الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يونيبرسيتي إسلام انتارابغسا مليسيا
Garden of Knowledge and Virtue

KULLIYYAH OF INFORMATION AND COMMUNICATION TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

FINAL YEAR PROGRESS REPORT

PROJECT ID

1551 SD

PROJECT TITLE

Speech-to-Text Based Scam Call Detection Using Automated Analysis

STUDENT(S)

1. MUHAMMAD AMIR ZARIEFF BIN JEFNEE (2216919)
2. MUHAMMAD AFIF BIN HUSNAN (2212583)

SUPERVISOR

ASSOC. PROF. NORSAREMAH SALLEH

JANUARY 2024
SEMESTER 1 2024/2025

FINAL YEAR PROGRESS REPORT

PROJECT ID

1551 SD

PROJECT TITLE

Speech-to-Text Based Scam Call Detection Using Automated Analysis

PROJECT CATEGORY

System Development

BY

1. MUHAMMAD AMIR ZARIEFF BIN JEFNEE (2216919)
2. MUHAMMAD AFIF BIN HUSNAN (2212583)

SUPERVISED BY

ASSOC. PROF. NORSAREMAH SALLEH

In partial fulfillment of the requirement for the
Bachelor of Computer Science

Kuliyyah of Information and Communication Technology
International Islamic University Malaysia

ABSTRACT

Scam calls have become an everyday nuisance and a serious threat, affecting people and organizations on many levels from financial losses to breaches of privacy and emotional toll. Traditional scam detection methods, which often depend on caller ID metadata and static blacklists, are no longer sufficient in an age where scammers continually evolve their strategies. This project proposes a smarter, more adaptive solution: a system that uses speech-to-text technology in combination with machine learning to listen to what's actually being said on the call. By transcribing calls in real time and applying a hybrid CNN-LSTM model to analyze the text, our system aims to detect scam-related language patterns with high accuracy and speed. Ultimately, this project contributes to a safer communication environment, where technology understands context not just numbers.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

API	Application Programming Interface
CNN	Convolutional Neural Network
CSS	Cascading Style Sheets
FTC	Federal Trade Commission
FYP	Final Year Project
GPU	Graphics Processing Unit
HTML	HyperText Markup Language
LSTM	Long Short-Term Memory
ML	Machine Learning
NLP	Natural Language Processing
OEM	Original Equipment Manufacturer
SDG	Sustainable Development Goals
SMOTE	Synthetic Minority Over-sampling Technique
UI	User Interface

CHAPTER ONE
INTRODUCTION (System Development Project)

1.1 Background of the Study

In recent years, telecommunication fraud, in particular, scam calls, has become an increasingly important problem. They are another type of scam in which fraudsters try to deceive people or companies in sharing personal information bank account information, password, social security numbers. The impacts of recipients' being scammed include financial loss and emotional harm, and victims toils under a heavy emotional burden and multibillion-dollar financial loss.Indeed, scam calls are now considered one of the world's largest financial frauds. The Federal Trade Commission (FTC) reportedly gets hundreds of thousands of complaints each year, with a significant portion of them accusing telephony fraud (Ma et al., 2025).

These scams have evolved over time, from simple robocalls to more-powerful social engineering ploys, where con artists convince their victims to send money or share personal information. And the fraudsters don't just use voice disguise, often they pretend to representing trusted companies banks, tax authorities, power companies and the like building a rapport and emotional bond, and so they are able to manipulate the victim better. This maturation has seen the detection of such scam become ever more challenging where traditional approaches adopted by the telco operators (e.g. the blacklisting of suspicious telephone numbers) and reliance on Caller ID information is no longer sufficient.

Today's scammers have a few tricks up their sleeves such as number spoofing, which changes the caller ID information to that of someone the recipient trusts. What's more, robo-calling is predicated upon widespread caller ID spoofing, meaning those receiving calls do not even realize they are being targeted. These tactics thwart the effectiveness of the standard fraud detection systems that are limited to the metadata alone (manifested through attributes such as the phone number or the caller location). Consequently, the demand for a content-based scam detection system is rising that reaches beyond the scope of who is calling to what is being said in the conversation. To address this problem differently, both speech recognition and machine learning techniques have gained attention to detect the scam. By listening to spoken language in a phone call, systems can identify language patterns indicative of scams, which often include overly commercial phrases like “free prizes,” “urgent financial help,” or “limited-time offers.” These are the sorts of phrases often employed by scammers, to try to make their would-be victims feel pressured or anxious. Using Natural Language Processing(NLP), deep learning and speech-to-text technologies, this initiative is trying to produce a solution to listen to what is being said in the conversation while also recognising if the call is a scam or genuine.

Speech recognition has made significant breakthroughs over the past few years with models, such as Mozilla DeepSpeech, showing impressive results in transcribing speech to text with high accuracy, even when the speech is noisy or spoken with an accent(Negrão & Domingues, 2021). The next logical step in improving scam call detection lies in the integration of machine learning models such as CNNs (Convolutional Neural Networks) for feature extraction and LSTMs (Long Short-Term Memory networks) for sequence prediction. While simultaneously recording the conversation’s context and flow, this hybrid technique aids in the detection of scam-related terms. In order to present a more dependable and flexible technique for detecting scam calls, this research will concentrate on content-based analysis instead of only caller metadata.

1.2 Problem Statement

Traditional metadata-based scam call detection systems have a lot of drawbacks. Caller ID data is the main source of information used by these systems, which flag and block recognized scam numbers. However, this strategy is losing effectiveness since fraudsters have adapted a number of techniques to mimic real phone numbers and spoof caller IDs, making it challenging to rely on number-based identification

Furthermore, social engineering techniques in scam calls entrail tricking the victim into divulging private information or completing fraudulent transactions. These strategies frequently entail intricate discussions in which the con artist establishes credibility and applies pressure to the victim by instilling a sense of urgency. Because of this, it is impractical to detect using only information, including the phone number, location, or duration of the conversation. Since scammers sometimes employ certain linguistic patterns intended to deceive the victim, the conversation’s content itself is a considerably more potent signal of fraud.

The context of these increasingly sophisticated scam techniques is beyond the scope of current technologies that only depends on number-based detection. Numerous reputable businesses (including banks and government agencies) also call people, which is frequently detected by metadata-based algorithms as a false positive. A real-time, content-based scam detection system that can identify fraudulent activities by examining the spoken content of a conversation is therefore desperately needed.

By concentrating on the language characteristics and contextual interactions inside the discourse itself. The suggested method would overcome this difficulty. Utilizing cutting-edge machine learning models like CNNs and LSTMs and voice recognition technologies like Mozilla DeepSpeech, the system would offer a more dependable, flexible, scalable fraud detection solution. This strategy allows for real-time fraud identification, which is essential for reducing the impact of scam calls on victims, in contrast to current approaches that mostly depend on metadata.

1.3 Project Objectives

The main obstacle to detecting scam calls is that fraud strategies are always changing. Traditional detection systems based on metadata are becoming outdated as scammers employ voice disguise, social engineering and number spoofing tactics more often. Furthermore, it might be difficult to detect scam calls in real time without compromising processing performance, particularly when handling big amounts of data.

The following are the project’s particular goal:

1. To create a reliable pipeline for speech-to-text: The initial goal is to use cutting-edge voice recognition technology to turn call audio into text. Real-time transcription of spoken language has shown potential thanks to technologies like MOzilla DeepSpeech(Negrão & Domingues, 2021).The technique allows machine learning algorithms to efficiently assess the information by transcribing the discussion.

2. To build a CNN-LSTM hybrid model: A hybrid machine learning model will be developed by merging Long-Short-Term-Memory (LSTM) networks to capture long-term dependencies in the discussion with Convolutional Neural Networks (CNN) to extract localized information from the text (like terms connected to scams). The hybrid model's capacity to distinguish between genuine and fraudulent calls based on linguistic content will be evaluated once it has been trained on datasets of scam calls.

3. To solve datasets limitations: Since legitimate calls usually outnumber scam calls, dataset imbalance is a major issue in fraud detection. To counteract this, methods such as data augmentation and SMOTE(Synthetic Minority Over-sampling Technique) will be employed to guarantee that the system is trained on a balanced dataset (Bharati & Podder, 2020).

4. To enhance the system's performance in real time: Reducing the harm caused by scam calls requires real-time fraud detection. When a scam call is identified, notifications may be sent instantly since the system will be tuned to analyze live audio feeds with the least amount of delay.

5. To enhance model precision consistently: Machine learning algorithms will perpetually learn from fresh call data, adjusting to new scam methods and boosting the system's ability to detect scams as time progresses. The system's adaptive characteristics render it a sustainable answer to the ongoing challenge of scam calls.

At the heart of this project lies machine learning. The system will utilize extensive amounts of labeled data to develop models capable of differentiating between fraudulent and genuine calls, enhancing over time and adjusting to emerging types of scam activities.

1.4 Scope of the Project

1.4.1 Scope

This project focuses on creating a system for detecting scam calls that converts speech to text and can access the content of phone conversations. The main aim of the system will be to convert spoken audio into written text and utilize machine learning algorithms to determine if the content is authentic or possibly deceptive. The focus is limited to content-based detection, and methods such as caller ID tracking, biometric authentication, and other fraud techniques are excluded from this study.

1.4.2 Target Audience

The system mainly focuses on telecommunication companies, cybersecurity solution creators, mobile application developers, and digital fraud prevention teams. The system could also assist end-users looking for enhanced scam filtering features on their personal devices. Integrating real-time scam detection capabilities into mobile applications or telecommunications system enables users to receive instant notifications about possible fraud.

1.4.3 Specific Platform

The system will be created with the Python programming language and Mozilla DeepSpeech will be employed for converting speech to text. The deep learning model will be developed with TensorFlow and Keras, which are among the most commonly utilized frameworks for machine learning. The first prototype will be created for a desktop setting, although later iterations might enable integration with mobile devices or cloud service, enhancing scalability and adaptability.

