FACULTY OF COMPUTING
UTM Johor Bahru

SECP 1513: Technology Information System

Semester 01, 2024/2025

PROJECT PROPOSAL

FRAUDFLEX: FAKE ONLINE PAYMENT RECEIPT SCANNER

TEAM NAME: KETECHKI

TEAM MEMBERS:

NO	NAME	MATRIC ID
1.	NABIHA NAJWA BINTI HALIM	A24CS0143
2.	NURUL ASYERA BINTI PONNIRAN	A24CS0173
3.	AINUR MARDHIAH BINTI SANIP	A24CS0041
4.	AKRAM ALI MURSHED AL-SHAM	A23CS4022
5.	ABDELRAHMAN ELFATIH ABDELRAHMAN AHMED	A23CS4032

CLIENT NAME:

1.SALMI BINTI ABD.MAJID

Table of Contents

1. Introduction

NEED (N)

As technologies continue to advance, online payment has become an essential part for business as it is more practical and convenient for both sellers and customers. However, with the rise of digital transactions, cases of fraud have also increased. A growing concern among sellers is the use of fake payment receipts by customers to deceive businesses and avoid making actual payments. Fake receipts can be easily created or manipulated using basic photo editing tools, making it difficult for sellers to distinguish between genuine and fake payment proofs. This leads to financial losses, disrupts business operations and undermines trust between sellers and buyers.

We had the opportunity to confront Puan Salmi Binti Abd.Majid, a mini market owner operating in Kolej Tun Dr Ismail, UTM, to gather insights on the challenges she faces with online payments. Puan Salmi stated that almost all of her customers prefer online payment over cash transactions. She also stated that she finds it to be more convenient for her too, especially since it reduces the need to prepare a small change for the customers.

However, while Puan Salmi believes that most of her customers are honest with the payment, she cannot completely deny that there have been some days where her daily cash-in records fell short, raising concerns about potential fake payment. She highlighted that manually verifying each receipt is impractical, especially during busy hours when customer traffic is high. This makes it difficult to catch every error or scam attempt.

APPROACH (A)

Our system, Fraudflex, can provide the solution for the problem. We created a system with user convenience and security in mind where sellers can use it to quickly and accurately detect fake receipts without the need for time-consuming manual verification. While checking it manually could also be convenient, they can become a burden for the sellers if they are dealing with a lot of customers leading to delays and potential human errors. Our automated system could improve the process with a more time saving and accurate process.

We understand that sellers value efficiency and time saving solutions, therefore, our system is designed with a simple, one step process that ensures quick and accurate receipt verification without any complicated procedures. Sellers are only required to upload or scan the payment receipt provided by the customer. This single action triggers the entire verification process automatically without any additional steps.

Once the receipt is uploaded, the system will automatically perform multiple analyses in real time. By using the Optical Character Recognition (OCR) technology, the system will extract text and numerical data from the receipt including transaction ID, payment date and time, amount paid, payment method (bank transfer, e-wallet and etc.), reference number and merchant details.

Then, by using Image Forensics Tools, the receipts will be analyzed for any sign of tampering or fake. Image forensics tools can help to detect how images were created using the metadata available. Different types of metadata can be extracted from the receipt image including, timestamp, editing history, and prompts and models used for Generative AI. This information can immediately detect if the receipt is fake or not.

We then use a fraud detection learning machine which is XGBoost (Extreme Gradient Boosting) to evaluate the receipts based on patterns from genuine and fake receipts. This will increase the accuracy to detect the fake receipts. XGBoost is great for its flexibility, high accuracy and effectiveness in dealing with large and complex datasets which are reliable for this system.

And finally, the system instantly classifies the receipt as valid, suspicious, or fake after all of the analyses are complete.

BENEFIT (B)

The proposed system offers numerous benefits for mart owners, particularly in addressing the issue of fraudulent payment receipts. One of the primary advantages is enhanced security. By utilizing advanced technologies such as Optical Character Recognition (OCR), image forensics tools, and the XGBoost machine learning model, the system ensures accurate and reliable detection of fake payment receipts. This helps mart owners protect their businesses from financial losses caused by fraud, which is a common issue in digital payment systems.

Another significant benefit is the improvement in operational efficiency. Mart owners often deal with high customer traffic, making manual verification of payment receipts impractical and time-consuming. Our system automates the verification process, allowing receipts to be validated in real time. This not only saves time but also reduces delays during peak business hours, enabling smooth and efficient operations.

