UTM

UNIVERSITI TEKNOLOGI MALAYSIA

SECP1513 SECTION 08

TECHNOLOGY AND INFORMATION SYSTEM

FRAUD TRANSACTION DETECTION SYSTEM

Prepared for

DR LAYLA RASHEED ABDALLAH HASAN

Prepared by:

FULL NAME	MATRIC NO.
NURUL ‘AFIFAH BINTI MOHAMAD YUSOF	A21EC0120
AIN SAFIAH BINTI MANAN	A21EC0155
LUQMAN HAKIM BIN MD SAID	A21EC0050
KAGINESWARAN A/L TAMIL VANAN	A21EC0035

Table of Content

1.0 Introduction

In our current world of ever-evolving technologies, people and companies are incorporating technology into almost everything, from the field of agriculture to the field of medicine such as delivering a baby, simulations of operation procedures, and many more. In addition to the COVID-19 pandemic, people have been more dependent on digital platforms and technology in daily activities. For example in making bill payments, purchasing daily necessities, etc.

The adoption of digital technology did help humans in a lot of aspects such as improvement in activities and innovation efficiency. However, despite all of the benefits it brings, these dependencies on technology can leave us vulnerable to much unwanted and malicious intent from third parties like cybercriminals. Cybercriminals are those who use technology to do malicious activities to gain benefit for personal or group purposes. Most of the cases are for financial gain.

Due to that, here are some common disadvantages of digitalization. Firstly, the lack of data security can cause the organization to lose information not only about the organization but also the personal information of the employers, employees, and even the customers which can be dangerous if it lands in the wrong hands. It may result in a financial loss at the enterprise or personal level. The worst thing is it may cause the organization to lose the trust of their clients and customers. Besides that, with the current growth of data received by organizations around the world, some cannot keep up with the increasing amount of data which makes them unable to set up proper cybersecurity procedures to protect all that data and detect any fraudulent data effectively.

These are just a few of the long list problems faced due to the lack of appropriate steps taken when using technology. Therefore, the step of prevention needs to be taken to prevent unwanted incidents. It is known that technology is beneficial in many ways with the appropriate measures taken to prevent any malicious intention from the internal or external entities. The implementation of IR4.0 technologies plays a role in achieving those benefits. With this, our objective for this project is to create a system that can detect fraudulent activities in the financial aspect with the aid of IR4.0 technologies and appropriate Cloud Computing architecture.

2.0 Project Steps and Description

For this Low Fidelity Prototype project, we would like to propose a project called "Fraud Transaction Detection System.". As the name states, the function of this system is to detect a plausible fraud transaction and prevent it from happening. The transactions here included online banking, and credit card transactions. The system is able to detect a fraudulent transaction through the data they receive during the transaction and the data that have been stored previously.

2.1 Project Ideas

In coming up with this project idea, we did go through a trial and error process with a few different project ideas while maintaining our concept to focus on the data. We want to come up with a data-related project because data is a crucial element in most aspects. Be it from the health, education, safety, technology development, and not to be forgotten the economic and finance. From the data, we can get information. The information is varied depending on the data itself. For example, from the data about cash-flow, and activities of an organization, we might be able to get information about the organization's condition and use it for benefit. Be it for good or bad. On the other hand, if the data are not managed properly, there will be a potential for inaccurate or worse, false information.

With the increasing amount of data, the task of managing, processing, and protecting the data has become more challenging. The diagram below is some of the ideas that we have been come out with:

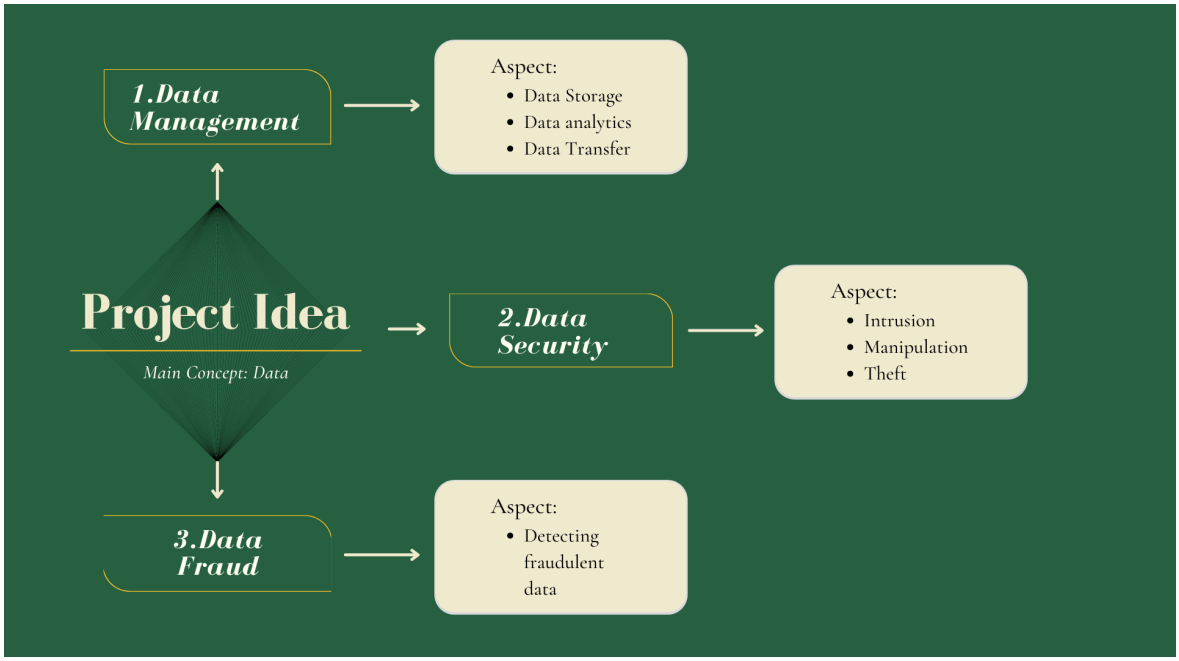


Figure 1: Project Ideas

Initially, we plan to do a data management system. The target for this system would be the developing company or the company that wishes to have better data management in terms of storage, analyzing, and transferring data. However, as we see through the idea, we agreed to focus on the security aspect of the data. We would like to have products that will prevent data intrusion, manipulation, and theft. Here is where we decide to come out with a fraud detection system because preventing an attack at the early stage is much better than battling the attack heads on. It also can help in preventing the loss of the victims.

2.2 Potential Client

As we have finalized the concept and idea about the project, we look for the possible client or the potential client for this project and the problem they have so that this project can help them overcome the problem more efficiently. There are two types of potential clients that we can find. First is the business organization and the second is the bank.