1.5 Constraints

The Speech-to-Text-Based Scam Call Detection System has a lot of possibilities for solving the scam calls problem, but its development and implementation must be taken into account for a number of limitations.

1.5.1 Availability of High-Quality, Annotated Datasets

The availability of high-quality datasets is one of the main obstacles to creating an efficient machine learning-based scam call detection system. The majority of scam detection datasets that are made publicly available are often either too small, inadequately labeled, or do not accurately reflect the variety of scam tactics that are employed in actual situations. A strong collection of scam call audio transcriptions can be found in the TeleAntiFraud-28k dataset (Ma et al.,2025), for example. However, the types of scams that are represented in this dataset are significantly out of balance, with some categories (e.g., lottery scams) being overrepresented in comparison to others (e.g., fraudulent technical support calls). Additionally, real-world datasets frequently contain a lot of noise (e.g., such as background chatter and overlapping speech), which might impair the precision of the classification models and speech-to-text engine.

The difficulty of manually labeling vast volumes of audio data, which is expensive and time-consuming, exacerbates the issue of annotated data scarcity. Techniques like data augmentation and synthetic data creation (e.g., SMOTE) are used to artificially expand the training set in order to address this problem. Even these techniques, though, have the drawback of occasionally failing to capture the intricacy of scam call situations in the real world.

1.5.2 Computational Demands in Real-Time Processing

The computing needs required to collect and interpret voice data in real-time represent another limitation. High processing power is needed for real-time audio to text transcription, feature extraction, and classification, particularly for large- scale applications like contact centers or telecommunication networks. Incoming calls must be processed rapidly by the system in order to provide real-time detection without adding delay that can degrade user experience.

Significant CPU and GPU resources are needed for the speech-to-text translation process itself, particularly when dealing with big datasets and loud situations. In order to minimize false positives or negatives and ensure timely detection, the system must strike a balance between processing speed and accuracy.

1.5.3 Dependence on Third-Party APIs for Speech Recognition

The use of third-party voice recognition APIs (e.g., Google voice-to-Text and Mozilla DeepSpeech) raises a number of possible issues with accuracy, latency, and usage limits. These third-party services might not function as well in the specific field of scam call identification because they are usually made for general-purpose applications. For example, commercial APIs might not be able to manage problems with accents, dialects, or background noise in scam calls. Additionally, heavy traffic or cloud service limits may cause these system's performance to deteriorate, increasing latency or causing service interruptions.

Furthermore, since the audio data needs to be sent to a third-party servers for processing, using third-party APIs presents privacy issues. This is especially important in applications related to telecommunications, where private client information may be used. It could be important to depend on locally deployed or self-hosted solutions for deployment in privacy-sensitive contexts in order to guarantee the security of user data.

1.6 Project Stages

There are five main steps in the methodical process of developing the Speech-to-Text-Based Scam Call Detection System. These phases aid in making sure that every system component has been thoroughly studied, put into practice, and tested. The following are the stages:

1.6.1 Literature Review and Exploration of Existing Technologies

A thorough literature analysis of previous studies on machine learning models, voice recognition software, adn scam call identification is part of the initial step. This involves determining the best machine learning models for examining scam-related conversational patterns and assessing several speech-to-text technologies such as Google Speech-to-Text and Mozilla DeepSpeech (Negrão & Domingues, 2021). This step lays the groundwork for creating a more reliable system by comprehending the limits that exist now.

1.6.2 Data Collection and Preprocessing

Data gathering from publicly accessible datasets, including TeleAntiFraud-28k and customer support call records, is the next step. These datasets undergo preprocessing, such as call segmentation, background noise reduction, and audio normalization, to guarantee their excellent quality. In order to transform unprocessed audio into clear, usable text for additional analysis, preprocessing is required. Furthermore, correctly classifying the data (i.e., scam vs. legitimate) is essential for model training (Ma et al., 2025).

1.6.3 System Development: Speech-to-Text Integration and Model Training

Integrating the machine learning model with the speech-to-text engine is the main goal of this step. After call audio is converted into text using the speech-to-text system (Mozilla DeepSpeech), the CNN-LSTM hybrid model processes the text. The preprocessed and tagged data is used to train the model, which optimizes it for fraud detection. While the LSTM layer records long-term dependencies in conversation context, the CNN layer extracts local information (such as words connected to scams).

1.6.4 Testing and Evaluation

The model is tested and evaluated once it has been trained. Key assessment criteria including accuracy, precision, recall, and F1-Score are used to evaluate the system’s performance. Testing in real time guarantees that the system functions in real-world scenarios, such as call center situations, finding places where the system might need to be modified for reduced latency or increased accuracy requires testing.

1.6.5 Documentation and Prototype Presentation

The last step involves compiling all of the analysis, methods, and outcomes into research project documentation. The system’s real-time scam call detection capabilities are shown through a prototype. To get input and make improvements, the system is also shown to stakeholders, such as cybersecurity specialists and telecom companies.

1.7 Significance of the Project

The initiative is important because it has the potential to significantly improve the reliability and security of modern telecommunications networks, which are essential to personal, commercial, and national digital infrastructures. Millions of individuals globally are affected by scam calls every year, often leading to financial loss, psychological trauma, and breaches of privacy. Existing metadata-based solutions, such as caller ID filters and static blocklists, are proving increasingly inadequate in handling the evolving nature of scam tactics. By shifting the emphasis toward the linguistic content of calls, this project proposes a proactive approach that analyzes the actual conversation in real time, enabling scam detection based on what is being said rather than just the number making the call. This move away from reliance on external data sources toward real-time semantic analysis introduces a more intelligent and context-aware mechanism for fraud prevention.

In addition to improving security, the use of machine learning provides an adaptive advantage. As scammers continue to change their techniques, the system can continually learn from new examples, expanding its detection capabilities automatically without constant human intervention. This automated adaptability allows the system to evolve alongside scam tactics, making it far more effective than traditional, manually updated blacklists. By intercepting scams before they succeed, the system helps reduce the financial burden on victims, while also minimizing the psychological stress caused by fraudulent interactions.

Importantly, this project's objectives and outcomes align closely with the United Nations Sustainable Development Goals (SDGs), particularly Goal 9: Industry, Innovation and Infrastructure and Goal 16: Peace, Justice and Strong Institutions. By contributing to the development of safer, more resilient telecommunication infrastructure, this project supports SDG 9, which promotes the building of reliable and sustainable technologies. Additionally, by helping prevent fraud and supporting secure communication systems, it advances SDG 16, which focuses on reducing exploitation, ensuring access to justice, and promoting the development of accountable institutions. The project also contributes indirectly to SDG 8: Decent Work and Economic Growth by helping safeguard users from financial fraud that could disrupt personal or business economic stability.

In practical terms, the system is designed to be scalable, accurate, and adaptable, making it suitable for integration into a variety of environments, including customer service centers, mobile applications, and national telecommunication infrastructure. By offering real-time detection and feedback, the system empowers users with immediate protection, giving them the confidence to engage in digital communications safely. As the technology advances, it holds the potential to become a critical component in global efforts to create secure digital e**nvironments**, directly contributing to broader digital trust and economic stability worldwide.

1.8 Summary

A thorough description of the suggested Speech-to-Text-Based Scam Call Detection System was given in this chapter. It described the history of telecom fraud, the issue of scam calls, and the project's goals and parameters. The limitations and difficulties of creating such a system were also covered, including the need for third-party APIs for voice recognition, the computing demands of real-time processing, and dataset restrictions.

The importance of the system was emphasized in the chapter, along with its ability to offer a proactive, content-based solution to identify fraudulent calls, a crucial problem in the telecom sector. The goal of this research is to provide a more efficient and flexible approach to fraud detection by eschewing metadata-based solutions and concentrating on the conversation's substance.

We will go into further detail about the methodological framework and technological background that will guide the creation of the suggested system in the upcoming chapters. In order to confirm the system's efficacy in identifying fraudulent calls, we will also investigate its assessment and practical testing.

CHAPTER TWO
REVIEW OF PREVIOUS WORK (System Development Project)

2.1 Introduction

Scam calls or phone fraud is a growing problem and has generated a lot of research interest from the academic community and commercial technology providers. This chapter provides an exhaustive review of the literature on scam call detection, speech-to-text technologies, and applications of machine learning to prevent fraud. In this review, I review and compare existing systems used, or in development to filter scam calls, their strengths and weaknesses, and applicability in the real world. Also, the chapter provides theoretical background, the technical foundations, and limitations of current systems which are the basis of the development of this project. By highlighting where existing systems have limitations, I provide a rationale underlying the need for a new content-based scam call detection system that can analyse phonemes, speech -to-text transcriptions, and features in real-time from Automatic Speech Recognition and Natural Language Processing systems.

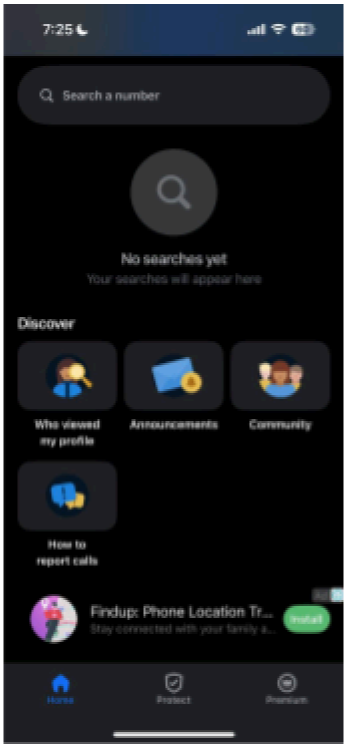
2.2 Overview of Related Systems

2.2.1 Truecaller

Truecaller, a global service firm, is one of the most notable tools in use to identify scam calls. The application offers caller ID services and spam call tracing. Truecaller has become an esteemed name in the world of smartphone-users for over ten years. Truecaller's main purpose is to assist in caller identification prior to answering by revealing who the caller is based on a crowd-sourced worldwide database. Truecaller uses a scam detection scheme that allows users to identify and report numbers they believe to be scams or spams. Knowing this is how Truecaller builds procedures for identifying scam calls.

