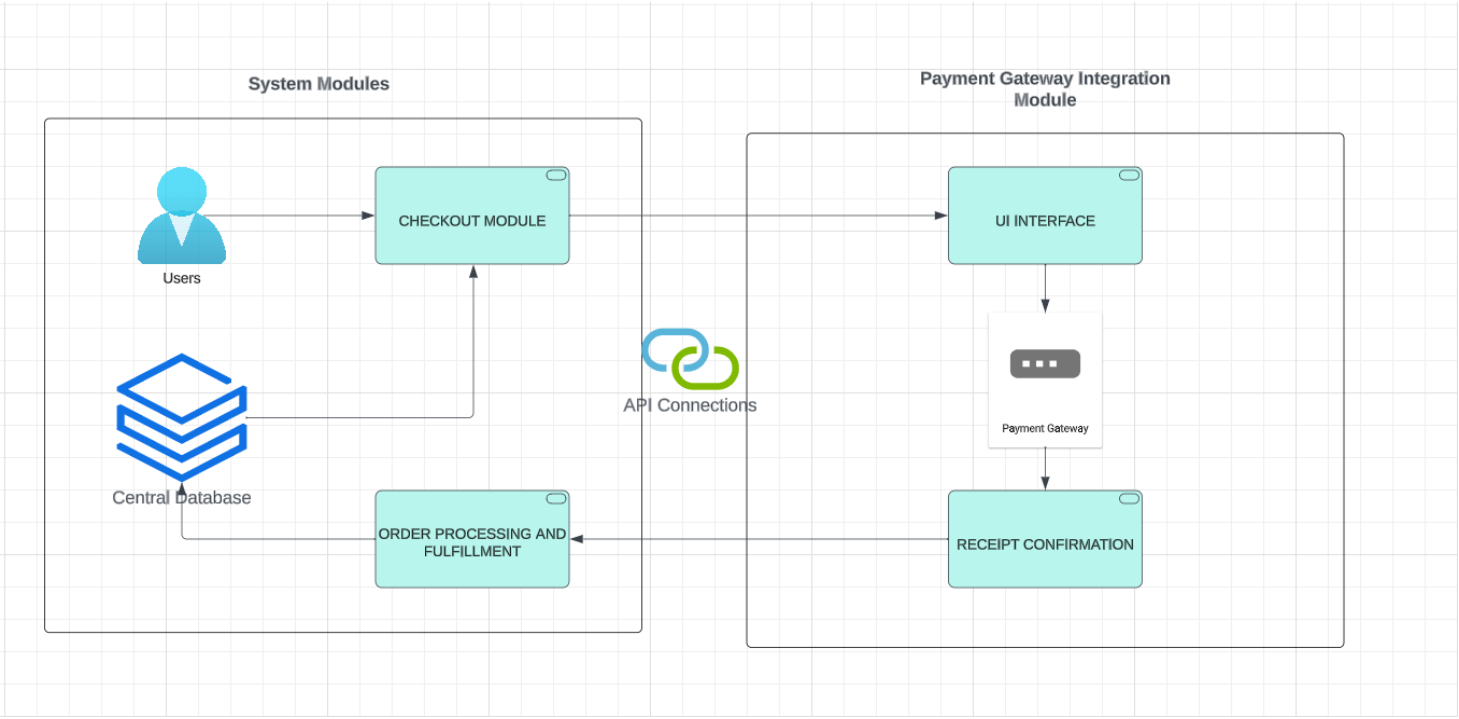
SYSTEMS INTEGRATION AND ARCHITECTURE

GROUP 1: PAYMENT GATEWAY & INTEGRATION