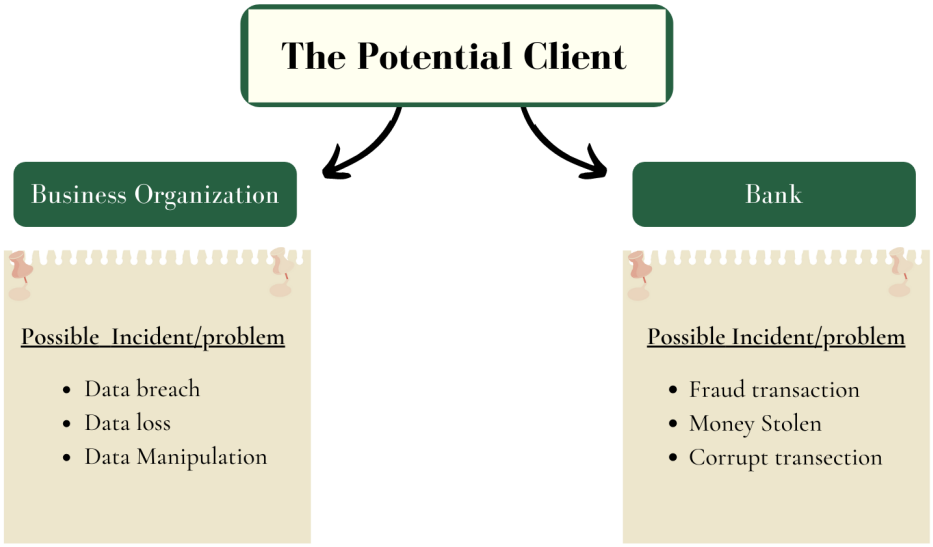


Figure 2: Problem possibly faced by the potential client.

For the business organization, getting the data in check is important as it is needed to operate the business, and data or information leakage might be harmful to the organization. It might be worse if it's stolen, lost, or manipulated. Having fraudulent data in the system might only lead to a worse situation, it would be best to detect it at the early stage where it might not be a huge harm and prevent the criminal from gaining what they want.

As for the bank, they hold quite a big part in protecting their clients' and customers' assets and money. As the bank is a great target by criminals in gaining financial benefit. Especially in the current world, robbing the bank might not need the robber to get physical with the bank because things can be done through the cyber aspect. It can be from phishing the bank's client to give them their bank information, or to the point perhaps attacking the bank's system. Therefore, detecting any possible attack or fraud transaction is important to prevent loss for the bank and victim.

Between the two potential clients, we choose to move forward with the banks because we might be able to help the community by preventing from their money being stolen when they might not even be aware

2.3 Problem Analysis and Solution

The implementation of a fraud detection system might be varied based on the type of data they processed and the way they process it. Therefore, we analyze the problem statement from the potential client and see what is the best way to overcome the problem. In the solution to overcome the problem, we implement the fraud detection system to detect fraudulent data in order to prevent fraudulent transactions. Make it a fraud transaction detection system. did include the 4IR technologies to enhance our system. This includes artificial intelligence and machine learning to allow the system to be dynamic and improve especially when it processes and trains with more data.

2.4 Project duration

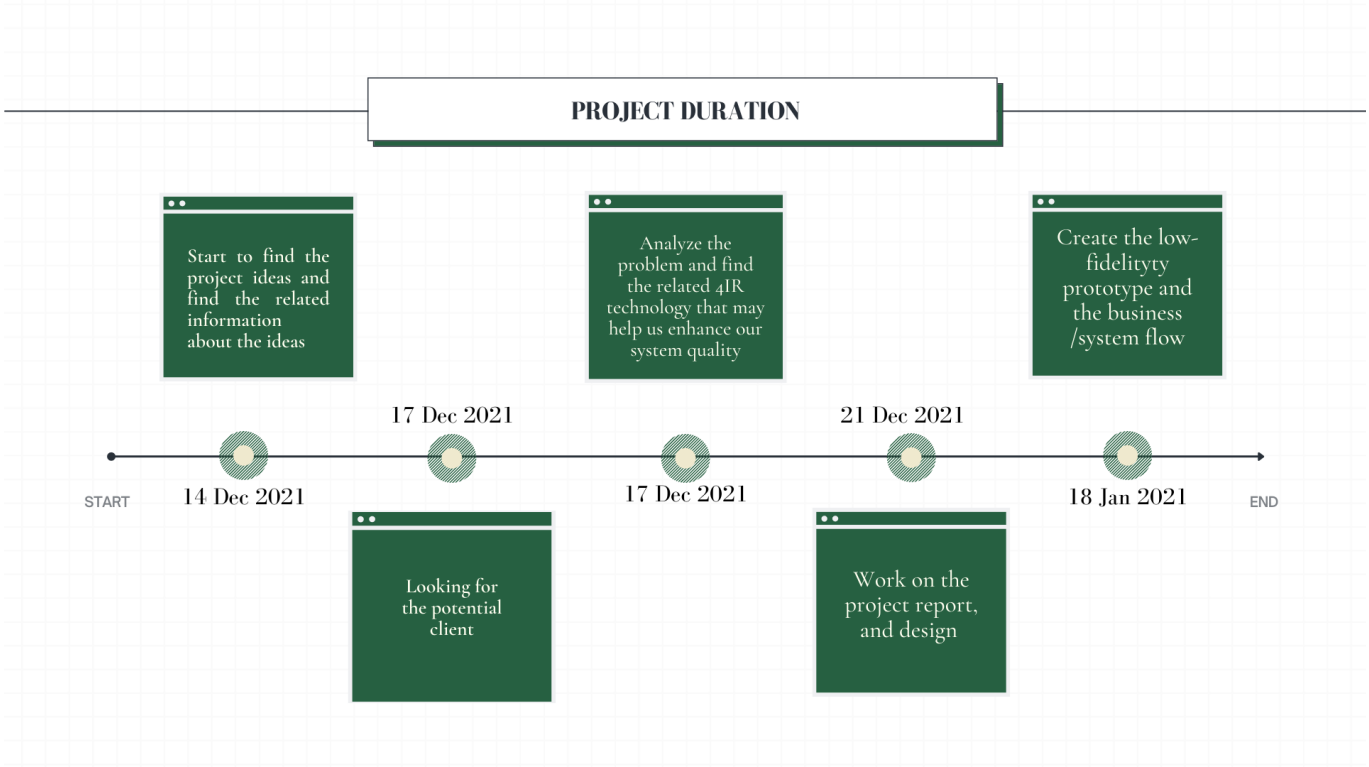


Figure 3: Project duration

3.0 Problem, solution, and team working.

3.1 Problem

As Bank A started to grow, they received complaints from customers that they lost their money from their accounts, and some of them did receive unauthorized credit card charges. However, they did not make those transactions. Hence, Bank A wants to detect payment and identity fraud to prevent and stop fraudulent transactions and activities. The fraudulent activities here mean the customers' activities throughout the bank such as accessing the account information.

3.2 Solution

For this project, we would like to create a system that can detect fraudulent activities or transactions throughout a bank called “Fraud Transaction Detection System”. The creation of this system includes the 4IR technology such as Cybersecurity, Artificial Intelligence, Machine Learning, and Cloud Computing.

3.2.1 Cybersecurity

Cybersecurity involves the policies and application of technologies used in protecting digital components, systems, networks, programs, devices, and data from cyberattacks which can bring harm to the victims mostly on the economic and financial aspects. This is because most cyberattacks that occur are intended to gain profit.