In addition, the system eliminates the risk of human error. During busy periods, manually checking receipts can result in mistakes or missed fraudulent transactions. By automating

this task, the system ensures consistent and accurate verification, reducing the workload on staff and minimizing errors.

The system is designed with user convenience in mind, featuring a simple one-step process that does not require technical expertise. Mart owners can easily upload or scan payment receipts, and the system performs all the necessary checks automatically. Furthermore, it supports a wide range of payment methods, such as bank transfers and e-wallets, making it highly adaptable to the needs of different businesses.

Finally, the system builds trust between mart owners and their customers. By ensuring accurate verification of payments, customers can be confident that their transactions are processed correctly, while owners can operate without concerns about fraudulent activities. This fosters a more reliable and transparent payment environment.

Overall, the system offers a secure, efficient and user-friendly solution for mart owners, addressing a critical problem in modern business operations. It not only protects against fraud but also streamlines the receipt verification process, making it an essential tool for businesses that rely on online payments.

COMPETITORS (C)

To address the growing issue of fraudulent activities such as fake receipts, a variety of tools and services have been developed to detect fraud in digital documents and receipts. Below is an overview of several existing solutions available in the market.

Figure 1: Homeppl’s Fraud Finder’s Logo

source:https://www.homeppl.com/

Homeppl's Fraud Finder is a specialized tool designed to detect tampered or altered digital documents, such as bank statements. It works by analyzing subtle signs of manipulation, including mixed fonts, altered layers, and other evidence of tampering within the document

(Homeppl, 2024). The tool is highly effective for financial institutions and auditors due to its advanced detection capabilities, especially in verifying documents for authenticity.

Figure 2: Taggun's Logo

source:https://www.taggun.io/pricing

Taggun uses Optical Character Recognition (OCR) technology to extract and digitize text from receipts, bills, and other printed documents. Its main strength is in automating data entry and creating digital records of receipts, which is useful for tracking expenses and inventory management (Taggun, 2024). Taggun's efficiency in record-keeping makes it a valuable tool for businesses that need to maintain digital documentation.

Figure 3: Fintelite's Logo

source:https://fintelite.ai/documents-fraud-detection/?gad_source=1&gclid=EAIaIQobChMImYTu_YD6igMVhqVmAh2XsR3gEAAYASAAEgJjM_D_BwE

Fintelite is designed specifically to detect fraud within bank statements in real-time. It uses fraud detection algorithms and pattern recognition to analyze transaction data, helping financial institutions identify fraudulent activity quickly (Fintelite, 2024). Its strength lies in providing continuous monitoring of bank statements, making it ideal for environments where constant vigilance is required to detect financial discrepancies.

These systems are highly specialized and each serves its intended purpose effectively. However, they are limited in scope and may not always offer solutions for broader fraud detection needs, especially in retail environments where quick verification of transactions is essential.

On the other hand, FraudFlex is designed specifically for the real-time detection of fake bank transaction receipts, particularly those based on QR codes. The app utilizes sophisticated AI detection techniques to instantly identify anomalies or signs of tampering, ensuring fast and

accurate verification of receipts at the point of sale. This makes FraudFlex highly suitable for retail environments, where quick fraud detection is essential. The app is user-friendly, offering an intuitive interface that can be easily used by both experienced users and those with little technological knowledge, such as elderly users or non-technical staff. Additionally, its affordability makes it accessible to small businesses that may not have the budget for expensive fraud detection systems. In today's increasingly digital payment landscape, FraudFlex provides an essential solution for real-time, low-cost fraud detection, making it ideal for everyday transactions and small-scale sellers.

2. Existing Systems

Below is a comparison of current systems, highlighting their limitations and how our proposed solution improves upon them:

Comparison of Existing Systems

Features	Homeppl's Fraud Finder	Taggun	Fintelite	Proposed System (FraudFlex)
Detects fake receipts	Yes	Yes	Yes (statements only)	Yes
Real-time verification	Yes	Yes	Yes	Yes
QR code fraud detection	Yes	No	No	Yes
User-friendly for non-tech users	No	Yes	No	Yes
Cost-effective for small sellers	No	Yes	No	Yes

Built-in app for mobile use	No	No	No	Yes

While several fraud detection systems are available, there are some issues with the current tools that need addressing.

