

사용자를 위한
실시간 피싱 탐지 어플리케이션

구해줘 피싱

컴퓨터공학과

김민서 김성현 박윤호

윤찬익 최현수

정보통신공학과

류효정



사례1

대구지방검찰청 형사 7부 000 검사입니다.
휴대폰에 수사 앱을 설치해야 합니다.

70대 A씨에게 검찰 수사관을 사칭한 전화가 옴

A씨 명의 계좌가 범죄에 연루됐다며 관련 부서 직인이 찍힌 문서를 보여주고 조사에 임해야 한다는 이야기를 들음

그 후 예금이 범죄에 이용될 수 있으니 안전계좌로 옮겨야 한다면서 여러 차례 이체를 요구

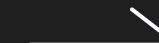
결국 수천만 원 이상을 송금하고 나서야 가족을 통해 사기임을 인지

위조 문서 활용

기관 사칭

보이스피싱

스마트폰·앱 구조를 잘 모르는
디지털 취약계층을 노린 ‘기관사칭’형 범죄



고령층 고액 피해가 많이 발생

사례2

[CG통운] 배송 주소 오류입니다.
링크 클릭 후 주소를 재입력해주세요.

20대 B씨에게 택배사 로고가 찍힌 택배 문자로 위장한 스미싱 도착

링크를 누르자 택배사처럼 보이는 페이지에서 여러가지 개인정보들을 요구

이후 계좌에서 수백만 원이 빠져나가고, 추가로 소액 대출까지 실행되어 피해 확대

최근 실생활에서 자주 사용되는 어플이나 사이트 사칭으로 여러가지 스미싱 문자가 많이 오기 시작하였음.

실시간 탐지 필요

스미싱 문자

외부 링크 피해

링크 클릭·메신저 사용이 일상화된
짧은 층을 노린 스미싱과 메신저 피싱



짧은 문장, URL, 계좌번호만으로 빠른 범죄 실행

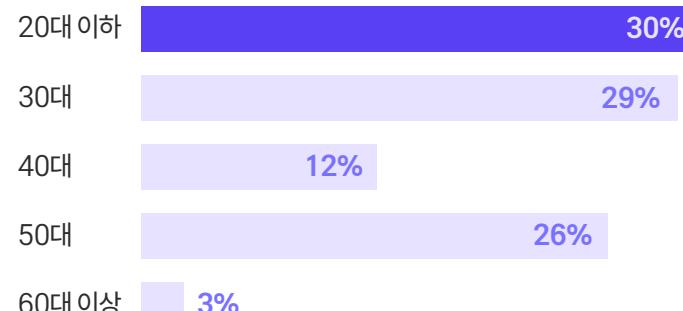
BEFORE RESEARCH

보이스피싱, 더는 ‘남일’ 이 아닙니다.

보이스피싱은 더 이상 높은 연령대만의 문제가 아닙니다.

모든 연령, 더 어린 연령을 타겟으로 매년 피싱 피해가 발생하고 있습니다.

01 전체 피해 연령별 비중



2023년 금융감독원 확정치 기준, 60대 이상의 경우 피해자 수는 적으나 피해 금액은 고액

02 20대 이하 피해자 수



2023년 금융감독원 확정치 기준, 전년도 대비 20대 이하 피해자 수 약 2배 급증

왜 20대인가?

최근 피싱 범죄는 짧은 문장과 URL만으로 범죄가 빠르게 이루어지기 때문에 링크 클릭과 메신저 사용이 일상화된 젊은 층을 노림
내용을 검증하기보다 즉각적으로 반응하거나 클릭하는 습관으로 인해 익숙한 ‘빨리빨리’ 문화가 독이 됨

PROBLEM AND SOLUTION

보이스피싱, 어떻게 막아야 할까요?

정확한 탐지를 통해 개인의 일상을 보호하고, 더 나아가 사회 전체의 피해 사례 감소를 기대할 수 있습니다.

01

공문서 및 직인 위조

PROBLEM

위조된 문서인지 판단이 불가능해요.

SOLUTION



직인, 레이아웃 탐지 등을 활용한 문서 위조 탐지 서비스가 필요해요.

02

보이스피싱

PROBLEM

전화 도중에 피싱인지 확인이 어려워요.

SOLUTION



통화 시 STT와 AI를 활용해 피싱 위험도를 실시간으로 알려주세요.