A fraudulent transaction or activity may occur in various ways. It can happen with account takeover by the cybercriminal, getting access by stealing the bank account information, or many more ways. There are a lot of cyberattacks that may be involved in the process but here we would like to emphasize Phishing and Malware attacks.

Phishing is a cybercrime frequently used to gain sensitive information from users, such as usernames, passwords, and credit/debit card numbers. It occurs when a cybercriminal assumes the identity of a legitimate entity through an email, instant message, or text message and convinces a victim to open those email, instant messages, or text messages. The recipients are deceived into opening a malicious link, which results in the installation of malware, the freezing of the victim's machine as part of a ransomware

attack, or the revealing of sensitive information. In other cases, it might occur when the victim is convinced to give out their personal information such as bank information through those platforms.

Malware is a generic phrase that refers to any malicious software designed to infect or exploit any programmable device, service, or network. Malware is classified into numerous categories, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper, and scareware. It is used to extract data or information from victims. This data may include sensitive data such as financial information, healthcare records, personal emails, and passwords. Else, it can be used to gain access to the victim's side such as the victim's accounts or devices.

With the related data, information, or access gained by those cybercriminals. Then, they might be able to make a fraudulent transaction. As the final protection for the customers, the bank can implement cybersecurity on the transaction process by detecting and stopping fraudulent transactions. This is possible by encrypting the data and using flexible security features to block unauthorized personnel from accessing the users' data.

3.2.2 Artificial Intelligence and Machine Learning

In detecting fraudulent transactions or activities, Artificial Intelligence and Machine Learning technologies can be used. Artificial Intelligence, AI is the simulation of human intelligence processes by machines, particularly computer systems, and Machine learning is a subset of artificial intelligence that has the ability to approach data analysis that involves building and adapting modes, which help the programs to improve their performance over time. Machine learning also contains the algorithm that will help the models to adapt and improve the ability to make any predictions.

AI and Machine learning can be used in transaction or activities verification such as facial recognition scanners because it is possible to swiftly evaluate many types of events and identify a variety of fraudulent data, ranging from false transactions to identity fraud or theft that could lead to a financial loss to the victims as an individual or as an organization. These systems may improve with time since Machine learning is used. Machine learning learns from the data received from the previous cases. This machine learning will then segment and extract the required features from the collective data. From this, machine learning can learn and train itself to detect a similar type of fraud or fraud that are not the same but have the similarity with the previous cases.

In the case of fraud detection, a machine learning model and example dataset from the previous transaction are being used. Perhaps, the transaction amount, the IP address of the device used for online transactions, location, or others. The fraud detection deploys a machine learning model and the example dataset to train the model to recognize fraud patterns. By comparing the data transaction with the fraud pattern, the model is able to recognize or predict whether the data is fraud or not. The model is dynamic since it is able to predict the new fraud pattern. It is possible with the ability of the model to self-learn with the new data. While detecting fraud data, the data received by the model is used to improve the fraud pattern.

3.2.3 Cloud Computing

For implementing the fraud transaction detection system, we would like to use Cloud computing technology to support the architecture of the system. Cloud computing is the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer. Examples of cloud computing providers are Amazon Web Services, Microsoft Azure, and Google Cloud. Most cloud computing providers apply pay-per-use services.

The use of cloud computing technology in implementing the system can bring a lot of benefits such as cost optimization since we don't need to build and maintain the hardware infrastructure of the system. The implementation of the on-premises infrastructure might result in a capitalized cost where cost needs to be covered or paid even if the service is not in use. In managing the hardware infrastructure, a lot of things need to be considered, the security aspect, maintenance, the storage of the server, the service needs to be used, and much more.

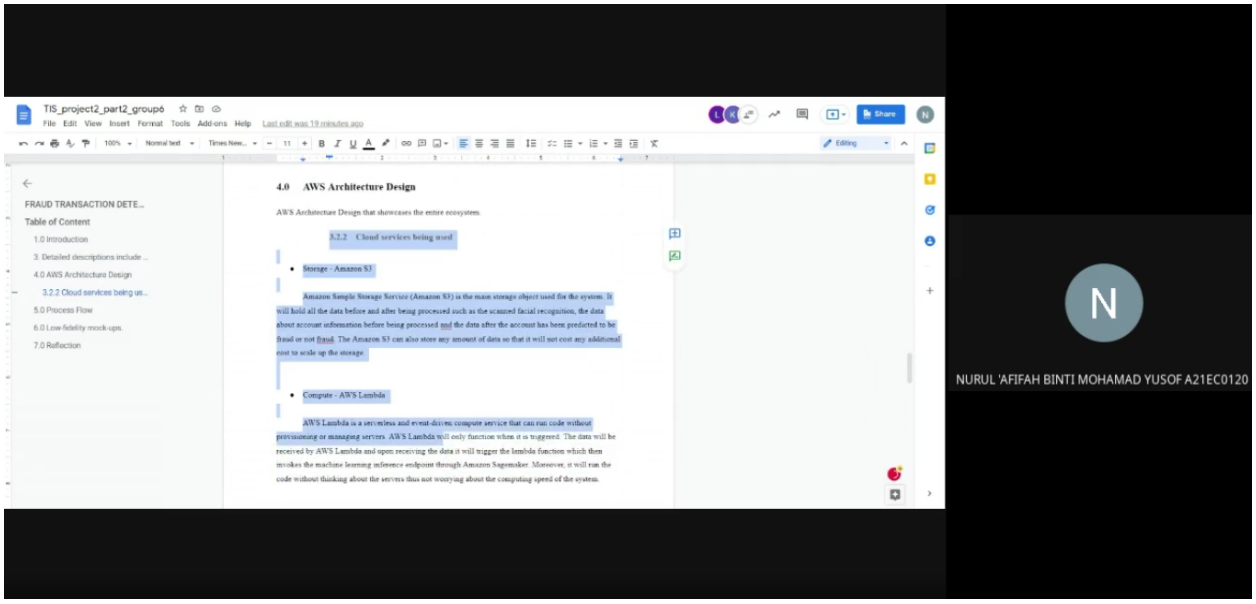
By using cloud computing, we didn’t need to worry about the hardware infrastructure since it is being taken care of by the cloud service provider. In contrast, if we decided to use the on-premises infrastructure, the risk for the hardware infrastructure to be attacked are high, especially without a high-security precaution which may result in the system malfunction and can’t operate properly. Even if there are no attacks on the hardware infrastructure, constant maintenance needs to be done. The utility cost such as the bills also needs to be considered.

The transaction process in and out of the bank involved a huge amount of data and an inconsistent data flow of numbers. Therefore, in the deployment of the system, we need to have a scalable infrastructure to prevent the system malfunction or when the system is down since it can't support any sudden increase in the amount of data. Hence, cloud computing can be used since it is scalable.