Homeppl's Fraud Finder, although effective for detecting tampered documents, its technical interface can be difficult for everyday users to navigate, limiting its use to environments that require extensive document verification, such as financial institutions and auditors. This makes it impractical for casual users or small businesses, who may not have the expertise or resources to utilize such a tool effectively.

Taggun, while efficient for record-keeping, lacks any fraud detection capabilities. It focuses solely on digitizing receipts and documents for tracking purposes but does not verify the authenticity of the documents. As a result, it cannot identify altered or fake receipts, which severely limits its use in preventing fraud.

Fintelite, which excels at detecting fraud within bank statements, is highly specialized and not suited for retail environments. It does not focus on verifying transaction receipts, which are more common in everyday transactions. Therefore, its application is narrow, and it cannot address fraud in retail settings where receipts need to be verified quickly and easily.

Justification of the Proposed System

Our proposed system fills these gaps by providing a specialized, real-time solution for detecting fake bank receipts. It leverages advanced AI algorithms to analyze receipts for tampering and offers instant feedback to sellers. The system also includes a built-in mobile app, making it highly accessible and easy to use in various scenarios. Designed with user-friendliness in mind, it caters to elderly users and small-scale sellers who often struggle with technical tools. Additionally, its affordability ensures that even small businesses can access this critical fraud detection technology, making it a practical and superior choice in the digital payment ecosystem.

3. Proposed System

3.1 Prototype

We designed a prototype to demonstrate the system functionality and serve as a guide for the user. To make our system look more realistic, we create a phone-like model from cardboard and use multiple pieces of paper that was glued together to simulate a touch screen effect.

Figure 4.1: Welcome Screen

It represents the **welcome screen** of the FraudFlex system. It features the system name, a shield icon (symbolizing security and fraud detection), and a **"START"** button to initiate the process. This screen serves as the entry point for users who want to verify the authenticity of receipts.

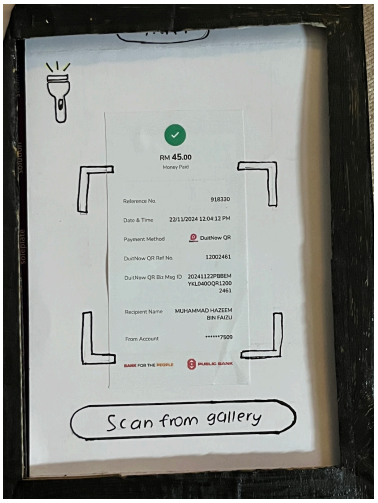

Figure 4.2: Receipt Scanning Interface

This screen allows users to either **scan a receipt using the camera** or **upload an image from the gallery** for verification. The receipt in the image is an example of a scanned/uploaded receipt. FraudFlex processes this receipt by extracting key details, such as:

- Amount Paid
- Reference Number
- Date & Time
- Payment Method
- Recipient Name

These details are then analyzed for inconsistencies or signs of forgery.

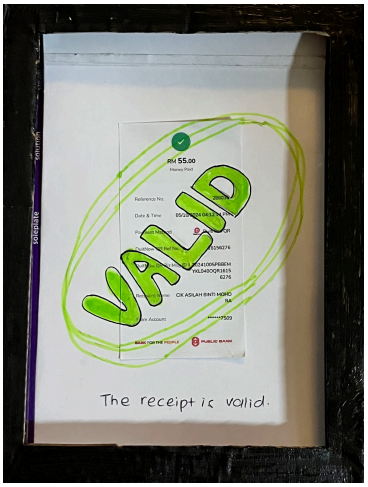

Figure 4.3.1: Verification Result - Valid Receipt

In this example, the receipt has been identified as **valid**, indicated by the large green “VALID” stamp. Below, a message confirms: **"The receipt is valid."** If the receipt were fraudulent, the system would instead display a warning indicating potential fraud.

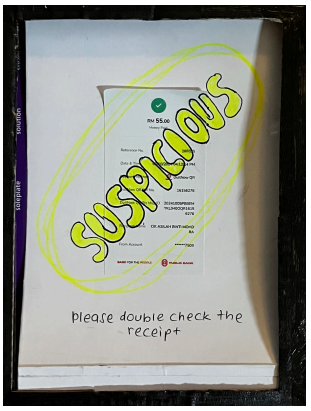

Figure 4.3.2: Verification Result - Suspicious Receipt

In cases where FraudFlex detects **potential inconsistencies** in a receipt but cannot confirm it as fake, it marks the receipt as **"Suspicious."** This may happen due to:

- Missing or altered details
- Blurry or low-quality images that prevent accurate verification.
- Mismatch with bank records (if applicable).