03

스미싱, 링크를 이용한 피싱

PROBLEM

나도 모르게 문자 링크를 클릭해요.

SOLUTION



도착한 문자에서 본문과 링크를 분리해 실시간으로 스미싱 위험을 알려주세요.

04

기관 및 사용자 사칭

PROBLEM

번호로 오는 연락이 사칭인지 알 수 없어요.

SOLUTION



수집된 데이터를 활용해 사용자 맞춤형 피싱 의심 연락처를 제공해 주세요.

디지털 취약 계층부터 젊은 층까지, 전연령대의 모든 사용자를 위한 실시간 피싱 및 위조 탐지 시스템이 필요해요.



구해줘 피싱

구해줘의 'q', 피싱의 유래가 된 '낚시'에서 물고기를 가져와
모든 연령대에게 친숙한 한글로 된 어플리케이션 이름을 구상

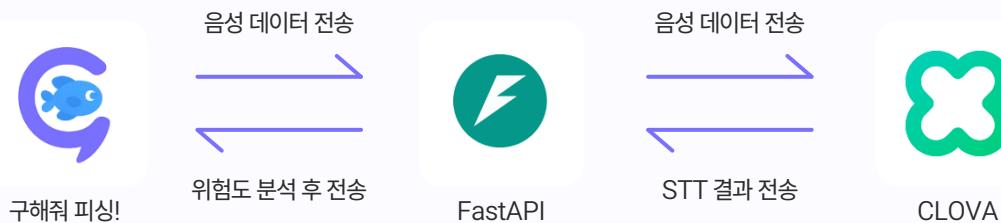


‘구해줘 피싱!’은 디지털 취약 계층에서부터 젊은 층까지, 전 연령대의 모든 사용자를 위한
문서 위조 탐지, 실시간 보이스피싱 및 스미싱 탐지 서비스 등 즉각적인 모니터링 서비스를 제공합니다.

PCM을 통한 Websocket 통신으로 실시간 통화 탐지 기능을 제공합니다.