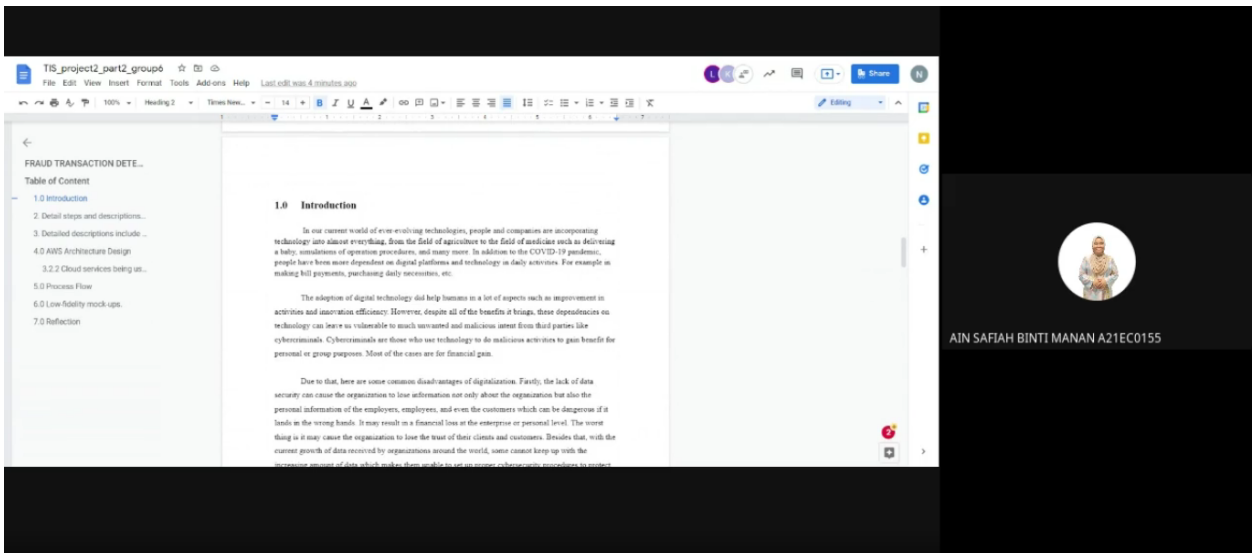
In this project, the fraud detection system, AI, and machine learning are being used. Therefore, cloud computing is suitable for system deployment since the cloud service provider AWS did provide services for AI and machine learning implementation

3.3 Team working

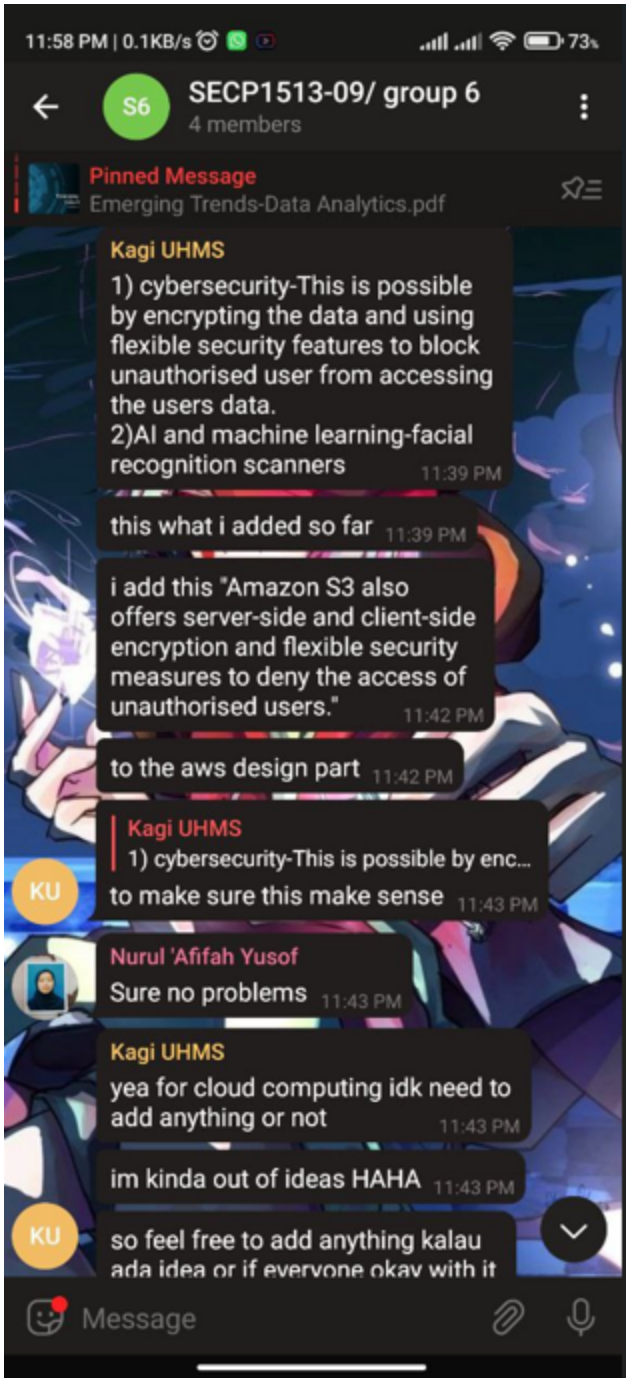
The platforms we have used to discuss our project for parts 1 and 2 where we have worked together to come up with a solution for the clients' problem is Telegram and Google Meet. Here are some evidence to show our discussion.



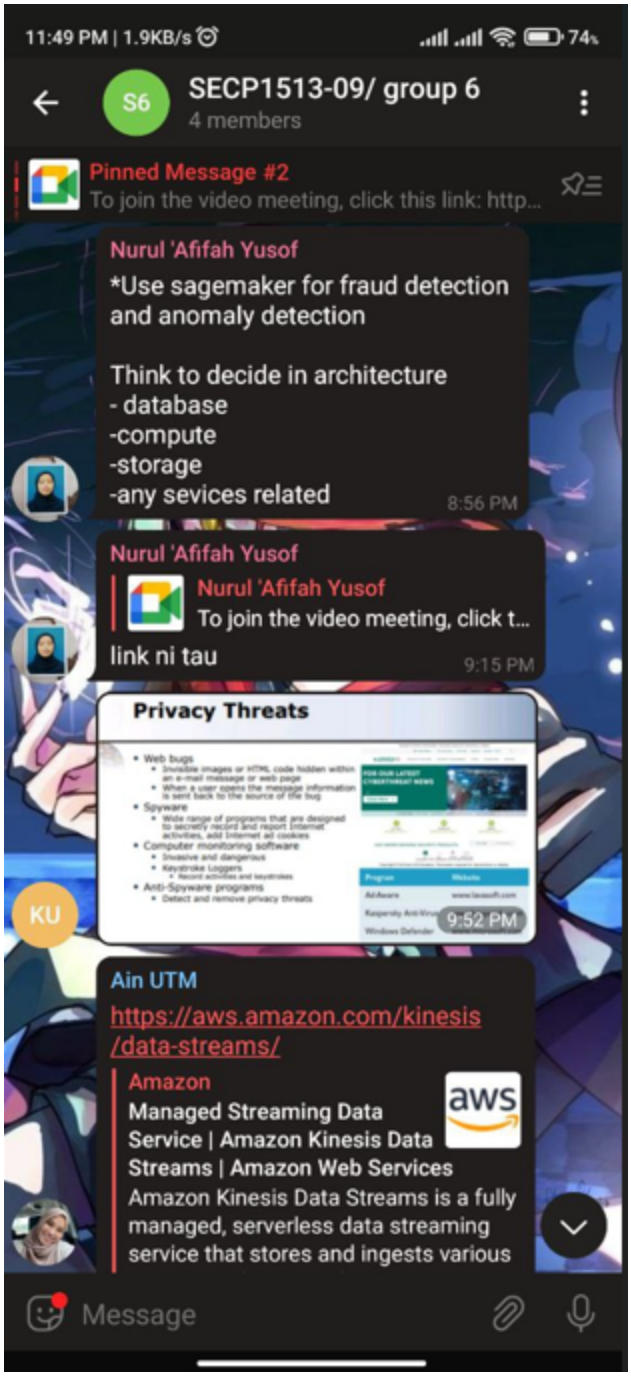
This screenshot shows that we are in a Google Meet discussion about AWS architecture design.