In this scenario, the system prompts the user with a **warning message** and advises **manual verification** or further investigation before accepting the receipt.

Figure 4.3.3: Verification Result - Fake Receipt

If FraudFlex determines that a receipt is **fraudulent**, it marks the receipt as **"Fake"** and alerts the user. The system may detect a fake receipt due to:

- Edited or manipulated elements (changes in font, layout or colors).
- Invalid transaction reference numbers that do not match genuine bank formats.
- Tampered logos or incorrect bank details that indicate forgery.

A red **"FAKE"** stamp is displayed along with a warning message, advising the user to **reject the receipt** and take necessary actions, such as reporting the fraud.

3.2 Advance System

The proposed system is designed to deal with the issue of fraud and corruption in payments and receipts efficiently, it uses existing technologies to validate the payments, making it the best solution for busy retail environments.

Features and Functionality

1. **Real-Time Verification**
   The system offers immediate analysis of receipts to determine their authenticity. Users can upload or scan a receipt, and the system processes it instantly.
2. **Advanced Technologies**
   - **Optical Character Recognition (OCR):** Extracts critical details like transaction ID, payment date, amount, payment method, reference number, and merchant details from uploaded receipts.
   - **Image Forensics Tools:** Detects tampering by analyzing metadata, including timestamps, editing history, and AI-generation prompts.
   - **Machine Learning Integration:** Utilizes the XGBoost algorithm to evaluate patterns from genuine and fake receipts, ensuring high accuracy in fraud detection.
3. **User-Friendly Interface**
   The system is designed to be intuitive, requiring minimal technical expertise. Sellers can upload receipts with a single step, triggering the verification process automatically.
4. **Wide Compatibility**
   It supports various payment methods, such as bank transfers and e-wallets, ensuring broad applicability across different business types.
5. **Fraud Classification**
   After analysis, the system categorizes receipts as valid, suspicious, or fake, providing actionable insights to sellers.

Advantages Over Existing Systems

The proposed solution addresses the limitations of current tools:

- Unlike **Homeppl's Fraud Finder**, it provides real-time fraud detection and a user-friendly interface suitable for non-technical users.
- Unlike **Taggun**, it goes beyond digitization by verifying receipt authenticity.
- Unlike **Fintelite**, it focuses on retail settings, offering QR code fraud detection and affordability for small-scale businesses.

Benefits

This system delivers multiple benefits:

- **Enhanced Security:** Protects businesses from financial losses due to fake receipts.
- **Operational Efficiency:** Automates verification, saving time and reducing delays during peak hours.
- **Minimized Human Errors:** Ensures consistent and accurate results, even during busy periods.
- **Increased Trust:** Builds customer confidence by ensuring transaction accuracy.

By leveraging advanced technologies, the system provides an affordable, accessible, and efficient solution to a critical problem faced by businesses reliant on digital payments.

4. References

[1] Subashini Jeyaraman. (2024). *Store owner scammed by woman using altered QR payment receipts*. Retrived from https://thesun.my/style-life/going-viral/cosmetics-businesswoman-allegedly-scammed-by-customer-using-altered-qr-payment-receipt-CC13002189

[2] OCR with Google AI. (n.d.). Google Cloud. Retrieved from https://cloud.google.com/use-cases/ocr

[3] Burns, M. (2020). *A quick guide to digital image forensics in 2020.* Retrieved from https://www.cameraforensics.com/blog/2020/03/06/a-quick-guide-to-digital-image-forensics-in-2020/

[4] Tanya. (2024). *5 New Machine Learning Algorithms for Fraud Detection.* Retrieved from https://trustdecision.com/resources/blog/5-new-machine-learning-algorithms-for-fraud-detection

[5] Homeppl: Customer Risk Assessment & Fraud Prevention. (2024). Retrieved from https://www.homeppl.com/

[6] Taggun. (2024). Retrieved from https://www.taggun.io/pricing

[7] Martha. (2024, January 17). Fintelite. Retrieved from https://fintelite.ai/documents-fraud-detection/?gad_source=1&gclid=EAIaIQobChMImYTu_YD6igMVhqVmAh2XsR3gEAAYASAAEgJjM_D_BwE