POINT 1

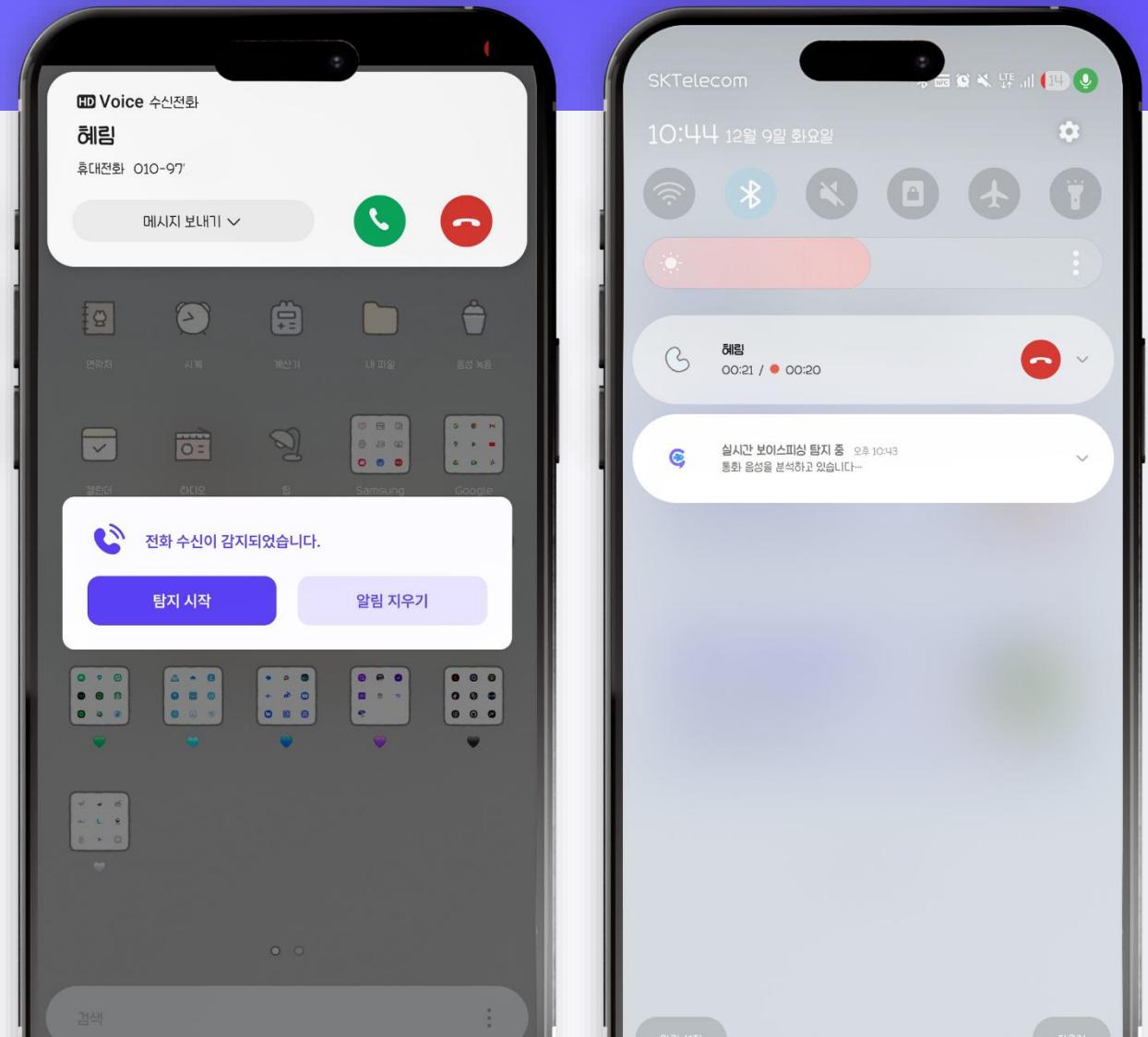
기능 구조도



POINT 2

기능 동작 과정

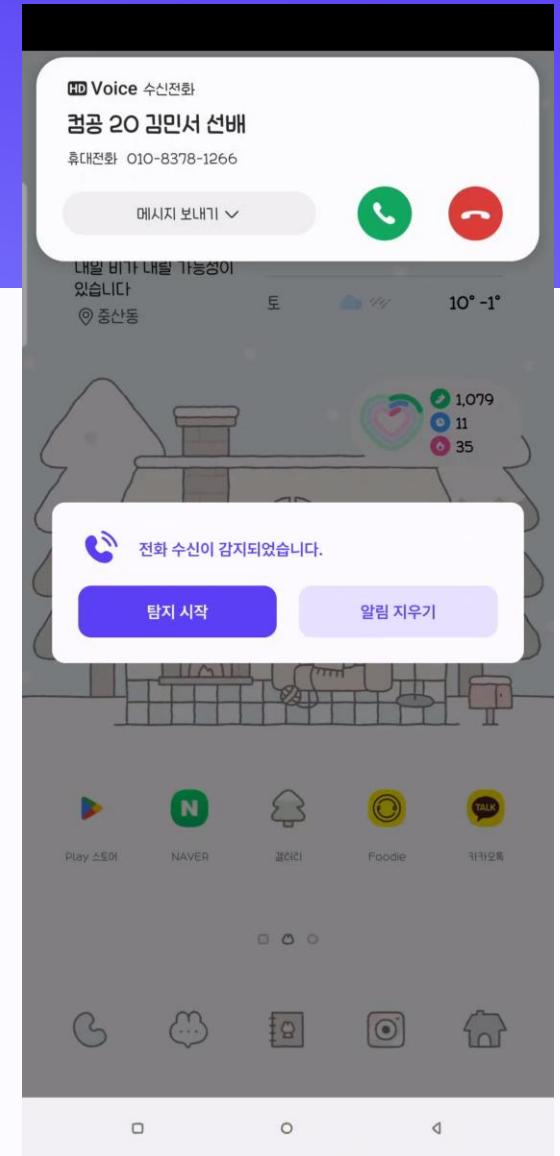
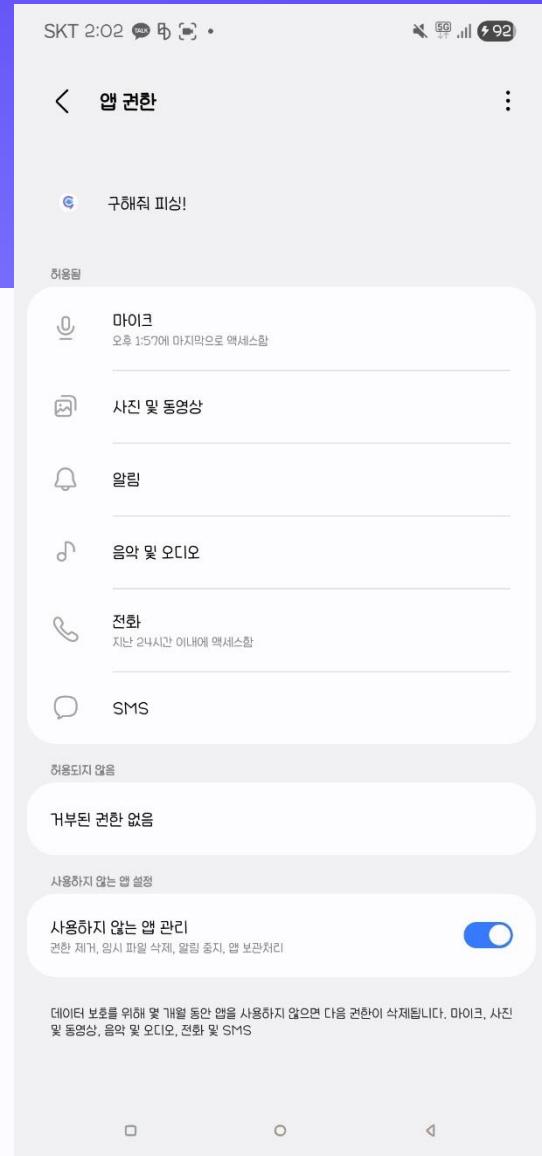
- 01 통화 도중 실시간으로 음성 정보를 수집해 STT를 이용해 변환
- 02 서버는 위험 키워드와 문맥을 종합적으로 분석
- 03 분석 결과를 토대로 보이스피싱 위험도를 판단
- 04 위험 탐지 시 사용자에게 알림