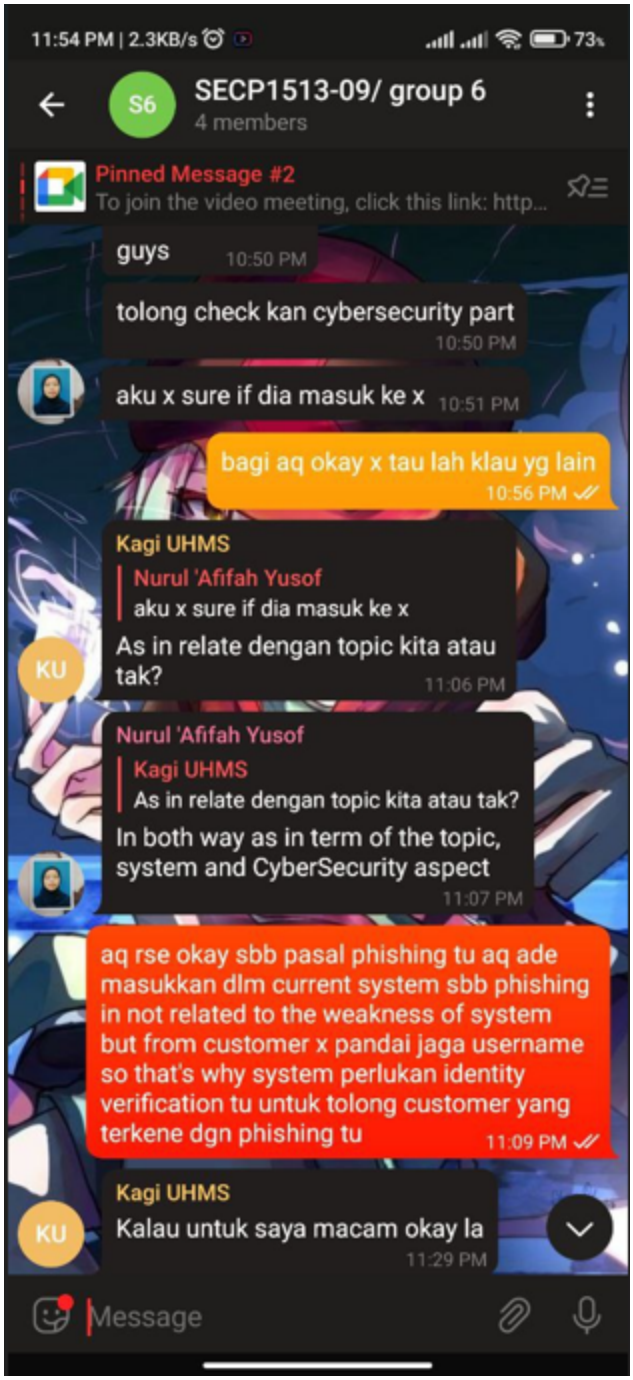
This screenshot shows that we are discussing the introduction of our project in Google Meet.



The screenshot shows we are adding more descriptive details into our solution for our project in part 2 using Telegram.



This screenshot shows we are discussing the services to use for our Fraud Transaction Detection System using Telegram.



This screenshot shows that we are reviewing the contents of 4IR in part 1 of the project using the Telegram platform.

4.0 AWS Architecture Design

4.1 Cloud services being used

- Storage - Amazon S3

Amazon Simple Storage Service (Amazon S3) is the main storage object used for the system. It will hold all the data before and after being processed such as the scanned facial recognition, the data about account information after and before being processed, and the data after the account has been predicted to be fraud or not a fraud. Amazon S3 can also store any amount of data so that it will not cost any additional cost to scale up the storage if needed.

- Compute - AWS Lambda

AWS Lambda is a serverless and event-driven compute service that can run code without provisioning or managing servers. AWS Lambda will only function when it is triggered. The data will be received by AWS Lambda and upon receiving the data it will trigger the lambda function which then invokes the machine learning inference endpoint through Amazon Sagemaker. Moreover, it will run the code without thinking about the servers thus not worrying about the computing speed of the system.

- Machine learning services - Amazon Sagemaker (Amazon Fraud Detector)

By using Amazon Sagemaker, the system will use Amazon Fraud Detector to build a fraud detection machine learning model that is customized to your data in a few clicks using a fully automated process. The detection logic works by combining your model with decision rules to turn model scores into actionable outcomes. For real-time fraud detection, call the Amazon Fraud Detector API with online event data to receive fraud predictions. Our system will be primarily using this service to identify suspicious online payments, it detects potential fraud to swiftly and correctly find abnormalities and patterns. With this, not only online payments but also irregular credit card usage will be monitored. This will then predict the data to be fraud or not fraud and then send a verification text to the user via Amazon SNS.