Truecaller stands apart from other caller ID applications in that it relies on people. Millions of users around the world, everyday, share warnings about numbers, so it's not a static list. It's a live, constantly updated list of scam numbers. If a user has marked a number as probable spam, and many other users have certainly flagged that number as spam each time, Truecaller sends a warning to all other users around the world to be cautious when speaking to this caller. Truecaller also provides users with the ability to block calls from numbers that are identified as spam or fake, which will simply auto hang up on the caller.

Despite its large global network and ability to utilize real-time reporting, Truecaller has significant limitations. The main problem is its reliance on external metadata (the phone number) instead of the content of communications. When scammers use a valid number or regularly change their phone number, they will generally not be reported to Truecaller at all. Also, there is no part of the system that would perform semantic analysis or speech recognition, so if a scam happens and a user can't see the number, the user is not protected from the words of the scammer. This means Truecaller is reactive rather than proactive, depending upon reports filed after scams have occurred. Truecaller would be very useful to flagging and blocking known scam numbers, but it does not afford much or any protection from more elaborate scams companies who manipulate actions through speech while they are talking regardless of content.

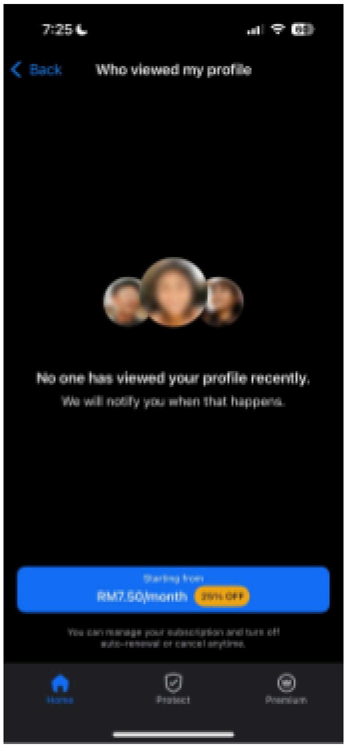


No searches yet

Your searches will appear here

Stay connected with your family a...

Figure 1 : Truecaller Home Page



No one has viewed your profile recently.

We will notify you when that happens.

You can manage your subscription and turn off auto-renewal or cancel anytime.

Figure 2 : Truecaller Who Viewed My Profile

Advantages of Truecaller

One of the key advantages of Truecaller is its global recognition and the size of its user community. By leveraging crowd-sourced data, Truecaller benefits from millions of users who actively report suspicious numbers on a daily basis. This creates a constantly evolving and dynamic database of scam numbers, making it highly effective at alerting users to widely recognized fraudulent callers. The platform also integrates seamlessly with smartphone devices, providing real-time caller identification before the user picks up the phone. Furthermore, Truecaller’s built-in spam blocking capabilities reduce the risk of users being exposed to known robocalls and scams, offering them a practical, user-friendly interface for managing and blocking unwanted numbers.

Disadvantages of Truecaller

Despite these strengths, Truecaller is limited by its dependence on phone number identification rather than conversation content. Scammers who frequently rotate or spoof phone numbers can often evade detection because the system relies heavily on prior reports from other users. This makes the detection process reactive, meaning that users are only protected against numbers that have already been flagged in the database. Additionally, Truecaller does not employ any form of speech recognition or natural language processing, meaning it cannot analyze the actual speech during a call. This leaves users vulnerable to scams that rely on sophisticated language manipulation, social engineering, or emotional persuasion techniques during the conversation itself.

Feature	Advantage	Disadvantage
Caller Identification	Provides real-time identification of unknown callers.	Cannot verify if a known caller is involved in scam activity.
Spam Number Reporting	Large, global, dynamic community reports new scam numbers constantly.	Relies entirely on user contributions for scam identification.
Scam Call Blocking	Allows users to block numbers already flagged as spam.	Ineffective against scammers using new or spoofed phone numbers.
Speech Analysis Capability	None	No content analysis of speech or conversation for scam detection.

Table 1: *Advantages And Disadvantages of Truecaller*

2.2.2 Hiya

Hiya is a widely used caller identification and spam call blocker. It is based in Seattle, USA, and has a goal of providing intelligent blocking of unwanted calls such as scam calls, spam calls, and robocalls. One advantage Hiya has over many competitors is that it works with major smartphone manufacturers and network providers, making it possible for users to have access to its features not only through stand-alone applications but also from the default dialer applications of some Android devices. Hiya will combine spam databases, intelligent algorithms, and user reports to provide real-time information on incoming calls.

A standout element of Hiya is its smart programs that can recognize abnormal calling patterns. These may be calls from numbers that may have previously flagged for scams, or short attention span calls that are continually repeated, signs of telemarketing or scam calls as well. In addition to these features Hiya offers great spam protection such as automated call blocking, reverse number lookups, and spam caller alerts. This provides users great tools to combat unwanted robocalls.

Hiya has a lot of nice features but exhibits the same issues as Truecaller. One is that Hiya can work well because it has a database of known scam numbers, yet new or fake numbers being used by scammers may not get detected right away. Even more, Hiya has no way to analyze speech or content. It does not record or analyze what is being said in the conversation shared between the receiver and caller. Because of this, Hiya cannot detect scams that are purely conversation fraud, including pretending to be a government agency or emotional conversation fraud. This means a new scam detection model will have to be created that listens to and processes spoken content, as this is still a fundamental weakness in Hiya's defense method.

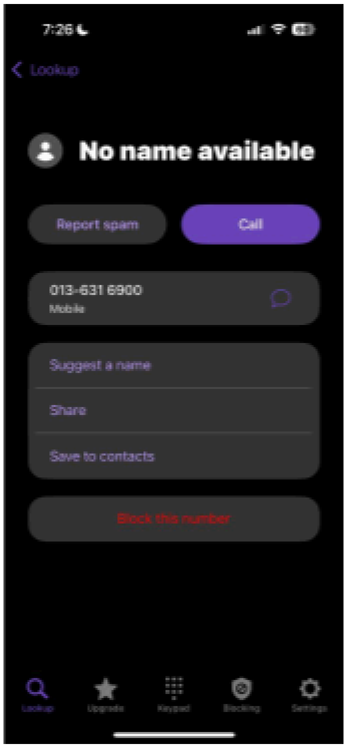
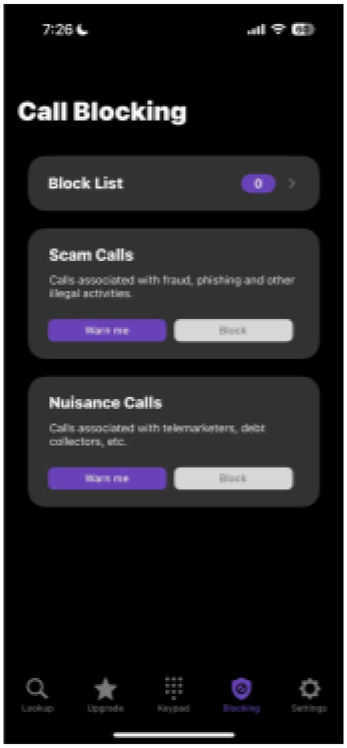


Figure 3 : *Hiya Searching For A Number To Block Page*



Calls associated with fraud, phishing and other illegal activities.

Calls associated with telemarketers, debt collectors, etc.

Figure 4 : *Hiya Call Blocking Number Calls Page*

Advantages of Hiya

Hiya brings several notable advantages to scam call protection, primarily through its use of predictive algorithms that go beyond static number lists. These algorithms analyze call patterns to predict whether an incoming call may be fraudulent, providing a more proactive line of defense compared to simple spam number reporting. Another strength of Hiya is its integration with mobile manufacturers and telecommunications networks, meaning that many users benefit from Hiya's protections without even having to download the standalone app. The seamless integration with device interfaces gives Hiya an advantage in terms of accessibility and convenience for everyday users. Additionally, the ability to automatically block identified spam calls helps minimize interruptions caused by nuisance calls.

Disadvantages of Hiya

Despite its predictive capabilities, Hiya still suffers from major disadvantages when dealing with conversational scams. Like Truecaller, Hiya's system is entirely dependent on external data such as phone numbers, call history, and behavioral patterns. If a scammer is using a newly generated or spoofed phone number, Hiya may fail to recognize it as a threat in time. More critically, Hiya does not include any mechanism for analyzing the content of a call. Without speech-to-text processing or linguistic analysis, the application is unable to detect scams that rely on voice manipulation or emotional pressure during a live conversation. This limitation renders Hiya ineffective against personalized scams that exploit trust or fear through conversation rather than easily detectable scam behaviors.

Feature	Advantage	Disadvantage
Caller Identification	Provides real-time caller identification integrated with OEMs.	Limited by the accuracy and scope of its database of known scam numbers.
Predictive Algorithms	Detects suspicious call patterns and origins.	Cannot identify scams that rely solely on spoken manipulation.
Spam Call Blocking	Automatically blocks known spam and robocalls.	Vulnerable to scammers using newly generated or spoofed numbers.
Speech Analysis Capability	None	No analysis of speech or conversation content for scam detection.