PCM을 통한 Websocket 통신으로 실시간 통화 탐지 기능을 제공합니다.

POINT 3 시연 영상 내용

- 01 앱 사용을 위해 필요한 권한을 전부 허용
- 02 앱 실행 유무와 상관 없이 전화 수신시 탐지 시작 알림이 뜸
- 03 탐지 시작 알림을 누르면 목록 페이지로 이동
- 04 Delay 이후 탐지가 시작되면 탐지 중임을 알림으로 확인 가능



PCM을 통한 Websocket 통신으로 실시간 통화 탐지 기능을 제공합니다.

POINT 3 실시간 서비스 테스트 로그

01 SERVER 테스트 로그

```
0|fastapi | 2025-12-02 05:51:26: INFO:    127.0.0.1:52740 - "WebSocket /api/transcribe/ws?sr=16000&lang=ko-KR" [accept
ed]
0|fastapi | 2025-12-02 05:51:26: 2025-12-02 05:51:26 - transcribe_stream - INFO - [WS OPEN] client=unknown sr=16000 lan
g=ko-KR
0|fastapi | 2025-12-02 05:51:26: INFO:    connection open
0|fastapi | 2025-12-02 05:51:26: 2025-12-02 05:51:26 - transcribe_stream - INFO - STT_PROVIDER=grpc
0|fastapi | 2025-12-02 05:51:26: 2025-12-02 05:51:26 - transcribe_stream - INFO - [STT_START] client=unknown
0|fastapi | 2025-12-02 05:51:26: 2025-12-02 05:51:26 - transcribe_stream - INFO - recv bytes len=2048, volume=0.00
0|fastapi | 2025-12-02 05:51:27: 2025-12-02 05:51:27 - transcribe_stream - INFO - recv bytes len=2048, volume=0.00
0|fastapi | 2025-12-02 05:51:27: 2025-12-02 05:51:27 - transcribe_stream - INFO - recv bytes len=2048, volume=0.00
0|fastapi | 2025-12-02 05:51:27: 2025-12-02 05:51:27 - transcribe_stream - INFO - recv bytes len=2048, volume=0.00
0|fastapi | 2025-12-02 05:51:27: 2025-12-02 05:51:27 - transcribe_stream - INFO - recv bytes len=2048, volume=0.00
0|fastapi | 2025-12-02 05:51:27: 2025-12-02 05:51:27 - transcribe_stream - INFO - recv bytes len=2048, volume=0.00
0|fastapi | 2025-12-02 05:51:27: 2025-12-02 05:51:27 - transcribe_stream - INFO - recv bytes len=2048, volume=0.00
0|fastapi | 2025-12-02 05:51:27: 2025-12-02 05:51:27 - transcribe_stream - INFO - recv bytes len=2048, volume=0.00
0|fastapi | 2025-12-02 05:51:27: 2025-12-02 05:51:27 - transcribe_stream - INFO - recv bytes len=2048, volume=0.00
```