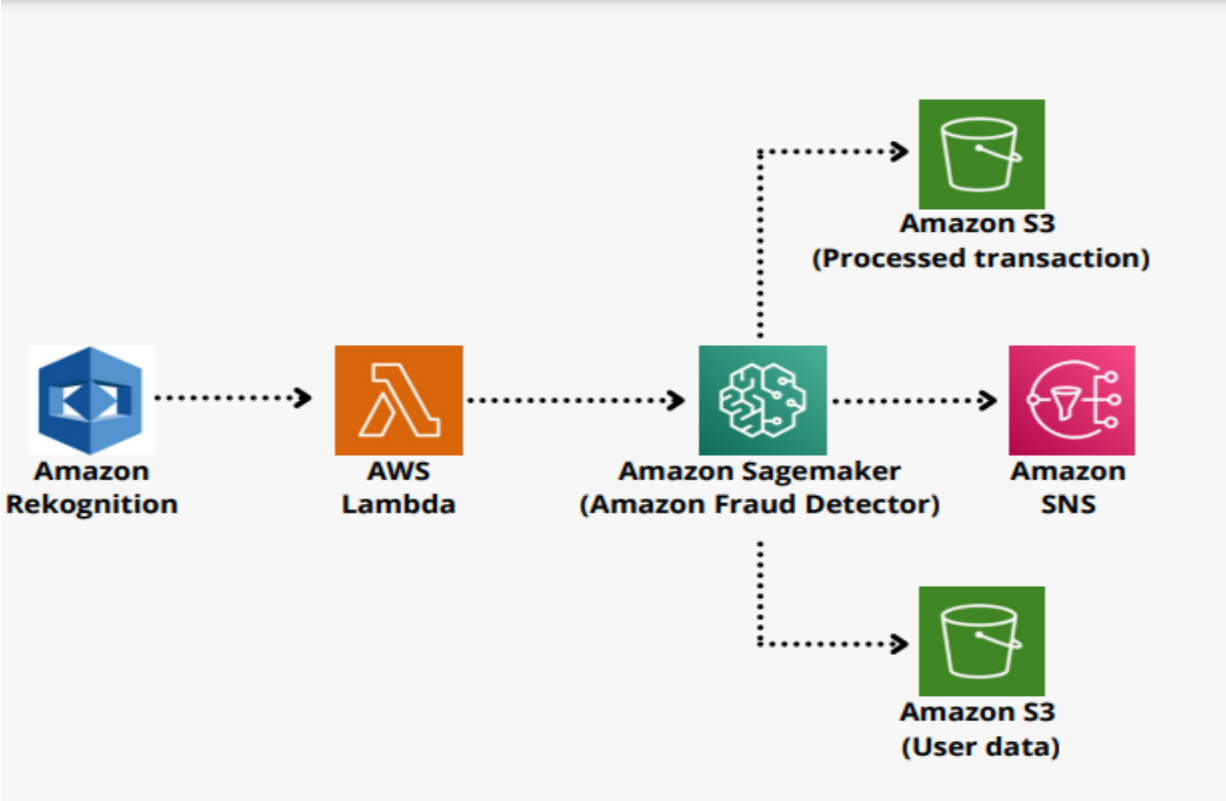
- Identity verification - Amazon Rekognition

By using Amazon Rekognition, the customers will be asked to provide a selfie picture and an identity document picture for initial registration. When doing transactions a scanned face of themselves will be asked to be provided. The system uses facial biometrics powered by machine learning to do identity verification. It also uses Amazon Rekognition Face Comparison, which helps measure the similarity of two faces to help you determine if they are the same person. Amazon Rekognition Face Index and Search enables the system to create a face collection of existing users and search for new user selfie pictures against all faces in the collection to detect duplicate or fraudulent account creation attempts.

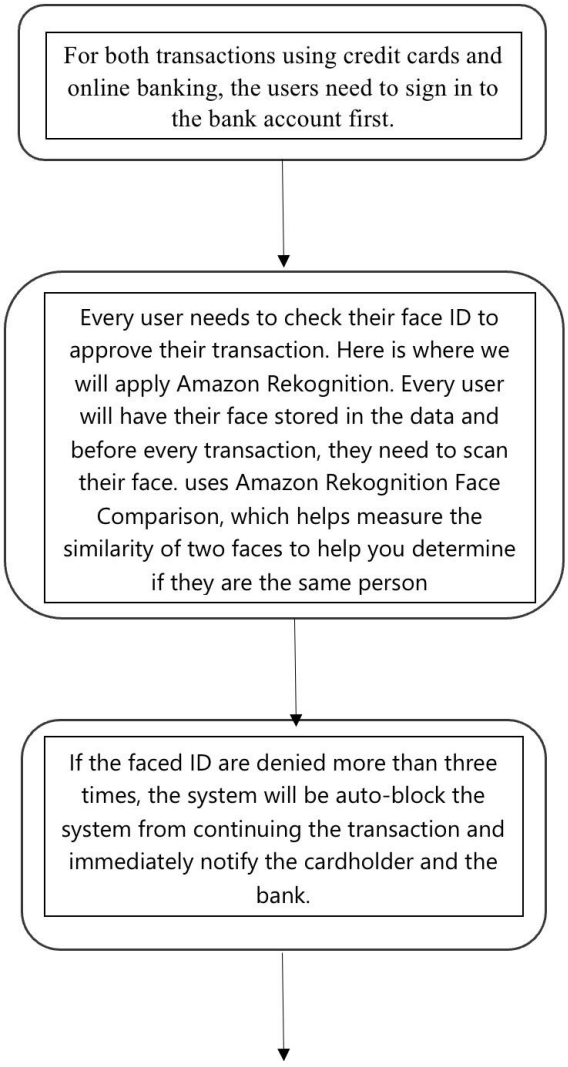
- SMS- Amazon Simple Notification Service (Amazon SNS)

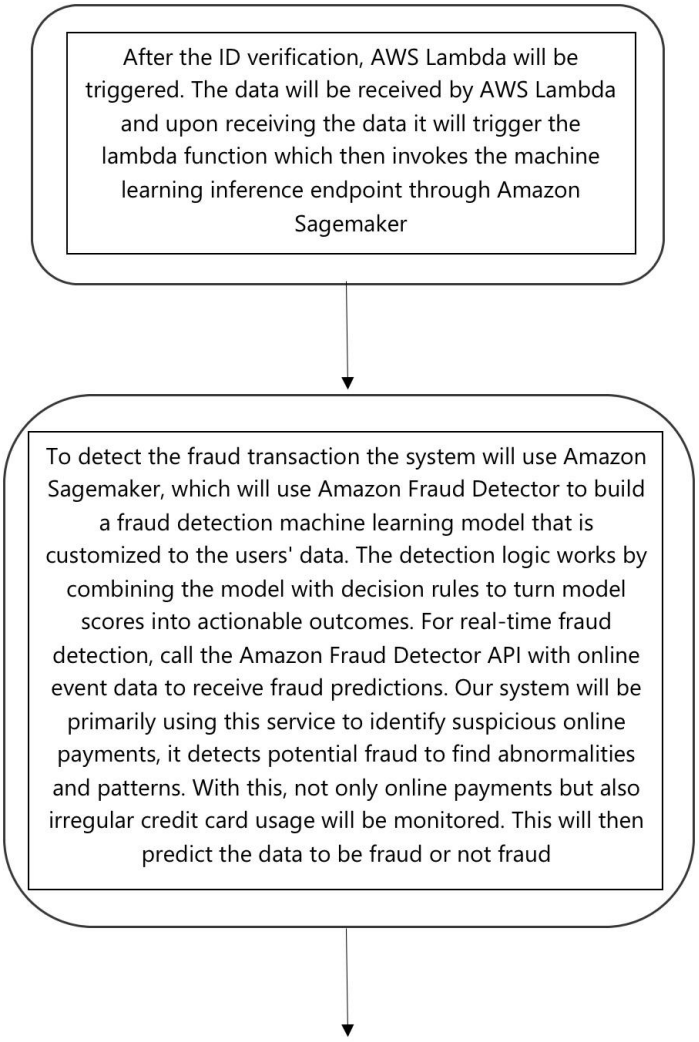
Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service that is for both application-to-application (A2A) and application-to-person (A2P). By using Amazon SNS either a verification text or an account balance update text can be sent after Amazon Fraud Detector API predicts the data to be fraud or not via SMS because Amazon SNS supports messaging to over 200 countries. This action is an example of application-to-person (A2P) communication.