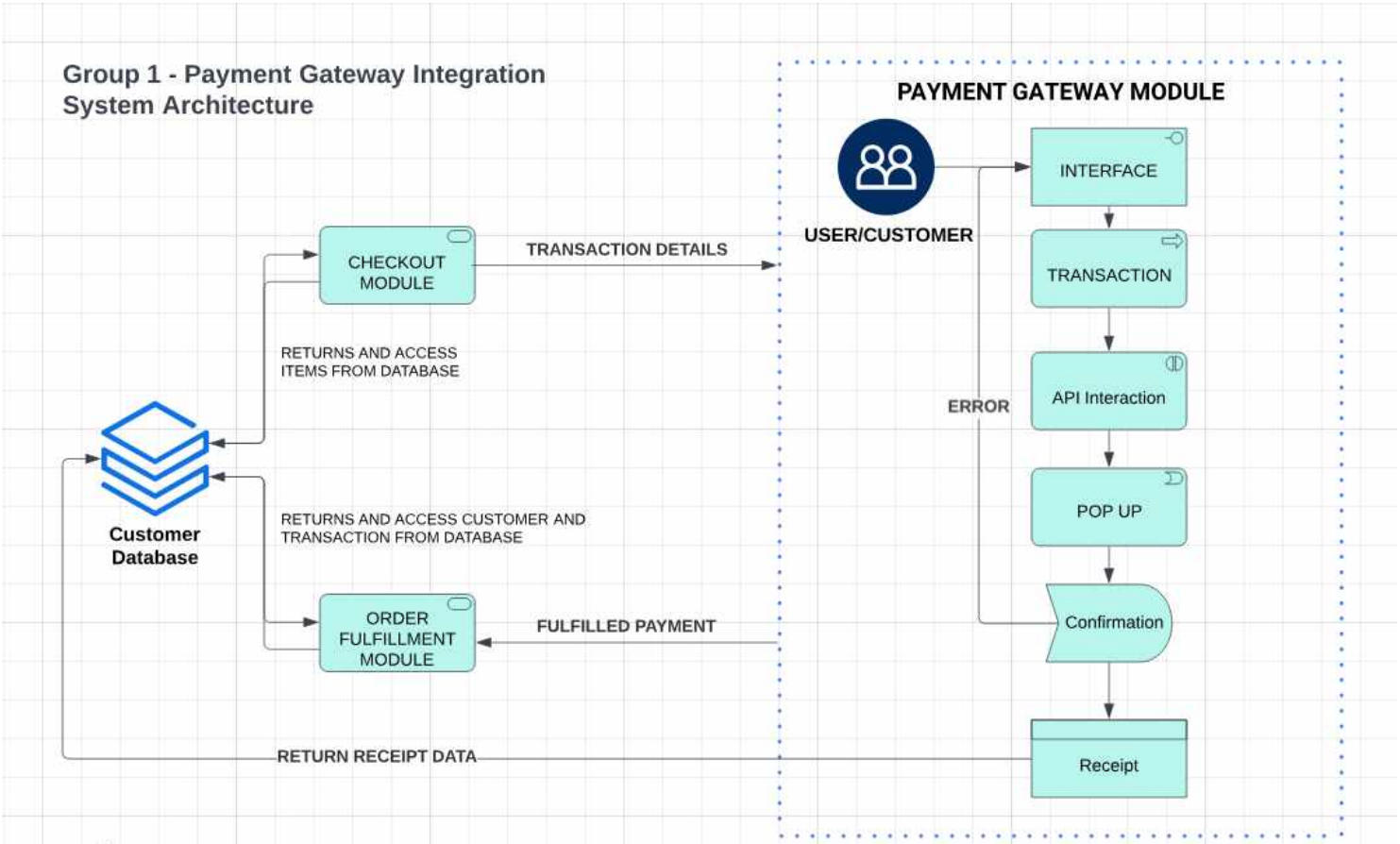
Baledoya, Kyla Keith
Domingo, Kirsten Charles
Parungao, Rafael Joar
Garcia, Mariel Kaye
Lopez, Maui Mark Daniel