5. Project Scheduled

Phase	Tasks	Responsible	Timeline
Requirement Analysis	- Conduct interviews with stakeholders - Gather requirements for the receipt scanner system - Finalize system specifications	Nabiha, Ainur	Week 1 (1-7 days)
Research & Design	- Research existing fraud detection technologies (OCR, Image Forensics, XGBoost) - Create the system architecture and flow diagrams - Design user interface (UI) mockups	Nabiha / Ainur / Asyera	Week 2 (8-14 days)

Prototype Development	- Set up the development environment - Develop OCR module - Implement Image Forensics Tools - Integrate XGBoost machine learning algorithm - Build initial front-end interface	Abdul, Akram	Week 3-4 (15-28 days)
Testing & Refinement	- Conduct unit testing for each module - Perform integration testing to ensure modules work cohesively - Gather user feedback from stakeholders	Nabiha / Ainur / Asyeral	Week 5 (29-35 days)
Final Deployment	- Deploy the system for real-world testing - Train the client (Salmi) on using the system - Prepare documentation and user manuals	Abdul, Akram	Week 6 (36-42 days)
Presentation & Submission	- Finalize the project report and presentation materials - Present the system to instructors and stakeholders	All team members	Week 7 (43-49 days)

6. Appendices

Screenshot

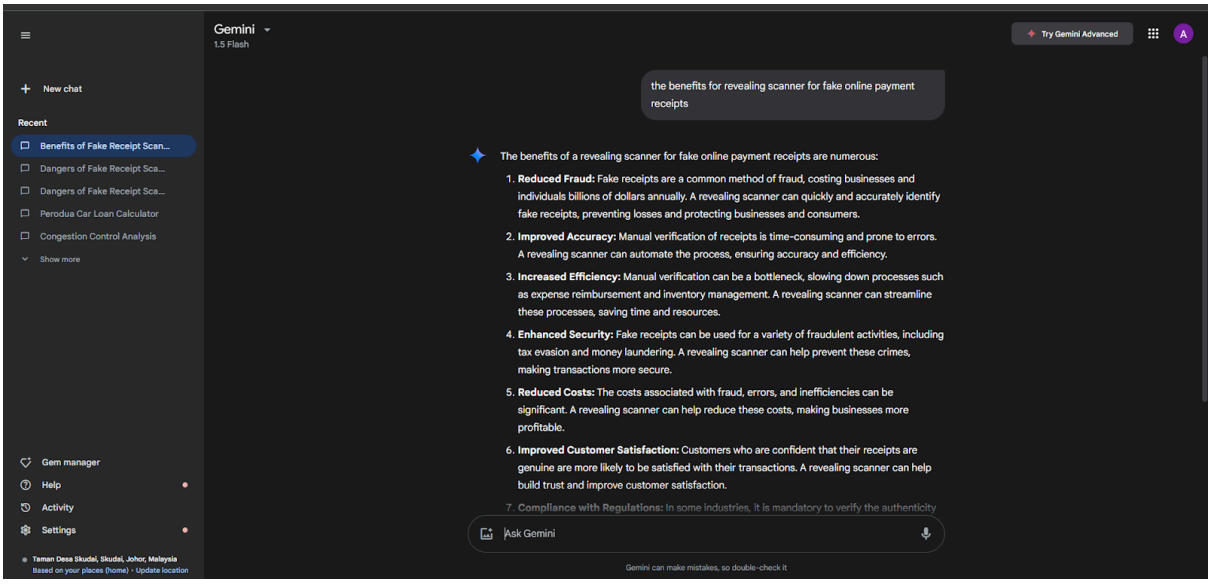

Figure 1: Screenshot Generative AI Benefits for Scanner for Fake Online Payment Receipts