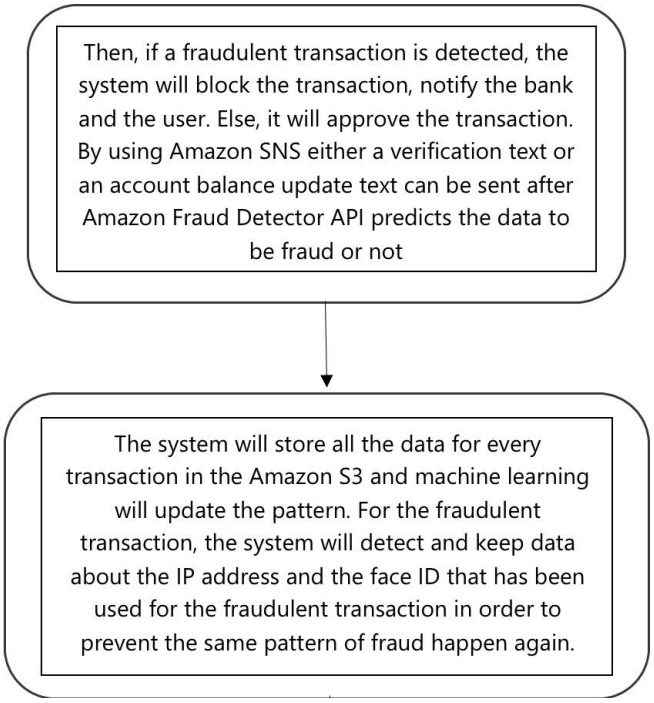
4.2 AWS System Flow



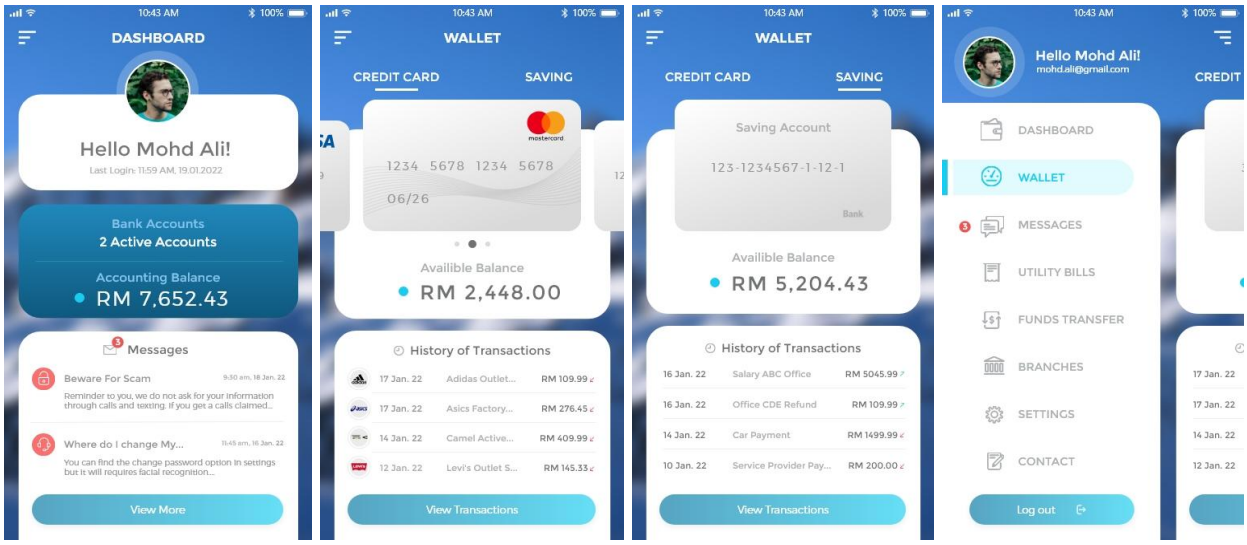
5.0 Process Flow




After the ID verification, AWS Lambda will be triggered. The data will be received by AWS Lambda and upon receiving the data it will trigger the lambda function which then invokes the machine learning inference endpoint through Amazon Sagemaker
To detect the fraud transaction the system will use Amazon Sagemaker, which will use Amazon Fraud Detector to build a fraud detection machine learning model that is customized to the users' data. The detection logic works by combining the model with decision rules to turn model scores into actionable outcomes. For real-time fraud detection, call the Amazon Fraud Detector API with online event data to receive fraud predictions. Our system will be primarily using this service to identify suspicious online payments, it detects potential fraud to find abnormalities and patterns. With this, not only online payments but also irregular credit card usage will be monitored. This will then predict the data to be fraud or not fraud


Then, if a fraudulent transaction is detected, the system will block the transaction, notify the bank and the user. Else, it will approve the transaction. By using Amazon SNS either a verification text or an account balance update text can be sent after Amazon Fraud Detector API predicts the data to be fraud or not
The system will store all the data for every transaction in the Amazon S3 and machine learning will update the pattern. For the fraudulent transaction, the system will detect and keep data about the IP address and the face ID that has been used for the fraudulent transaction in order to prevent the same pattern of fraud happen again.

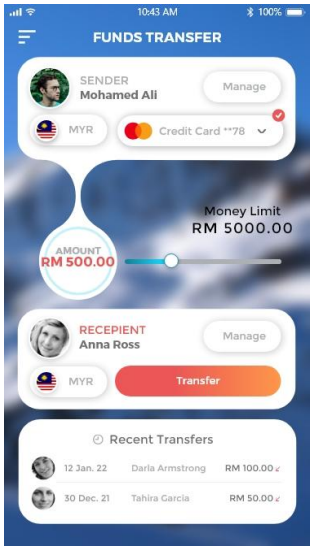
6.0 Low-fidelity mock-ups.



- *Bank Dashboard*

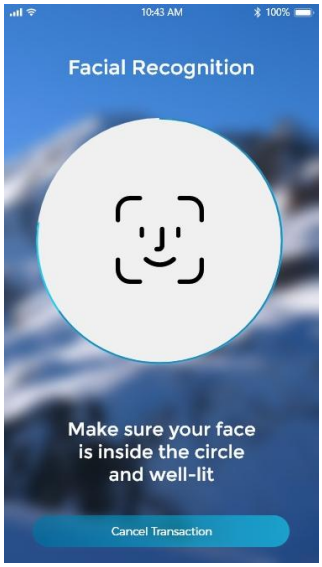
This is a simple bank User Interface(UI) design. It has a dashboard, types of wallets which are credit cards or saving accounts, and a sidebar for user interaction. The dashboard varies depending on the banking system. The dashboard only has the basics needed for a banking system for this project. After the user logs into the system, the first page is the dashboard that shows the user information like balances and card and saving account numbers.