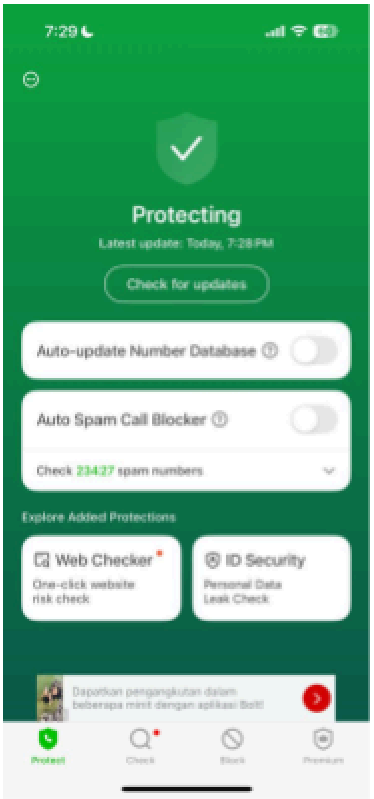
Table 2: *Advantages And Disadvantages of Hiya*

2.2.3 Whoscall

Whoscall, a product of Gogolook from Taiwan, is another strong player in the area of call identification and spam call protection. Growing in popularity throughout Asia, including Malaysia, Whoscall implements great caller ID features and a growing spam database to provide real-time call filtering and blocking. Unlike the Western-centric alternatives, Whoscall clearly focuses on the Asian market giving it more regionally specific relevance for users in Malaysia and neighboring countries. Users can use Whoscall to quickly identify unknown callers, block malicious calls, and even use an offline database to identify a caller if internet service is not available.

Whoscall has established itself as a necessary tool in regions emerging from the pandemic not only with aggressive scam calls but also aggressive telemarketing. With a large user base in Asia, each actively contributes to the spam reporting database, and local scam numbers can often be identified in a matter of hours before they reach widespread regional popularity. Whoscall gets support in spam reporting and caller identification from partnerships with regional telecommunication providers. Whoscall is especially helpful in areas with poor or non-existent internet access because it utilizes an offline spam protection database, which allows users to still benefit from spam protection even when they are not online.

Yet, Whoscall, along with similar services such as Truecaller and Hiya, are not equipped to address scams that rely on sophisticated conversational manipulation. The system is inherently dependent on identifying phone numbers (not analyzing phone conversations). So if the scammers used new, unregistered or even personal numbers, and the calls relied on emotionally manipulative language, Whoscall has insufficient capabilities to protect against scams. Having no built-in speech-to-text analysis, or conversational pattern analysis capabilities shows a significant limitation of Whoscall and further justifies a need for scam-detection tools that allow for content-based analysis of speech, while it is occurring.



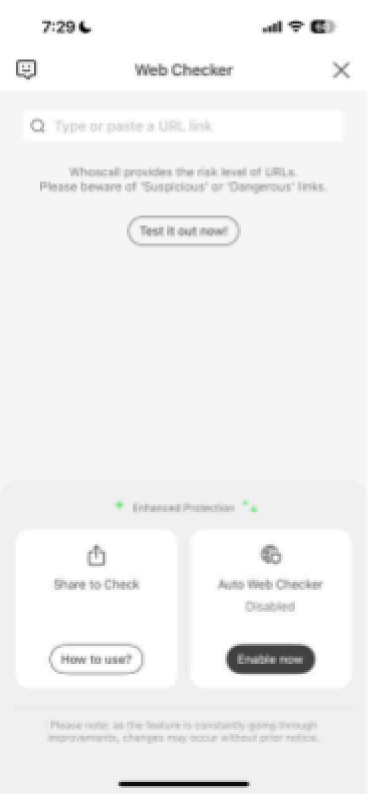
Auto-update Number Database ○

Auto Spam Call Blocker ○

Check 23427 spam numbers

Dapatkan pengangkutan dalam beberapa minit dengan aplikasi Bolt!

Figure 5 : Whoscall Home Page



Whoscall provides the risk level of URLs.
Please beware of 'Suspicious' or 'Dangerous' links.

Auto Web Checker: Disabled

Please note: as the feature is constantly going through improvements, changes may occur without prior notice.

Figure 6 : Whoscall Web Checker Page

Advantages of Whoscall

Whoscall offers unique advantages, particularly in regions like Asia and Malaysia, where its localized spam detection capabilities are more refined than many international alternatives. One of its most significant strengths is the inclusion of an offline caller identification database. This allows users to receive information about suspicious numbers even without an internet connection, making it especially valuable in areas with unstable or intermittent network coverage. Whoscall also benefits from strong partnerships with regional telecommunication providers, enhancing its ability to detect and block numbers associated with scams or fraudulent activities in specific local contexts. These features make Whoscall an excellent choice for users seeking localized spam protection tailored to their geographical region.

Disadvantages of Whoscall

While Whoscall excels in regional relevance, it faces the same critical weakness as both Truecaller and Hiya: an inability to analyze speech content during calls. Its scam detection system is built entirely on identifying known scam numbers through community reporting and provider partnerships. If a scammer uses a new or unlisted number, Whoscall is powerless to protect the user from potential fraud during the call. Furthermore, it does not feature real-time transcription or content analysis, making it ineffective against scams that rely on persuasive speech or social engineering tactics. This gap highlights why a speech-based, real-time scam detection system is essential for providing users with a more comprehensive layer of security.

Feature	Advantage	Disadvantage
Caller Identification	Offers regionally relevant spam identification, especially in Asia.	Relies on user reports and telecommunication provider partnerships.
Offline Database	Enables caller ID lookups without internet access.	Cannot detect scams that rely on new or unregistered numbers.
Spam Call Blocking	Blocks known spam and scam calls reported by the community.	Does not include speech recognition or conversational analysis features.
Speech Analysis Capability	None	Lacks the ability to transcribe or analyze speech content in real time.

Table 3: *Advantages And Disadvantages of Hiya*

2.3 Discussion

Feature / Platform	Truecaller	Hiya	Whoscall
Caller Identification	✓	✓	✓
Spam Number Reporting	✓	✓	✓
Predictive Algorithms	✗	✓	✗
Offline Database	✗	✗	✓
Spam Call Blocking	✓	✓	✓
Speech Analysis Capability	✗	✗	✗
Real-Time Speech Analysis	✗	✗	✗
Supports Regionally Relevant Data	✗	✗	✓

Table 4 : *Summary of All Disadvantages*

A comprehensive review of current systems designed for detecting scam calls like Truecaller, Hiya, and Whoscall indicates an accepted and large limitation in their overall efficacy: content-based detection is absent from these systems. Each of these systems is focused on detecting possible or potential scam calls based on the external descriptors of the call, mainly the scam call's phone number and the user-reported reputation of the number. Such reliance on external metadata is a major weakness especially in light of sophisticated scam schemes which leverage caller ID spoofing tactics, as well as the use of many different new and unregistered phone numbers. All of these tactics lead to the inherently poor reliability of number-based systems as such systems will generally not be able to detect threats that are not included at the point of sale database, to date no other users have reported as part of their scam and scam detection experience. Furthermore the gap becomes wider (titanically) because many scam operations co-opt psychological manipulation and emotional coercion and subsequent victim actions that exist during the call itself (as part of the overall scam operation), meaning that the actual content of the call is the best indication of intent to defraud.

While Truecaller does have the potential to capitalize on its vast global user community to warn of spam in real-time, it does not analyze or influence spoken words. It takes a reactive approach to warning users after many have identified the same number as "suspicious". Hiya does introduce an aspect of predictive analytics by assessing calling behavior and patterns to try and improve "real-time" spam detection, but again only gets ahead of the scammer's methods when they are unchanged and not solely based on real-time speech manipulation. Similarly, Whoscall only provides coverage in regions, such as Asian countries such as Malaysia, but is better at leveraging its offline database functionality which again offers little to no protection from new and emergent scam calls that use unregistered or unknown numbers. Even these SMS or app-based systems never set out to protect against any scams that occur inside the calling environment, including the linguistic scams using both deception and social engineering, or the emotional exploitation of victims.

The changes in scam strategies show how necessary it is to analyze the actual language based on the conversation. Most scams will utilize a language to build trust with the victim by using formal greetings and deposits, like creating a friendly tone, emotional blackmail tactics, formal pleasantries first, and can escalate up to asking for personal information or transfer money. Relying on the identification of the number isn't enough anymore because scam caller schemes have changed to actively exploit this vulnerability. Thinking about the process of who is calling as opposed to what is being said is necessary when mentioning scanners. If systems focus on phonetic analysis of spoken content, it can make a proactive tool rather than reactive defenses that only have the capacity to catch at-risk known scammers.

This is where natural language processing (NLP) and machine learning models, primarily in the form of a hybrid in the form of a Convolutional Neural Network (CNN) and a Long Short Term Memory (LSTM), can make a difference. CNNs focus on local patterns, and can ultimately provide localized pattern recognition intended to identify a specific word or suspicious phrase concerning a scam. On a completely different end of the spectrum, LSTMs will recognize the lexical sequence of words, and help with determining patterns in regard to deceiving conversations, even if those conversations may ultimately seem innocent. Taking advantage of LLMs, recent developments have proven great advances in contextual understanding of human speech. For example, detecting small visual signs of a scam during a live call is now possible. Moreover, when these models are used with effective speech to text engines, such as Mozilla DeepSpeech, it is conceivable to identify a scam conversation on the fly, as LSTMs have advanced enough to combine the poor usages of number identification.

In conclusion, the review of the various existing systems has identified an important technological gap in their scam call detection processes. Truecaller, Hiya, and Whoscall offer acceptable first lines of defense against the filtering of known scam telephone numbers, but they do not offer protection against mobile voice-based dynamic scams. Addressing the technological gap of integrating speech to text processing in real-time with NLP algorithms that offer conversational analysis and the ability to make predictive classifications of scam behaviour, is the main purpose of this project and will mark an advancement in the ongoing war against telephone fraud.

2.4 Summary

In summary, we have investigated the systems in place to counter scam calls, specifically Truecaller, Hiya and Whoscall, in this chapter. Each has individual components that are useful, such as real-time caller identification, predictive analysis and spam reporting through community feedback, that are found to protect users from common scams. While these systems will provide this protection they all have one significant limitation; the collection and use of only numbers, and integrating information from external databases for the purposes of making decisions about scams, that they do not include forms of speech content analysis, thus in this way they are all useless against scams perpetrated through the use of language manipulation or social engineering through a conversation.