02 APP 테스트 로그

2025-12-10 13:58:03.662 29215-18218 AudioDebug	com.example.antiphishingapp	D maxVal=0
2025-12-10 13:58:03.662 29215-18218 RealtimeRepository	com.example.antiphishingapp	D sendPcm size=2048 connected=true
2025-12-10 13:58:03.722 29215-18218 RealtimeCallService	com.example.antiphishingapp	D bytesRead=2048, connected=true
2025-12-10 13:58:03.722 29215-18218 AudioDebug	com.example.antiphishingapp	D maxVal=0
2025-12-10 13:58:03.722 29215-18218 RealtimeRepository	com.example.antiphishingapp	D sendPcm size=2048 connected=true
2025-12-10 13:58:03.802 29215-18218 RealtimeCallService	com.example.antiphishingapp	D bytesRead=2048, connected=true
2025-12-10 13:58:03.802 29215-18218 AudioDebug	com.example.antiphishingapp	D maxVal=0
2025-12-10 13:58:03.802 29215-18218 RealtimeRepository	com.example.antiphishingapp	D sendPcm size=2048 connected=true
2025-12-10 13:58:03.862 29215-18218 RealtimeCallService	com.example.antiphishingapp	D bytesRead=2048, connected=true

클로바 STT를 활용한 음성 텍스트 변환으로 음성 통화 녹음 분석을 제공합니다.

POINT 1 OneUI 기반 안드로이드 14의 음성 권한

AudioRecord VOICE_COMMUNICATION, RECOGNITION과 함께 사용 시 차단

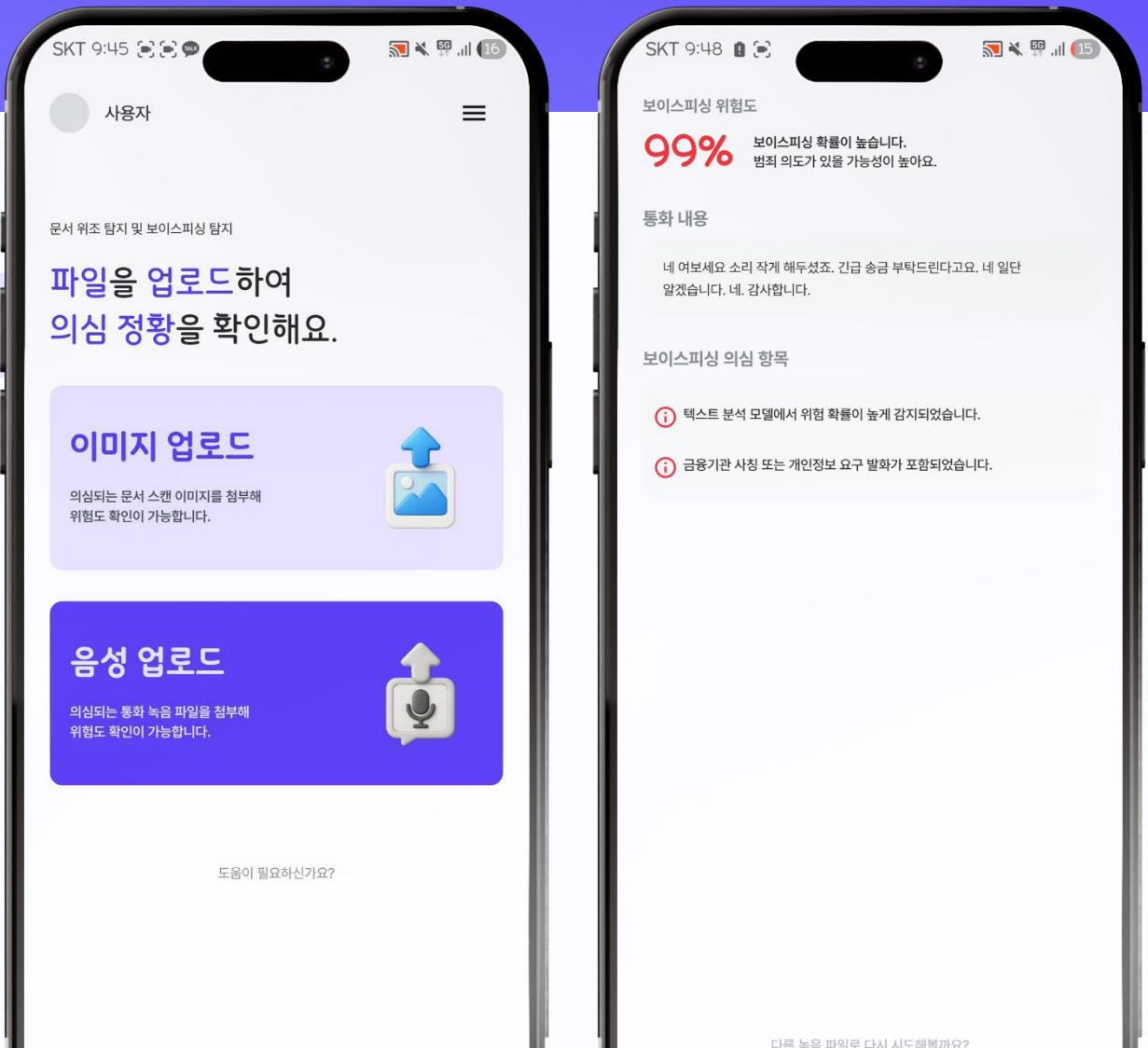
VOICE_CALL Start() 자체가 실패하거나 음성 0 처리, 권한이 완전 차단됨

