HUAWEI

Spark Infinity

Huawei Developer Competition

Project Name: SecureCom - AI-Powered Communication Fraud Defense Platform

Team Name: SMGyupsal

University Name: Technological Institute of the Philippines - Quezon City

Team Leader Email: qarsantos02@tip.edu.ph

Team Leader WhatsApp Contact Number: +63 911 656 1428

HUAWEI CLOUD
EVERYTHING AS A SERVICE

Project Overview

Overview

Project Name	*SecureCom - AI-Powered Communication Fraud Defense Platform*
Team Name	*SMGyupsal*
Contacts	*garsantos02@tip.edu.ph* *ghamanuel@tip.edu.ph* *gmjkegob@tip.edu.ph*
Technical Field	*AI, Machine Learning, Natural Language Processing, Cybersecurity*
Technologies	*BERT Transformer Models, PyTorch, Flask REST API, Flutter, Firebase, Huawei Cloud OBS (planned), Google Colab*
Keywords	*Fraud Detection, AI, Smishing, Vishing, NLP, Mobile Security, Transformer Models, Communication Safety*
Applicable Fields	*Cybersecurity, Mobile Security, Financial Protection, Digital Safety, Public Safety*
Description (in 200 words)	*Communication fraud through smishing (SMS phishing) and vishing (voice phishing) has emerged as a critical cybersecurity threat, with global losses exceeding USD 2.9 billion in 2023. In terms of our local considerations, the Philippines itself faces acute challenges due to high mobile penetration (170M subscriptions) and SMS-centric communication patterns (2.4B daily messages).* ***SecureCom** addresses this through AI-driven fraud detection using advanced natural language processing. We have developed core technical components including comprehensive data preprocessing pipelines, dual transformer models (BERT-tiny architecture) specialized for SMS and voice call detection, and Flask-based REST API infrastructure.* *Our working prototype demonstrates proof-of-concept functionality with semantic analysis that goes beyond traditional keyword-based filtering. The dual-model strategy captures channel-specific fraud patterns, while the lightweight architecture enables fast inference suitable for real-time mobile deployment.* *The system is architected for Huawei Cloud OBS integration for scalable model distribution in production. SecureCom targets vulnerable populations in high-risk regions, supporting UN SDG 8, 9, and 16 by enabling safe digital adoption and strengthening trust in telecommunications infrastructure.*

Contents

1 Team Introduction

2 Project Introduction

3 Technical Architecture

4 Features

5 Innovations

6 Business Value

7 Development Status & Roadmap

8 Demo

Team Introduction

Mark Jeonel Kenn Gob

University Name:
Technological Institute of the Philippines
– Quezon City

Position/Role:
Backend API Development

Background/Experience:
Undergraduate, Computer Engineering
Major in Cyber-Physical Systems

Hazel Aillson Manuel

University Name:
Technological Institute of the Philippines
– Quezon City

Position/Role:
Mobile Application & System Integration

Background/Experience:
Undergraduate, Computer Engineering
Major in Systems Administration

Andrei Santos

University Name:
Technological Institute of the Philippines
– Quezon City

Position/Role:
AI Model Development & Training Lead

Background/Experience:
Undergraduate, Computer Engineering
Major in Human-Computer Interaction

Project Introduction

Project Background & Context

Communication fraud has evolved from crude spam into sophisticated social engineering campaigns exploiting human psychology: trust, fear, and urgency. Modern smishing and vishing attacks impersonate legitimate institutions (banks, government agencies, healthcare providers, delivery services) with alarming authenticity.