The investigation also demonstrates how today's scams have developed from the means in which number-based detection systems can recognize. With the rapid advancement of scam techniques, particularly scams that involve personalized communications from scammers pretending to be representatives of legitimate agencies, there is a necessity for a more advanced detection system that can inform a user about verbal cues through a conversation. There is a significant transition occurring from former systems to new systems that use the combination of speech-to-text technology and machine learning to offer new capabilities in the detection of scam calls allowing for real-time screening of the language used while on a call regardless of how that call is initiated or through which number it was received.

This project, focused on content analysis of speech, addresses the particular shortcomings of current systems and offers a new contribution to issues raised by all types of modern scam activity. By utilizing a content based approach, the existing systems are either better served or supplemented by a defense architecture, offering proactive, intelligent scam detection as calls happen in real-time. The limitations identified in this chapter suggest that any new generation of scam detection systems should be based on enhanced NLP, speech recognition and adaptive machine learning models. In the next chapter, we will be explicit about the process and methodology we adopted to devise and build such a system, its structure, development and technical elements.

CHAPTER THREE
METHODOLOGY (System Development Project)

3.1 Introduction

All systems are created by developing them over time, and as one goes through the system development process -- especially one as technically challenging as a scam call detection platform -- it is essential to have advanced thinking, consistent practice, and incremental change throughout the system's life. The methodology selected for this project is designed to confirm that all stages of development will support the intended application of creating a scam call detection system that is highly accurate, efficient and user-friendly. There are many aspects involved in developing a system that integrates speech-to-text processing with machine learning for natural language understanding. This requires the merging of various fields within computer science, including speech recognition, artificial intelligence, software engineering, and user interface. In addition, having to develop real-time applications for scam detection is complicated in itself, requiring consideration of trade-offs like speed, computational load and accuracy.

A critical consideration informing the choice of methodology for this project is the changing and unpredictable nature of telephone scams. Scammers are constantly improving their schemes, therefore any prescribed or regulated development model would not be able to represent these dynamically changing threats. Given this need for flexibility and adaptability it has been decided to use Agile Software Development Methodology as a framework, which breaks the project into smaller functional cycles (iterations or sprints). Each iteration delivers a functional increment of the system that the development team can use to test, refine, and improve the components of the scam detection pipeline. This will also enable the development team to use feedback cycles to perform regular reviews and make incremental adjustments to the system, enabling the project to adapt to new challenges and respond to any needs for change along the way.

The methodology presented in this chapter sits as a foundation upon which the entire development process rests, guaranteeing that all technical decisions such as relying on hybrid CNN-LSTM models, deploying speech-to-text transcription engines, and putting in place database systems for data persistence are properly planned, tested for every conceivable situation, and validated before the eventual deployment stage. The stepwise procedures enumerated herein for system building take into account requirement gathering, iterative design, overall system architecture planning, module implementation, testing phases, and preparation for deployment. By adopting such an adaptable yet formalized methodology, the team working on development shall output a solution which is able to satisfy the essential goal of detecting scam calls through real-time analysis of the spoken content.

3.2 Development Approach

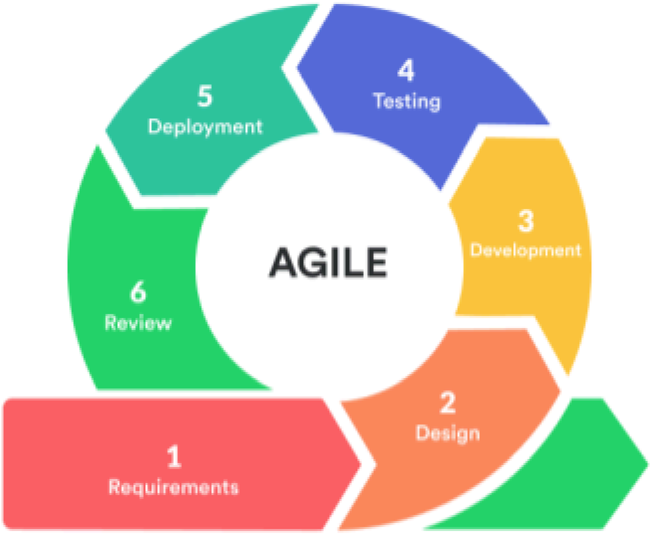


***Figure 7 :** Agile Software Development*

The Agile Software Development Methodology serves as the guiding approach for executing this project successfully. The Agile approach matches perfectly with projects that need flexible development and continuous feedback and iterative improvements because these elements are essential for machine learning and speech processing system development. The scam call detection system follows a phased development approach which starts with basic prototypes before advancing to more refined models. Through Agile methodology developers receive ongoing evaluation and review processes that enable them to enhance the system's functionality and accuracy and usability throughout development. The Agile process in this project includes six essential stages which begin with requirement analysis followed by system design and system development and then system testing and deployment and conclude with review.

The Agile process begins with the Requirement Analysis Phase which centers on identifying and collecting the precise requirements of the system. The system requirements definition process determines system functionality and user identification and technical requirements that will guide development work. The requirement analysis includes research into existing scam detection technologies to understand their weaknesses and develop strategies for improvement through speech-to-text and machine learning integration. The project vision takes shape through user feedback and supervisor consultation during this initial stage.

Next, we have the Design Phase, during which the general architecture or blueprint of the scam call detection system is planned. This very much entails designing architectural diagrams, conceptual models, data flow diagrams, and wireframes for the user interface. During this design phase, the intent is to create a design for the interaction of all major components such as the speech-to-text engine, the CNN-LSTM classifier, and the data storage system. Having a concrete design phase minimizes confusion during the implementation phase while providing a foundation for the developers to stand on.

The moment the design phase is finished comes the start of the Development Phase in which the system is constructed module by-module. First, the speech-to-text conversion component is implemented using Mozilla DeepSpeech, then the hybrid CNN-LSTM machine-learning model is developed and trained. During this phase, cleaning, labeling, and processing of raw call recordings datasets take place so that the machine-learning model will have quality input for training. Coding is then performed iteratively; that is to say that there are several coding-test-refine cycles of coding features to ensure continual refinement of the system.

The project is then subjected to the Test Phase, wherein various types of testing are performed for the assessment of both components and the overall system. Unit testing checks whether each module, that is, the transcription engine, the machine learning classifier, performs its function correctly. Integration testing follows, assuring that the different modules do indeed integrate into a working system. System testing then ensures that the entire system works, including the user interface-the users should be able to upload/process audio files for scam prediction. During this Testing Phase, the system is also subjected to stresses to see how it behaves with regard to speed and accuracy as well as resource consumption. Those areas, if any, that bottleneck the system or otherwise adversely affect its real-time usability would be flagged.

The next stage is the Deployment Phase, in which the fully tested software system is prepared to be operationally used. In this phase, the prototype will be packaged and installed on a specified environment for demonstration or trial use. The deployment phase also consists of backend services, such as setting up the database system that will be used to store the transcripts and predictions. If possible, relevant documentation is produced to assist in operating the software. The documentation, as appropriate, considers technical users, as well as normal users, and what features will be available in the platform for use.

The last phase in the Agile process is called the Review Phase, where feedback is collected from managers, reviewers, or test users. The feedback is analyzed thoroughly for searching out areas that need more improvement or new features that would be beneficial for future development. Because Agile is iterative, deployment does not signal the end of development but rather initiates a cycle of improvement, testing, and deployment as needed. With Agile methodology, the process of development is kept open to change, flexible, and responsive to altering requirements throughout the project's life cycle.

3.3 Requirements Specification

The process of gathering requirements for this scam call detection system involved multiple structured methods to ensure the system's design meets both academic expectations and real-world needs. The primary method used was continuous consultation with the project supervisor, who provided expert guidance regarding software engineering practices and the technical feasibility of various features. These consultations were essential for refining the project scope, identifying key system functionalities, and ensuring alignment with the expected outcomes for a final-year project. In addition to supervisor guidance, extensive literature reviews were conducted to analyze both academic publications and technical resources related to scam call detection, speech recognition systems, and machine learning applications in fraud prevention. These resources provided critical insights into the strengths and limitations of existing systems like Truecaller, Hiya, and Whoscall, allowing for the identification of specific weaknesses that this project aimed to improve, particularly the lack of content-based analysis. Informal interviews were also held with potential users, particularly individuals who had previously experienced scam calls. These informal conversations provided valuable practical feedback, helping to refine the system's feature set to ensure it addresses the actual pain points faced by users, such as real-time alerts and clarity of scam warnings. Together, these methods provided a complete and reliable set of requirements to guide the system's development.

The **functional requirements** define the core activities that the scam call detection system must be able to perform to fulfill its objectives:

1. The system must provide the capability to accept audio input from users. This can be in the form of uploading recorded phone calls in standard audio file formats. This functionality is essential because it forms the starting point of the entire scam detection process by supplying raw speech data for analysis.

2. The system must process the uploaded audio using a speech-to-text engine to convert spoken words into text. This transcription step is crucial because the machine learning model relies on textual data to perform scam detection analysis.

3. The system must classify the transcribed text using a machine learning model,

specifically a hybrid CNN-LSTM architecture. This model will analyze the linguistic content of the call to determine whether it matches known patterns of scam speech or conversational tactics commonly used by scammers.

4. The system must display the result of the analysis to the user. This output should include a clear indicator of whether the call is predicted to be legitimate or potentially a scam, as well as a confidence score showing the probability or certainty of that prediction.

The **non-functional requirements** describe how the system should behave to provide a reliable, user-friendly experience and support practical usage in real-world scenarios:

1. The system must be able to process and analyze uploaded calls quickly enough to provide feedback before a scammer is able to fully manipulate or deceive the user. The aim is to minimize system delays to support near real-time feedback.

2. The machine learning model must be trained thoroughly to differentiate between normal conversational speech and potentially fraudulent language, minimizing false positives and false negatives to maintain user trust in the system's output.