BSIT 3-1

I. HIGH-LEVEL OVERVIEW



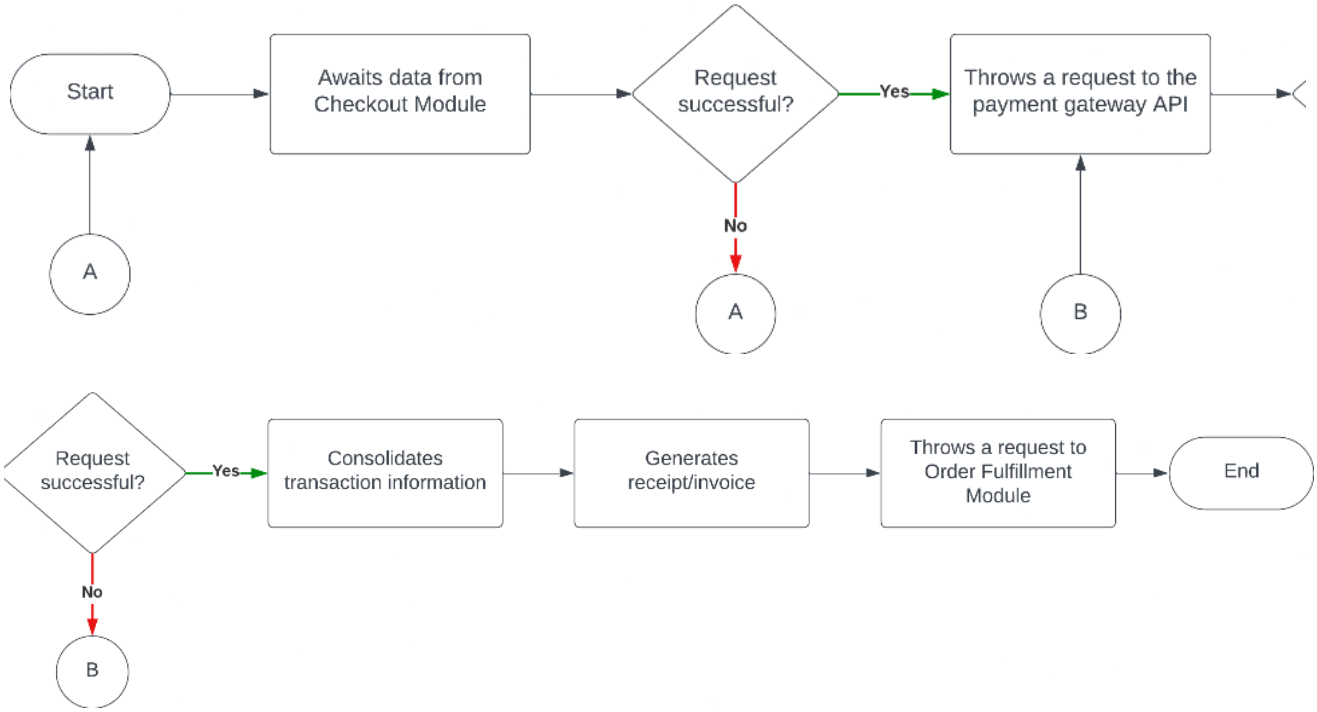
II. ARCHITECTURE DIAGRAM



III. COMPONENTS

- **REST API Connections -** The system will utilize the API connection from other system modules (Checkout Module, Order Fulfillment Module), as well as an API connection to the payment gateway service. The transfer of data from one system module to another will take place using the API Connection. As well as the, payment gateway API will be accessed to process the payments, and the module will await the response to confirm the fulfillment of the transaction.
- **Payment Gateway -** This component will act as the middleman between the e-commerce website and the acquirer's network. The system will access this through the payment gateway's API to throw a request with the customer's transaction details for payment processing and will wait for the response to confirm the transaction.
- **Data Encryption -** The system will utilize data encryption to encrypt the data when accessing API connections to ensure the safety of the user's data.

IV. DATA FLOW



V. COMPLIANCE

The payment integration is BSP-accredited as the payment method associated with the system is Gcash. Gcash is listed under Bangko Sentral ng Pilipinas (BSP) Supervised Electronic Money Issuers(EMIs). Gcash is proven by the compliance certification that it received from the Payment Card Industry Data Security Standards(PCI-DSS). The payment integration consists of data encryption as the standard for protecting user information. The associated payment gateway also consists of end-to-end encryption to protect user's against various threats. The overall system also requires users to have a 2-factor authentication for their safety that will help them in the security of their information. That also applies to the integrated application to ensure that the system can confirm the authenticity of users using the system. It also comes with maintenance updates to make sure that the integrated application will be up-to-date and ensure that the updated security information is strong enough to block most malwares and viruses. The system ensures that there are audits to perform regular conducts to the system and identify various vulnerabilities in the system to prevent further damage and repair the system to ensure the safety of the payment integration. The system also comes with training for managing the system and making sure to establish the course/rundown of the system ingrained with every personnel that will be managing the system. The system will include notifications to all users regarding their information, as part of the User Privacy Agreement for the system. This ensures that the user consents to the usage of their data for building their profile under the system and be used for their satisfaction.The system also prompts the user incase of emergencies and errors, that will have their transaction put on hold for as long as the issue/'s is fixed or terminated regarding with the level of the issue/s. This helps to maintain that users' privacy and information will be protected under certain circumstances.