Global Crisis Statistics:

- USD 2.9 billion in losses from phishing/vishing in 2023 (FBI IC3 Report)
- Philippines ranks among top 5 countries for mobile fraud incidents per capita
- 37% of vishing attacks in 2024 used AI-generated voice cloning
- 65% of victims are elderly or financially vulnerable individuals
- Small businesses lose average USD 75,000 per successful fraud incident

Regional Context - Philippines & Southeast Asia:

- Over 170 million mobile subscriptions (population: 115 million)
- 2.4 billion SMS messages sent daily (highest globally)
- Rapid shift to mobile banking and e-wallets creates new fraud opportunities
- Mix of English, Filipino, and Tagalog complicates detection
- Limited cybersecurity awareness among general population

Problems Solved:

Critical Gaps in Existing Solutions:

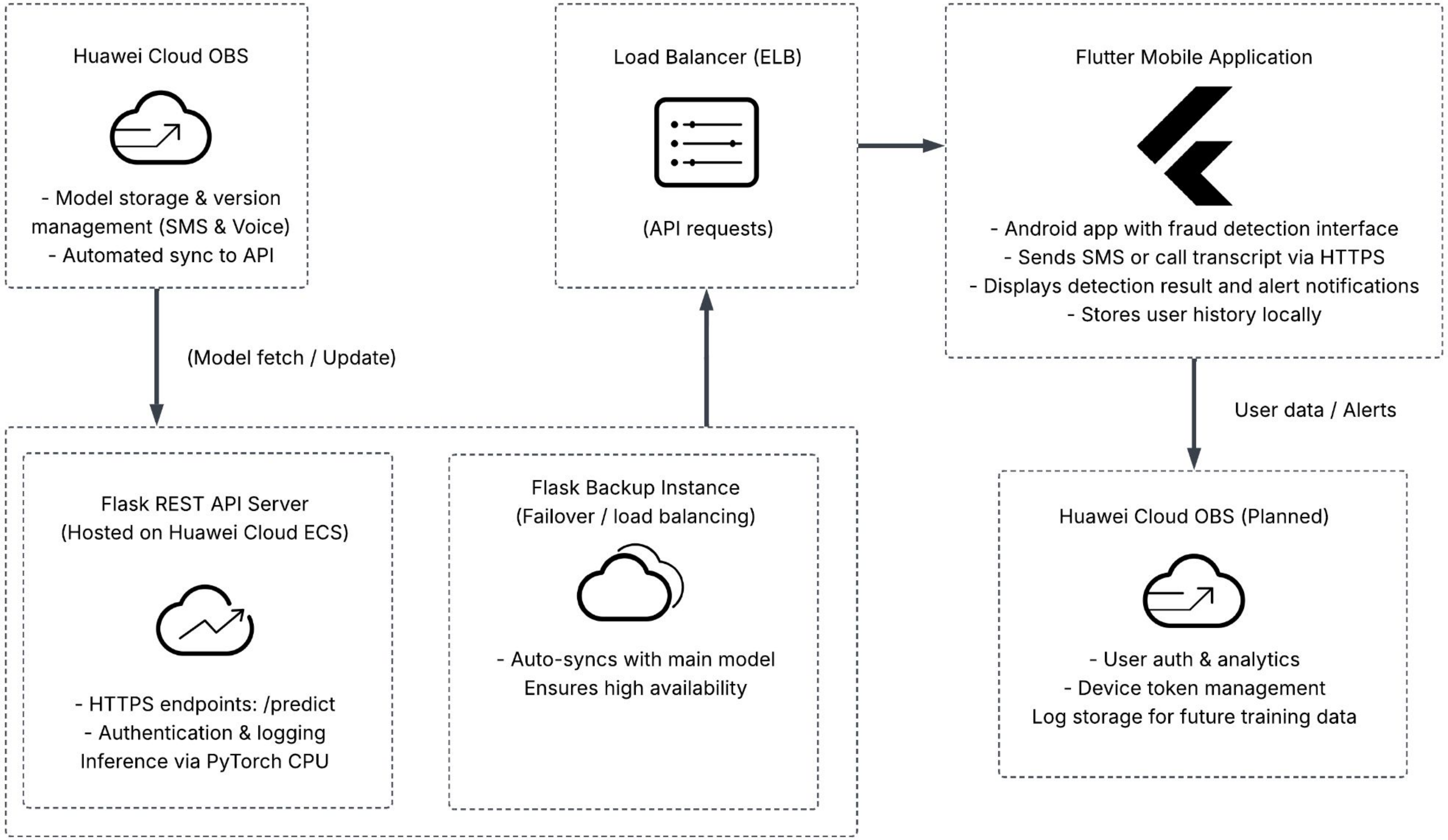
Current Approach	Why It Fails
Keyword blacklists and pattern matching	Cannot understand context, intent, or semantic manipulation
Crowdsourced phone number blacklists	Scammers change numbers instantly; reactive not proactive
No voice call analysis	Vishing attacks go undetected until damage is done
Network-level filtering after delivery	Users already exposed to fraudulent content before analysis