3. The system must function consistently, without crashing or producing errors, even when multiple files are uploaded or longer audio recordings are analyzed. It should handle unexpected inputs gracefully without system failure.

4. Given that users may upload personal or sensitive conversations, the system must ensure that all audio and transcription data is stored securely, processed responsibly, and protected from unauthorized access or misuse.

5. The system should be designed in a modular manner to allow for future upgrades, such as live audio stream analysis, multilingual support, or deployment to mobile and cloud platforms.

3.4 Logical Design

3.4.1 System Analysis And Design Diagram

3.4.1.1 System Architecture Design

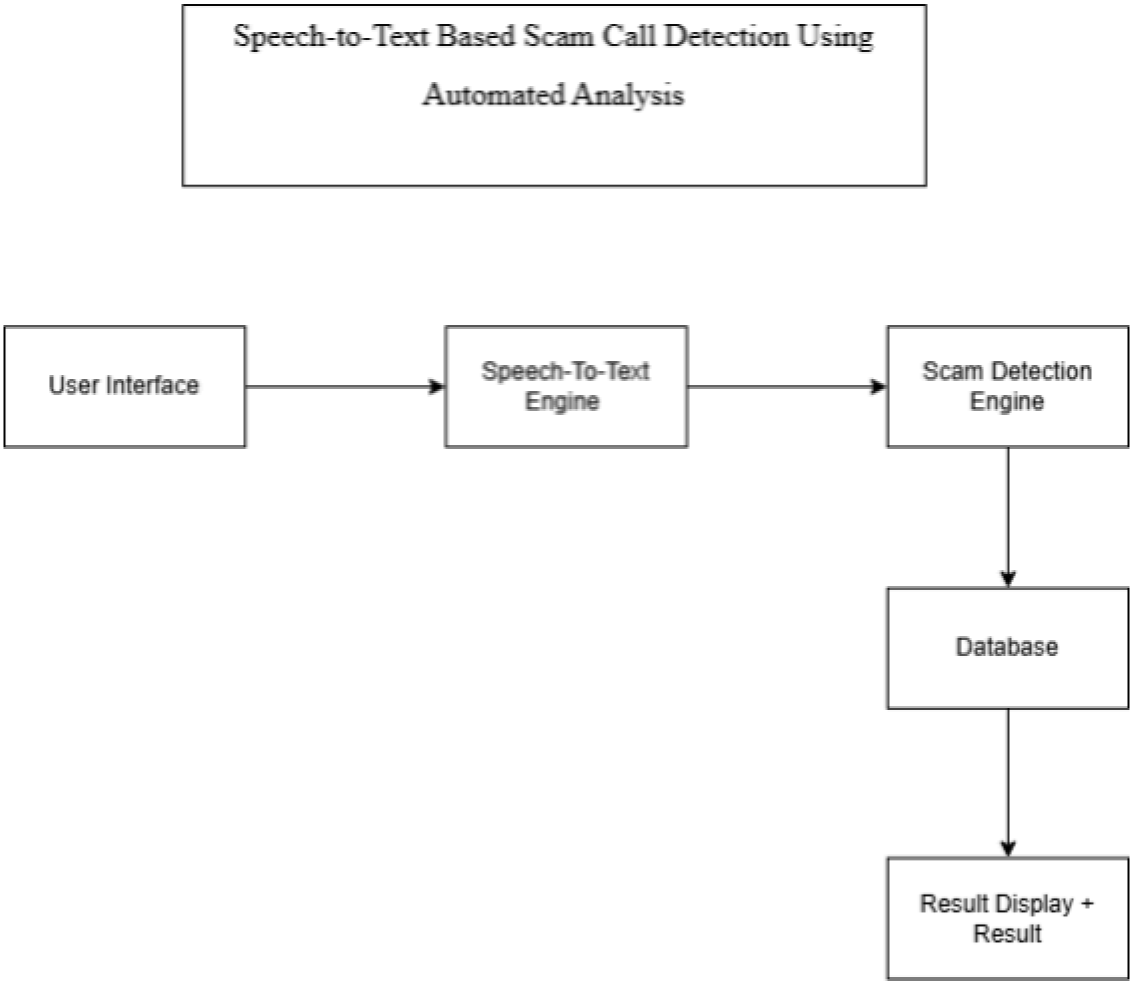


Figure 8 : *System Architecture Design*

3.4.1.2 Flowchart

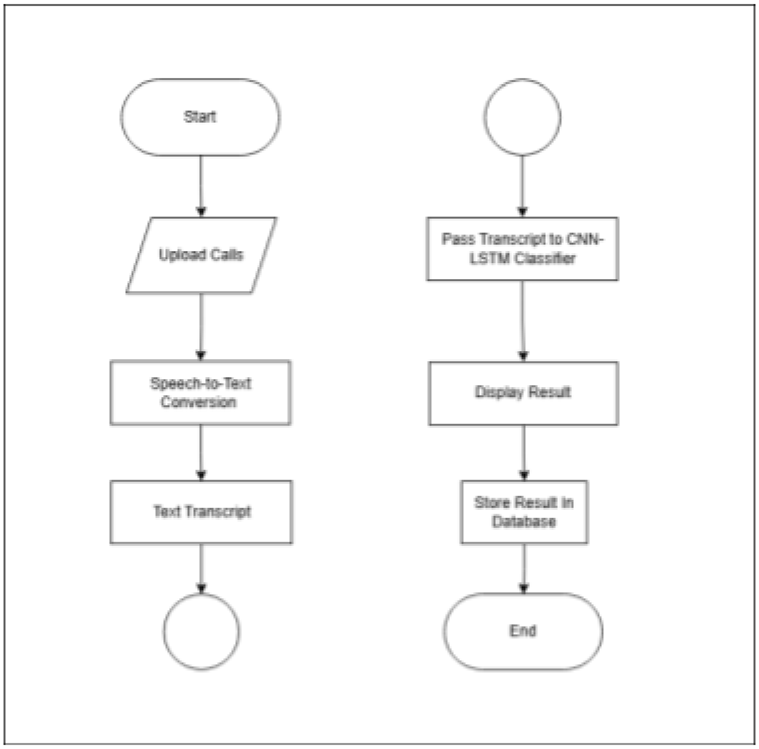


Figure 9 : *Flowchart*

3.4.1.3 Use Case Diagram

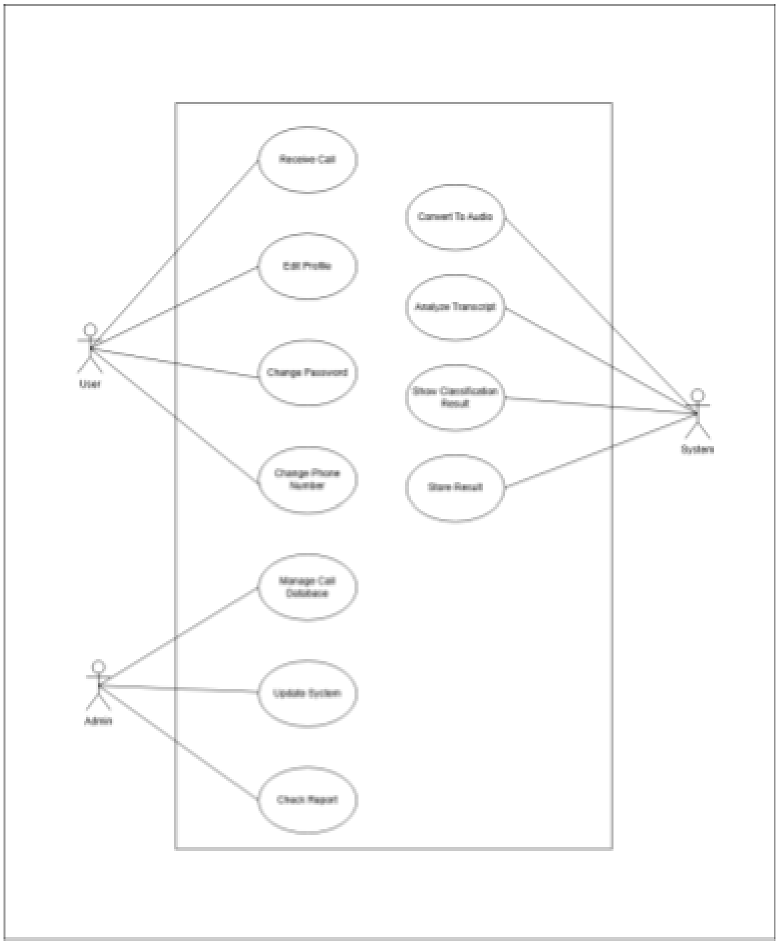


Figure 10: *Use Case Diagram*

3.4.1.4 Activity Diagram

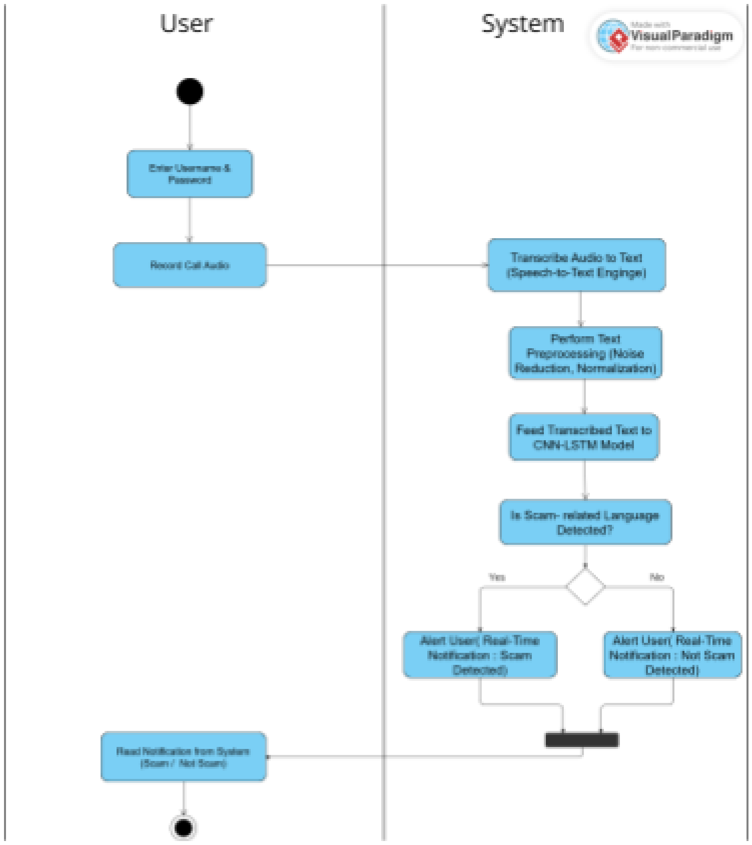

User
System
Made with Visual Paradigm For non-commercial use
Enter Username & Password
Record Call Audio
Transcribe Audio to Text (Speech-to-Text Enginge)
Perform Text Preprocessing (Noise Reduction, Normalization)
Feed Transcribed Text to CNN-LSTM Model
Is Scam- related Language Detected?
Yes
No
Alert User(Real-Time Notification : Scam Detected)
Alert User(Real-Time Notification : Not Scam Detected)
Read Notification from System (Scam / Not Scam)