MediaRecorder 통화 연결 시 자동으로 음성 0 처리, 녹음 파일 생성되나 빈 파일로 생성

» 안드로이드 12 이상부터 통화 녹음 원천 차단, OneUI에서는 일반 녹음도 제한

POINT 2 기능 동작 과정

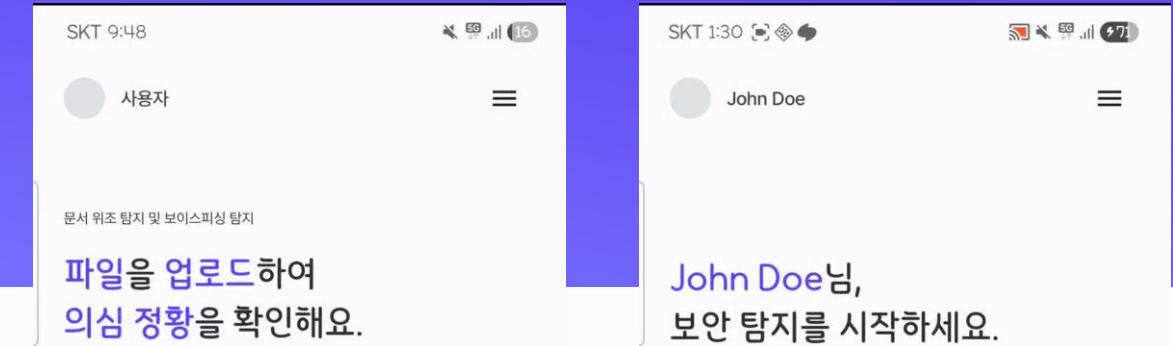
- 01 음성 파일을 업로드 하면 STT를 이용해 변환
- 02 서버는 위험 키워드와 문맥을 종합적으로 분석
- 03 분석 결과를 토대로 보이스피싱 위험도를 판단
- 04 위험 탐지 시 사용자에게 알림



클로바 STT를 활용한 음성 텍스트 변환으로 음성 통화 녹음 분석을 제공합니다.

POINT 3 시연 영상 내용

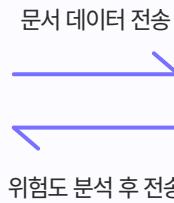
- 01 음성 파일을 업로드 하면 STT를 이용해 변환
- 02 서버는 위험 키워드와 문맥을 종합적으로 분석
- 03 분석 결과를 토대로 보이스피싱 위험도를 판단
- 04 통화 내역 본문과 판단 근거, 종합 위험도를 확인 가능함



OpenCV, OCR, 레이아웃 탐지로 문서 위조 여부를 판단하고 위험도를 제공합니다.