Target Users

- **Primary Users:** Individuals in high-risk social settings - primarily young adults vulnerable to communication fraud
- **Secondary Users:** Law enforcement, organizations, and public health groups requiring reliable, aggregated data to improve policy and resource allocation
- **Enterprise Users:** Businesses seeking to protect employees and customers from fraud attacks
- **Telecom Providers:** Network operators looking to enhance security offerings

Technical Architectures

Solution Deployment Architecture Diagram



Huawei Cloud OBS
- Model storage & version management (SMS & Voice)
- Automated sync to API
(Model fetch / Update)
Load Balancer (ELB)
(API requests)
Flutter Mobile Application
- Android app with fraud detection interface
- Sends SMS or call transcript via HTTPS
- Displays detection result and alert notifications
- Stores user history locally
User data / Alerts
Flask REST API Server
(Hosted on Huawei Cloud ECS)
- HTTPS endpoints: /predict
- Authentication & logging
Inference via PyTorch CPU
Flask Backup Instance
(Failover / load balancing)
- Auto-syncs with main model
Ensures high availability
Huawei Cloud OBS (Planned)
- User auth & analytics
- Device token management
Log storage for future training data

Service Description

SecureCom deploys dual AI fraud detection models using Huawei Cloud OBS and Flask-based APIs to analyze SMS and voice transcripts. The system ensures secure, scalable, and real-time protection against communication fraud.

1. The latest SMS and voice models are stored and versioned in **Huawei Cloud OBS**, automatically synced to Flask API servers hosted on **Huawei ECS**.
2. The **Load Balancer (ELB)** distributes incoming HTTPS prediction requests from the **Flutter mobile app** to available Flask instances.
3. The **mobile app** authenticates users via **Firebase**, then submits SMS or voice transcripts through secured API endpoints (/predict_sms, /predict_calls).
4. The **Flask API** verifies the request, loads the appropriate model from local cache or OBS, and performs inference using **PyTorch**.
5. The **classification result** (legitimate or fraudulent) is returned to the mobile app, which displays alerts and logs activity for analytics or retraining.
6. The system is finally planned to periodically sync with **Huawei Cloud OBS** to ensure both primary and backup API servers run the latest model versions, maintaining availability and accuracy.

Features

SecureCom integrates transformer-based AI fraud detection with dual-channel architecture and Flask API infrastructure to provide immediate, context-aware identification of smishing and vishing attacks.

Key Features:

- Provides objective AI classification beyond keyword blacklists through semantic understanding of fraud patterns, urgency manipulation, and social engineering tactics
- Utilizes dual BERT-tiny models analyzing SMS and voice transcripts separately, with specialized optimization for each channel's linguistic characteristics
- Processes input through preprocessing pipeline (cleaning, normalization, tokenization) then analyzes with fine-tuned transformers to classify: *LEGITIMATE (0)* or *FRAUDULENT (1)*

AI Detection Capabilities vs. Traditional Systems

Capability	**Traditional Systems**	**SecureCom AI**
Detection Method	Keyword matching	Semantic context analysis
SMS Protection	Static blacklist	BERT transformer (SMS-optimized)
Voice Protection	None	BERT transformer (voice-optimized)
Adaptation	Manual updates	Retrainable AI models
Response Time	Post-exposure	Real-time inference

Table 1. SecureCom AI-driven detection capabilities compared to traditional fraud prevention systems

SecureCom is the first platform to integrate transformer-based NLP, dual-channel specialization, and mobile-ready inference for communication fraud detection. Unlike traditional blacklist systems, SecureCom's AI model understand context, intent, and manipulation patterns, providing quantifiable fraud assessment that adapts as threats evolve, immediately enabling users to recognize sophisticated attacks without relying on constantly-updated keyword lists.