Next, the wallet interface shows the credit card and the savings account and indicates the available balance and transaction history. The sidebar is for user interaction to move between pages. For example, the dashboard icon will lead to the dashboard page.



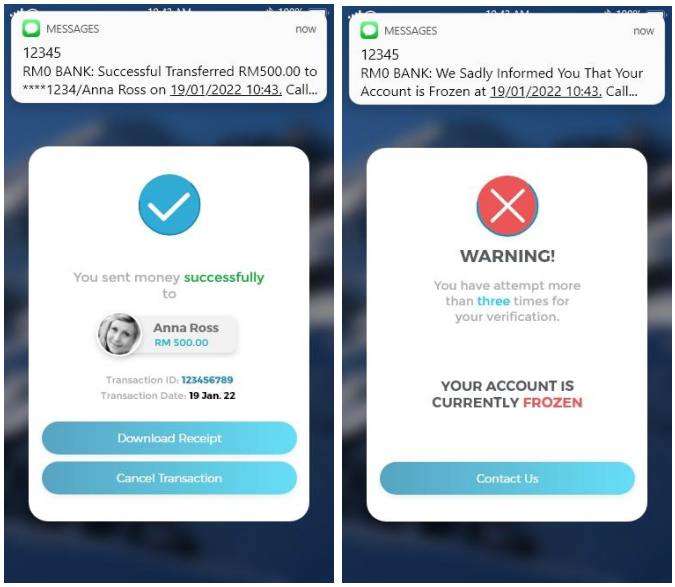
- Funds Transfer

This interface is for transferring money from one's account to another. If the users want to transfer their money to someone, they can choose between many currencies. It also shows the limit on how much money can be transferred for the month. The user also can see the details of past transactions on their account if they sent or received money to someone.



- *Facial Recognition*

If users want to make any transactions or log in to their accounts, it will show the facial recognition interface. This part will be where Amazon Rekognition services take place. The user will be required to scan their face using their camera to verify their attempt to log in or transaction activity. Next, Amazon Rekognition Face Comparison compares the input face with the face in the database when the user registers.



- *Transaction status*

After facial recognition, the system will show whether the transaction is successful or not. The user will be directed to the successful transaction interface if the transaction is successful, but the user will be directed to the unsuccessful transaction interface if the transaction fails. For failing the facial verification, the bank will freeze the account as a precaution to avoid data fraud. The user will also get a message notifying them of every transaction and failed login attempt.

7.0 Reflection

7.1 What have you learned and your motivation to complete this project?

Throughout this project, we have learned a lot of things. Especially, about the selected fourth industrial revolution technologies. In this case, artificial intelligence, machine learning, cyber security, and cloud computing. Things we have learned in this project include the basic concept of those technologies, how they can be used or applied into action, and many more. The knowledge that we get might not be too deep about those technologies. However, it opens us to the current technologies out there and makes us eager to explore more.

Our motivation to complete this project is we want to see the product of our project. How it may possibly work through the low-fidelity mock-ups. This includes the flow of the system, how it will interact with the users, and a lot more. We would say that our motivation is our own satisfaction in being able to come out with the product and learn new things. Of course, the support and participation from all of the team members help us to keep on moving forward.

7.2 What issues and solutions are implemented to make the project a success?

The first issue we faced was being inexperienced as a team. Since this is our first time doing a low fidelity prototype project we are very inexperienced on how to start with the flow of doing the project and have many doubts and questions about the requirements of the project. Although we were facing this problem, we managed to overcome it by frequently asking our lecturer questions about the criteria and requirements of our project to make up for the lack of experience.

The second issue we faced was communication limitation. Since we are currently undergoing classes via online learning, the team members have not got the chance to meet each other since we are all from various parts of the country and could not physically meet up with each other to share our findings and ideas. We managed to solve this problem by having our discussions using platforms such as Google Meet and Telegram to discuss our projects by scheduling meetings and reviewing our findings using those platforms.

The third and final issue we faced was being an unorganized team. Initially, our group was having issues sticking with just one problem statement and we changed our problem statement multiple times due to our unorganized planning. To overcome this issue we decided to choose a team leader and give our opinions one by one and eventually agreed on a problem statement that our team leader chose after careful consideration of all the other team members. The team leader also helped delegate our tasks effectively to the team members which solved our unorganized team.

7.3 What is your direction after completing this project?

Our inexperience has made our project take longer than it is to finish. Hence, after completing this project, our direction is that we will gain more experience in this 4th Industrial Revolution era. We will learn as many pieces of knowledge as possible to help us with our future projects. The expertise we build from every project we do and the knowledge we gain might open up a new technology that we might create someday. Our focus for this new technology will be to help all people and maybe create something called an intelligent world.

We might start by learning more about Amazon Web Services(AWS), one of the most effective cloud computing platforms in this revolutionary era. AWS has offered over 150 services to help individuals, companies, and even governments to make cloud computing architecture. It will have a massive impact on us if we manage to comprehend all of Amazon's services in the future. AWS will be our stepping stone to achieve further in the technology world because there is no limit to what technology can be improved.

7.4 What is the improvement necessary for you to improve your potential in the industry?

In my opinion, the improvement that is needed for us to improve our potential in the industry is to have more knowledge about new technology and also the way it is being applied to prevent new cyber threats that happen in our daily life. Day by day, the number of frauds increased by the factor of technological advancement. These are serious issues that need to be prevented before they become worse. Having good technology such as machine learning, artificial intelligence, cyber security, geotargeting and other advancements in information technology specifically set the stage for more technological evolution.

We can use this technology to prevent data from being stolen, losing important information in our data, fraud in our banking system, and more. Nowadays, our life depends on technology that we use as mass communication in our daily lives, and cyber fraud cases have also increased, so most companies require someone that has good knowledge and skills in technology to prevent and obstruct the same cyber fraud from happening again. So, we will have a higher potential in the industry because, with the good knowledge and skills that we have, it may be one of the criteria needed in order to get any kind of jobs that are related to technology.

As future employees, we need to be smart in organizing our tasks in order to produce a good quality of work and I think this improvement is necessary for us to improve our potential in the industry. Good organizational skills can help to save time, prevent miscommunication, and improve the efficiency and quality of work. Planning what to do and prioritizing the urgent tasks can help to manage all the tasks wisely. As an example, list all the tasks based on priority, which is from the highest to lowest priority. This is to ensure that all the projects or tasks are completed in the time given. Plus, if you are smart in organizing your work, people will have eyes on you and you will have the opportunity of getting a better job in the future.

Next, having good communication skills is a must in order to improve our potential in the industry. Communication ranked first among the most sought-after soft skills among employers in a 2016 LinkedIn survey performed in the United States. This has shown that communication is very important to allow others to understand what you are saying and also for yourself to understand information accurately. When having good communication skills, helps us excel in our jobs interview and passes the selection process because the employers will attract with the way we are confident in the state of our points and also, we are being able to communicate with them effectively. Good communication skills are also one of the important criteria by which you need to communicate with your colleagues to do your job effectively, by which you have to discuss problems, request information, and interact with others. By having good communication skills, the employer will see your potential in their company and it will make you have good potential in the industry.