Figure 11 : *Activity Diagram*

3.4.1.5 Sequence Diagram

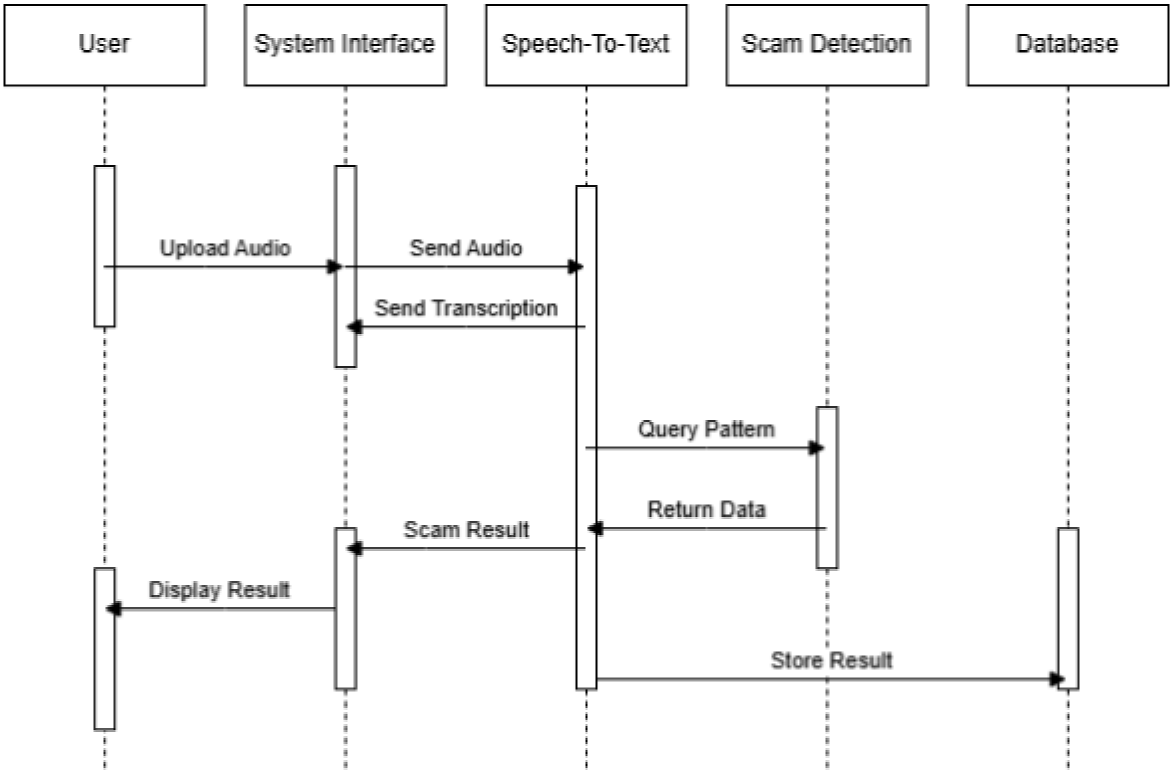


Figure 12 : *Sequence Diagram*

3.5 Prototypes

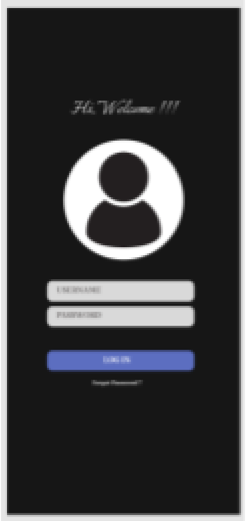


Figure 13 : *Log In Page*

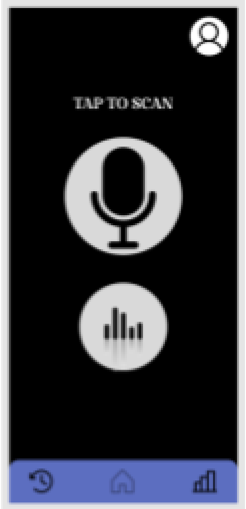


Figure 14 : *Home Page*

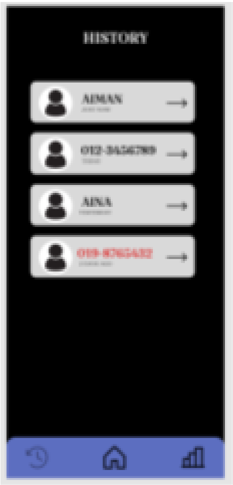


Figure 15 : *History Page*

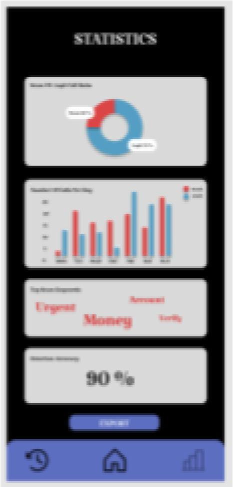
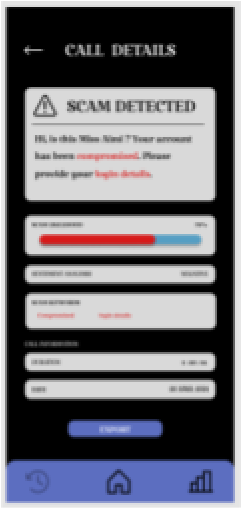
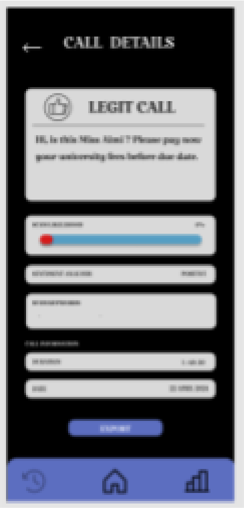


Figure 16 : *Statistics Page*



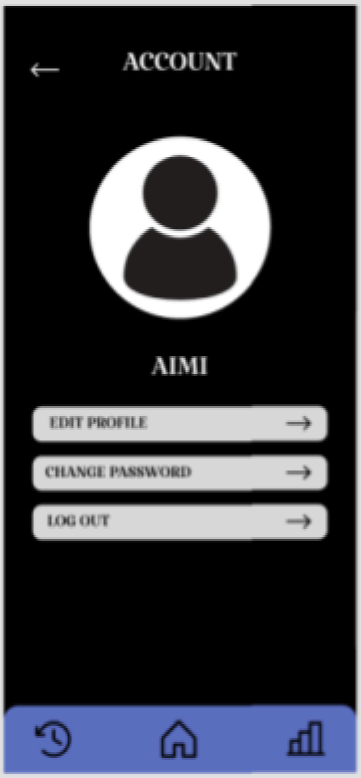
Hi, is this Miss Aimi ? Your account has been compromised. Please provide your login details.

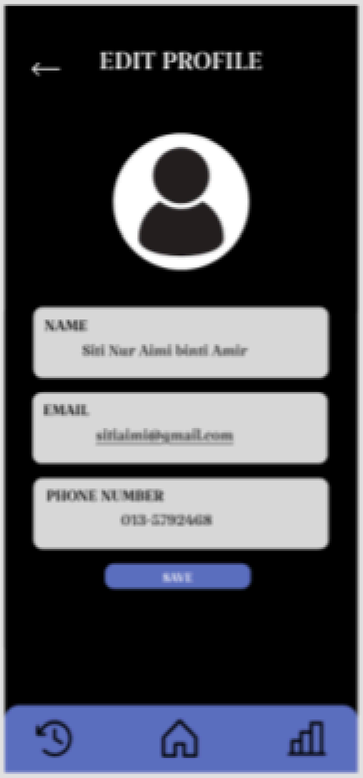
Figure 17 : *Call Details Page (Scam Page)*



Hi, is this Miss Aimi ? Please pay now your university fees before due date.