Innovations

SecureCom is the first fraud detection system to apply transformer neural networks to communication content analysis, moving beyond simple pattern matching to semantic understanding.

Technical Breakthroughs:

- **AI Semantic Detection** – First BERT transformer application for communication fraud, detects manipulation patterns keyword filters miss
- **Dual-Channel Models** – Separate SMS and voice models optimized for each channel's fraud characteristics
- **Mobile-Ready Inference** – BERT-tiny architecture enables real-time detection with practical response times

In comparison to keyword blacklists and phone number blocking systems, SecureCom is the first platform to integrate transformer NLP, dual-channel specialization, and mobile-ready inference for communication fraud detection. The AI models understand semantic context, urgency manipulation, and social engineering language, providing quantifiable fraud assessment that adapts as threats evolve, rather than relying on static rules requiring constant manual updates.

Business Value

Social & Economic Impact

- Protects users from smishing/vishing losses and psychological harm
- Enhances telecom trust and supports secure digital participation
- Contributes to **UN SDGs 8, 9, and 16** by promoting safe digital economies

SDG	Contribution of SecureCom
SDG 8 – Decent Work and Economic Growth	Protects individuals and small businesses from fraud-related financial losses, enabling safer participation in the digital economy.
SDG 9 – Industry, Innovation, and Infrastructure	Strengthens the reliability of digital communication networks and promotes trust in mobile technologies through AI-driven cybersecurity innovation.
SDG 16 – Peace, Justice, and Strong Institutions	Reduces cyber-enabled crime by identifying fraudulent communications early, supporting law enforcement and public protection efforts.

SecureCom delivers both economic and social impact by protecting users and small businesses from communication fraud, fostering safer participation in the digital economy. By strengthening trust in mobile communication systems, it supports **SDG 9 (Industry, Innovation, and Infrastructure)** and **SDG 8 (Decent Work and Economic Growth)** through secure digital adoption. Additionally, by detecting scams early and potentially aiding law enforcement, it advances **SDG 16 (Peace, Justice, and Strong Institutions)** . Overall, SecureCom positions itself as a sustainable, AI-driven solution that promotes financial safety and digital confidence.

Development Status & Roadmap

Current Status (Prototype Achievements)