URL

https://g.co/gemini/share/245b91d54f43

Screenshot

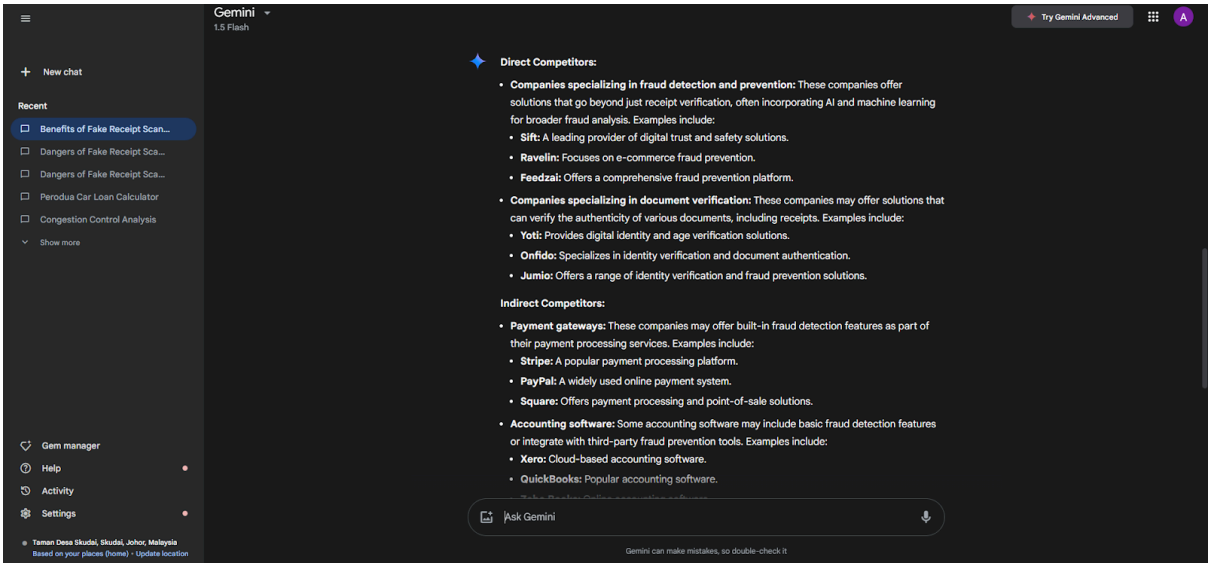

Figure 2: Screenshot Generative AI Competitors for Scanner for Fake Online Payment Receipts

URL: https://g.co/gemini/share/6b49f5e5b1e6

Screenshot

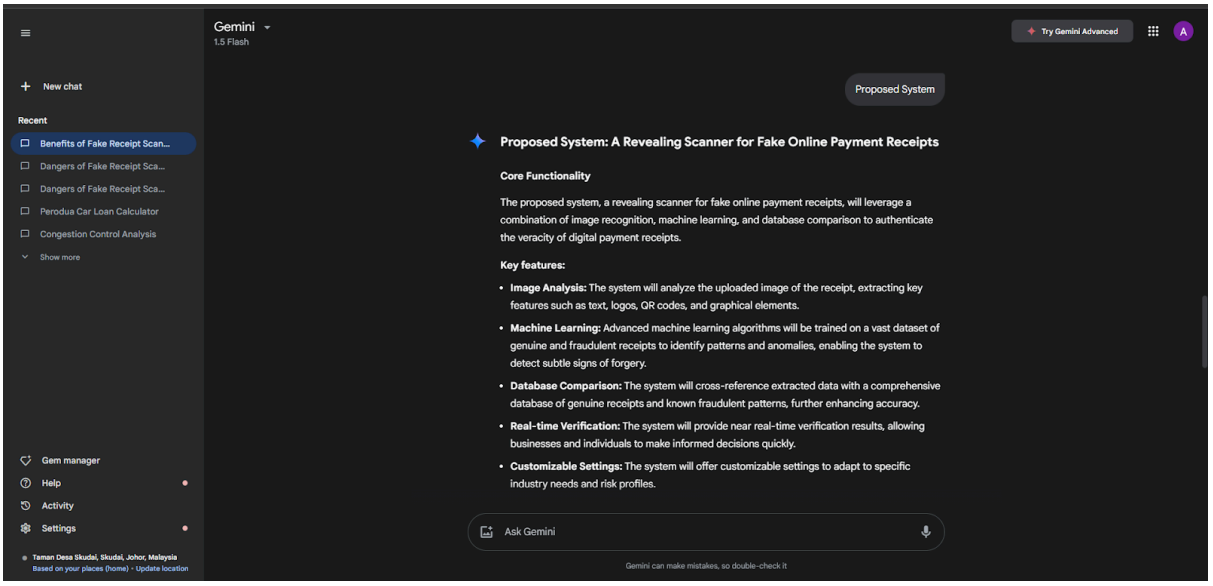

Figure 3: Screenshot Generative AI Proposed system for Scanner for Fake Online Payment Receipts

URL: https://g.co/gemini/share/a395d3086068