fraud Detection Component:** The component will detect fraudulent transactions based on patterns and trends in transaction data.

- **Integration Component:** The component will integrate with existing fraud detection systems.

4.2 Data Flow:

- **Data Encryption:** In the first stage, the credit card information is encrypted using homomorphic encryption before sending it to the fraud detection system. This ensures that the credit card data is protected and kept private during the entire fraud detection process.

- **Fraud Detection:** In the second stage, the encrypted credit card data is processed using fraud detection algorithms to identify any potential fraudulent activity. The detection algorithms analyze various factors such as transaction amount, location, time, user behavior, and any other relevant data points. The fraud detection system then determines whether the transaction is legitimate or fraudulent based on the analysis.

- **Alert Notification:** In the third stage, if the fraud detection system identifies any suspicious activity, it generates an alert or notification to the credit card issuer or merchant, who can then take appropriate action to prevent any potential losses. The system may also generate a notification to the user to inform them of the suspicious activity detected on their credit card account.

- The data flow of the system is designed to ensure that credit card data is kept private and secure throughout the fraud detection process while still allowing the efficient and accurate identification of fraudulent activity. The system's design also enables real-time processing of credit card transactions to prevent any potential fraudulent activity before any losses occur.

5. User Interface:

- The system will not have a user interface. The system will be accessed through APIs.