Figure 18 : *Call Details Page (Legit Page)*





NAME
Siti Nur Aimi binti Amir

EMAIL
sitiaimi@gmail.com

PHONE NUMBER
013-5792468

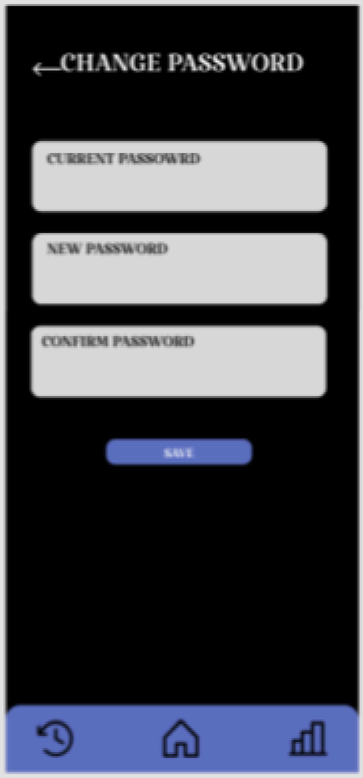


Figure 19 : *Account Page* ***Figure 20 :*** *Edit Profile Page* ***Figure 21 :*** *Change Password Page*

3.6 Summary

This chapter provided a thorough look at the methodology used to create the speech-to-text scam call detection system. The project embraced a structured, iterative approach by utilizing the Agile Software Development Methodology, which allowed for flexibility, adaptability, and ongoing improvement throughout the development process. Each stage of the Agile framework from analyzing requirements to deployment and review was crafted to tackle both the technical intricacies of integrating speech recognition and the real-world hurdles of identifying scam calls in real time. By breaking the development into distinct phases, the project team could concentrate on making steady progress, continuously enhancing system features and performance through regular testing and feedback.

Additionally, the chapter outlined the strategies employed to gather system requirements, which included consultations with supervisors, thorough literature reviews, and casual interviews with potential users. These methods ensured that both the functional and non-functional requirements of the system were accurately identified and documented. The functional requirements centered on essential tasks like audio processing, transcription, scam classification, and result display, while the non-functional requirements highlighted crucial elements such as performance, reliability, security, and scalability.

In summary, the methodology discussed in this chapter has laid a strong groundwork for developing a resilient and adaptable scam call detection system. By merging speech recognition with machine learning within a well-structured development process, the system fills gaps in current solutions and presents an innovative way to combat scam call threats. The next chapter will delve into the results, testing outcomes, and analysis of the system's performance, further confirming the effectiveness of the chosen methodology and design approach.

REFERENCES

Fei, L. S. (2015, April). Assessment of Flood Hazard Risk Based on Catastrophe Theory in Flood Detention Basins. Retrieved December 20, 2022, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5774402&tag=1

Fauziana, A., Tomoki, U., & Takahiro, S. (2017). Determination of Z-R Relationship and Inundation Analysis for Kuantan River. Research Publication No. 2, 1–39.Retrieved from http://www.met.gov.my/data/research/researchpapers/2017/researchpaper_201702.pdf

Ma, Z., Wang, P., Huang, M., Wang, J., Wu, K., Lv, X., Pang, Y., Yang, Y., Tang, W., & Kang, Y. (2025). TeleAntiFraud-28k: An audio-text slow-thinking dataset for telecom fraud detection. *arXiv preprint arXiv:2503.24115*. https://arxiv.org/abs/2503.24115

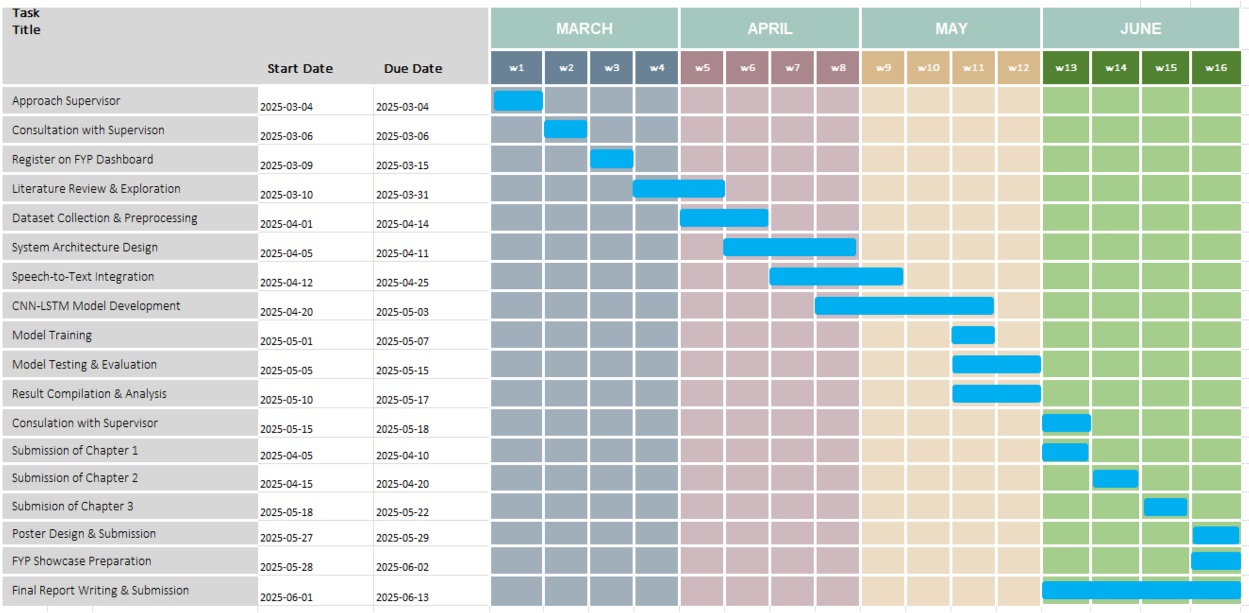
Negrão, M., & Domingues, P. (2021). SpeechToText: An open-source software for automatic detection and transcription of voice recordings in digital forensics. *Forensic Science International: Digital Investigation*, *36*, 301311. https://doi.org/10.1016/j.fsidi.2021.301311

Shen, Z., Yan, S., Zhang, Y., Luo, X., Ngai, G., & Fu, E. Y. (2025). "It warned me just at the right moment": Exploring LLM-based real-time detection of phone scams. *arXiv preprint arXiv:2502.03964*. https://arxiv.org/abs/2502.03964

Bharati, S., & Podder, P. (2020). *Performance Analysis of Gaussian, Median, Mean, and Wiener Filters on Biomedical Image Denoising*. Preprints. Retrieved from https://doi.org/10.20944/preprints202005.0053.v1.

APPENDICES

GANTT CHART



Task Title	Start Date	Due Date
Approach Supervisor	2025-03-04	2025-03-04
Consultation with Supervison	2025-03-06	2025-03-06
Register on FYP Dashboard	2025-03-09	2025-03-15
Literature Review & Exploration	2025-03-10	2025-03-31
Dataset Collection & Preprocessing	2025-04-01	2025-04-14
System Architecture Design	2025-04-05	2025-04-11
Speech-to-Text Integration	2025-04-12	2025-04-25
CNN-LSTM Model Development	2025-04-20	2025-05-03
Model Training	2025-05-01	2025-05-07
Model Testing & Evaluation	2025-05-05	2025-05-15
Result Compilation & Analysis	2025-05-10	2025-05-17
Consulation with Supervisor	2025-05-15	2025-05-18
Submission of Chapter 1	2025-04-05	2025-04-10
Submission of Chapter 2	2025-04-15	2025-04-20
Submision of Chapter 3	2025-05-18	2025-05-22
Poster Design & Submission	2025-05-27	2025-05-29
FYP Showcase Preparation	2025-05-28	2025-06-02
Final Report Writing & Submission	2025-06-01	2025-06-13

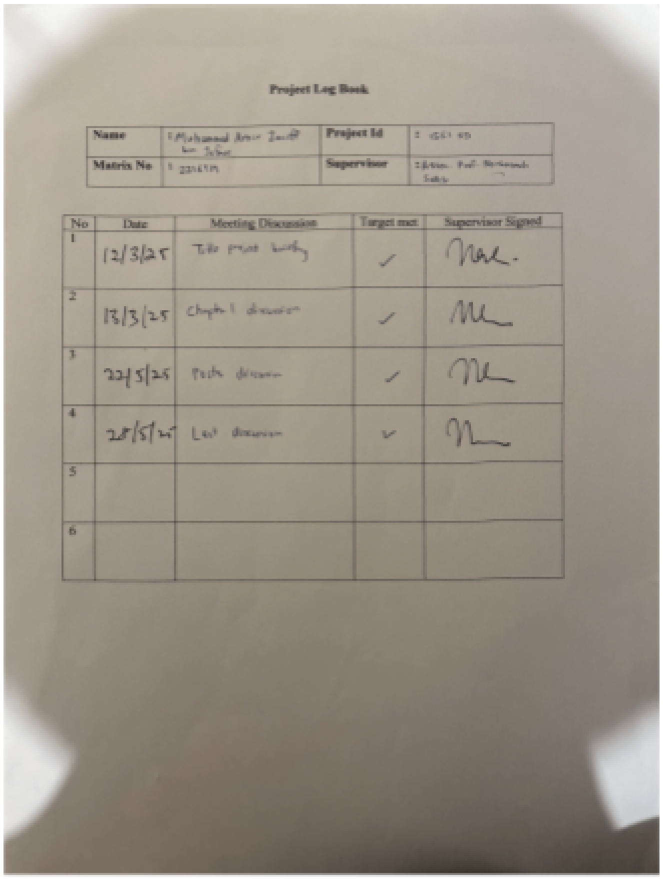
Appendix 1: Gantt Chart of Speech-to-Text Based Scam Call Detection Using Automated Analysis

DIVISION OF WORK

Name	Task
1. MUHAMMAD AMIR ZARIEFF BIN JEFNEE 2216919	Chapter 1 Chapter 2 Chapter 3
2. MUHAMMAD AFIF BIN HUSNAN 2212583	Chapter 1 Chapter 2 Chapter 3

Appendix 2: Work Distribution Table

PROJECT LOGBOOK



Project Log Book

Name	: Mohammad Amir [illegible] bin Jafar	Project Id	: [illegible]
Matrix No	: [illegible]	Supervisor	: [illegible] Prof. [illegible]

No	Date	Meeting Discussion	Target met	Supervisor Signed
1	12/3/25	Title project briefing	✓	
2	13/3/25	Chapter 1 discussion	✓	
3	22/5/25	[illegible] discussion	✓	
4	28/5/25	Last discussion	✓	
5				
6				

Appendix 3 : *Log Book*