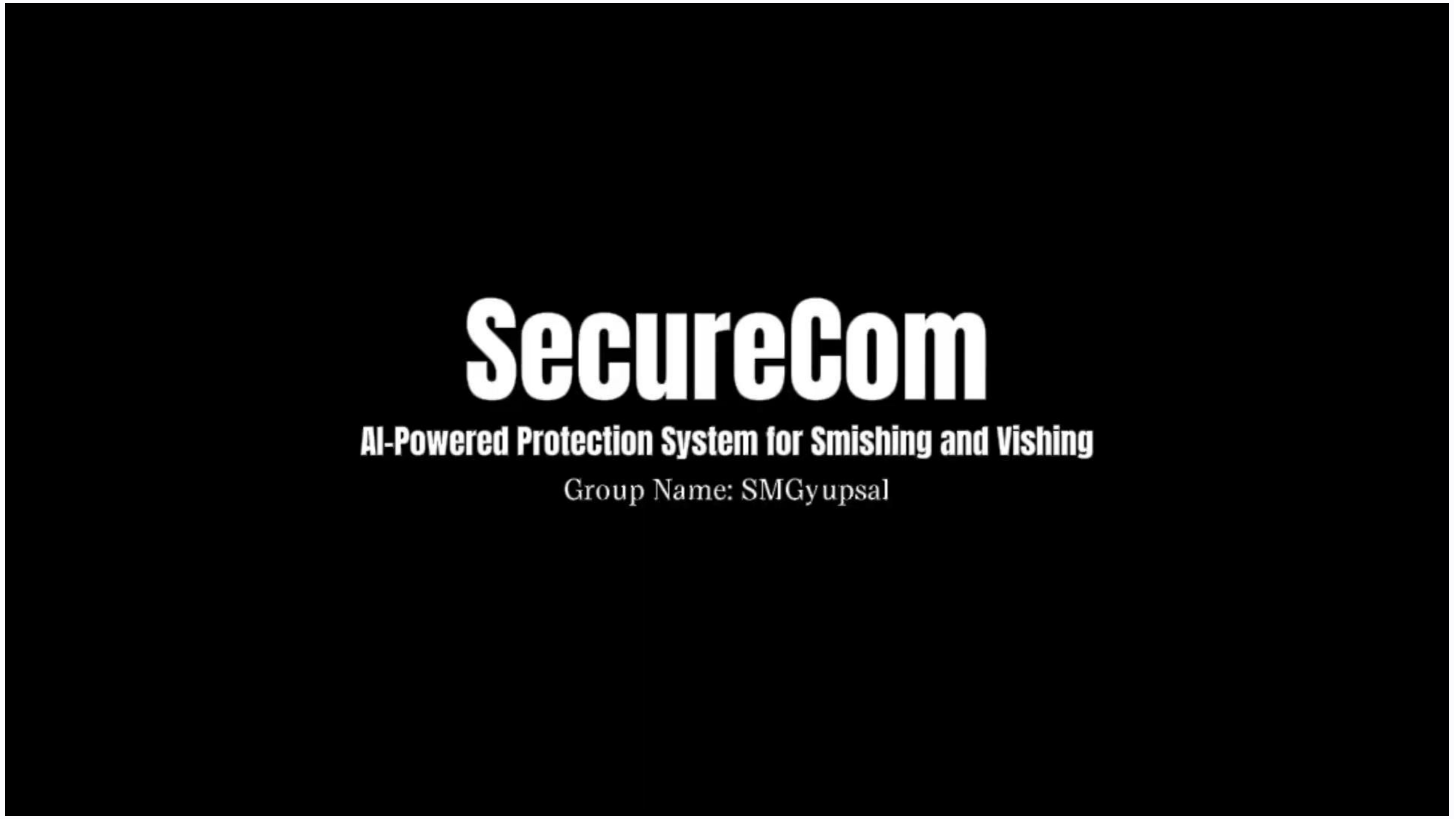
- ✔ Data Infrastructure: Complete preprocessing pipeline (cleaning, normalization, tokenization) tested on SMS and voice datasets
- ✔ AI Models: Dual BERT-tiny models fine-tuned for SMS and voice fraud detection
- ✔ Backend API: Flask REST API with authentication, dual endpoints
- ✔ Mobile Interface: Flutter prototype developed with fraud visualization UI
- ✔ Deploy models to Huawei Cloud OBS for scalable distribution

Next Steps & Expansion

- ❑ May integrate FunctionGraph for automated updates, ModelArts for model lifecycle management, and Huawei Mobile Services (HMS) to enable real-time SMS and call event detection
- ❑ Expand datasets to include other main and regional languages
- ❑ Establish pilot partnership with telecom provider/s for real-world testing

Demo (For Semi-finals)

- Demo



SecureCom

AI-Powered Protection System for Smishing and Vishing

Group Name: SMGyupsal

Google Drive Link:

https://drive.google.com/drive/folders/15P3v2yMIQmAtSPdY8zMQgd9ZZrXyIJbc?usp=sharing

THANK YOU

Team SMGyupsal

- Gob, Mark Jeonel Kenn -
- Manuel, Hazel Aillson -
- Santos, Andrei -