Faculty of Information Technology
University of Moratuwa
BSc Hons in Information Technology
BSc Hons in Artificial Intelligence
BSc Hons in Information Technology & Management

IN 2211 – Object Oriented Analysis and Design

Level 2 – Semester 1 **Lab sheet 03**

Question 01

Given below is a detailed specification of an advanced payment authentication system of a financial institution. You are asked to analyze and design the system providing the required diagrams.

Customer authentication is a mandatory process but also can be a vulnerable point of security most of the time. Therefore the user authentication has become a complex process which may contain several sub processes utilizing the state-of-the-art security breach detection techniques.

The Authentication Card:
The customers of the institution are given a debit card which is equipped with a magnetic strip encoding a unique ID (card ID) which has been linked with the customer's records in the system. Customers can use the card online as well as at point of sale (POS).

Transaction at Point of Sale:
When a customer needs to make a payment at a POS he or she must provide the debit card to the seller. The seller will swap the card though the payment machine and enter the seller's password. The payment machine reads the card and fetches the card ID. Then the card ID is sent to the backend server and gets verified. In both cases where the machine cannot read the card or the backend server responded as the card ID cannot be verified, the card is considered to be invalid. If the card is valid then the seller can enter the amount to proceed with the payment. Otherwise the payment machine shows the error message and the seller can inform the customer about the error in the card. If the backend server has successfully processed the transaction the machine will print the receipt.

If the POS is in a different country than the customer's origin, the payment machine will ask for the passport number of the customer, hence the seller should ask for the passport and enter the passport number just before entering the amount. Inability to providing the passport will cancel-out the transaction.

Online Payments:
When the card is used for online payments, the customer should submit the customer's name, card number, expire date and the three digit security number through the web interface. The web interface will then submit the information to the backend server. While the server is verifying the information provided by the customer, the web interface should inform the user not to interrupt the process by any means. If the customer enables two-way verification, then a one-time-password (OTP) will be sent to the customers' mobile phone through an SMS. Then the web interface should collect the OTP from the customer. If the backend server has successfully processed the transaction the web interface will show the receipt.
Otherwise it shows the relevant error message on the web interface.

Process in Backend Server:
The task of the backend server is to verify the information submitted at a transaction, detect security breaches and complete the payment process. When the information is submitted through a POS machine, the information is compared with the available information in the database and if they are matched, then the information sends to an intelligent security breach detection system. The security breach detection system checks for any abnormality in the purchasing pattern of the customer. If no security breach or

abnormality detected, the server then proceed with the rest of the process. If an abnormality is detected the system will allocate an agent from the institution to make clarification by contacting the customer. If the agent decided that the breach detection is a false alarm, he can grant permission to proceed with the transaction. Otherwise the agent can lock the card permanently. Granting permission also sends a feedback to the breach detection system to update the knowledge about the purchasing pattern of the customer. If the information is not matched the front end will be notified to cancel the transaction with providing the reason.

The process is similar when the transaction is initiated using a web interface but it uses the intelligent security breach detection system only when the user has not activated the two-way-verification for the authentication.

1. Identify the users and the objects involved in the system.
2. Draw activity diagrams to show the flow of the system.