POINT 1**기능 구조도**

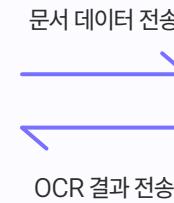
구해줘 피싱!



직인

레이아웃

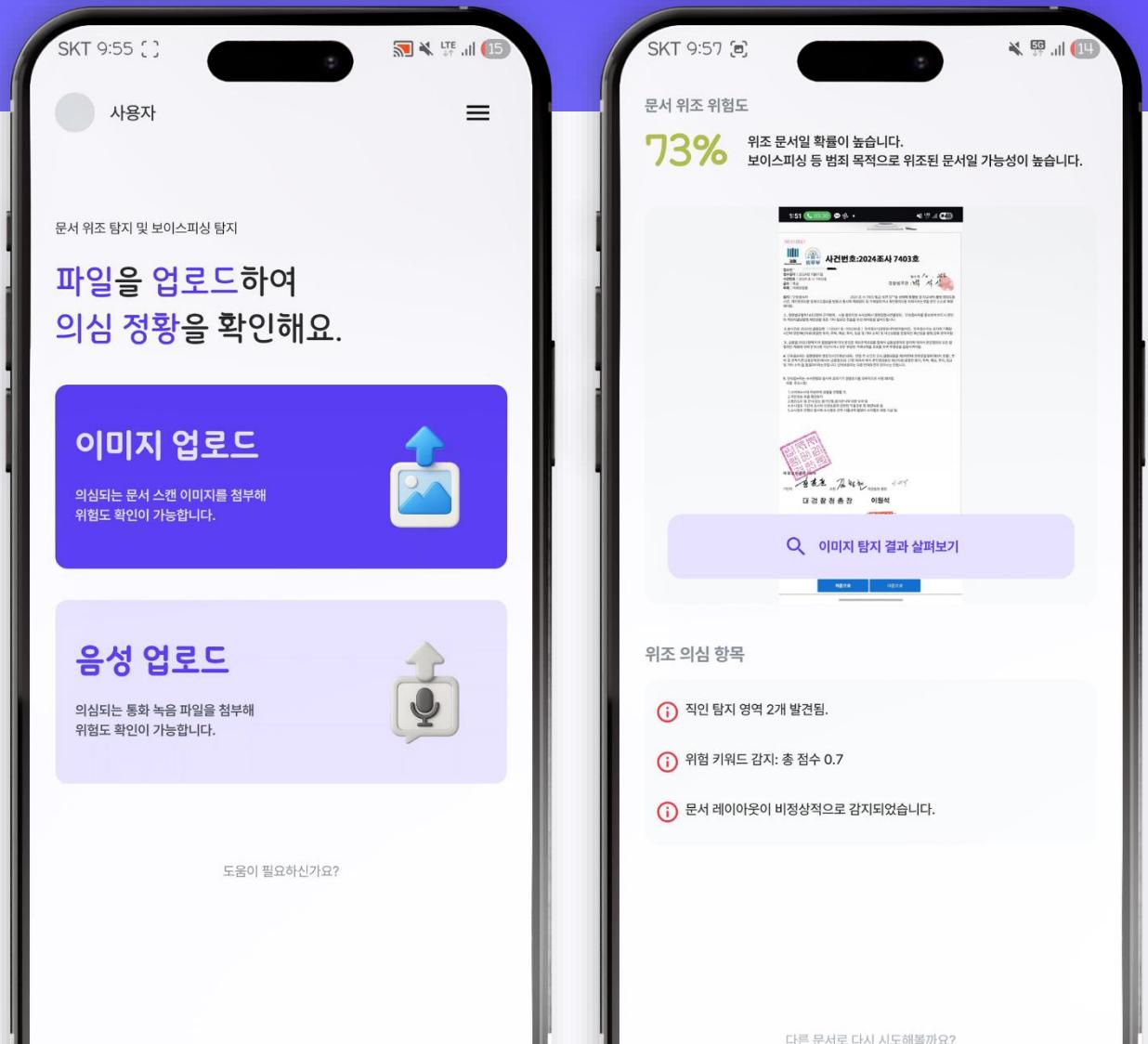
키워드



CLOVA

POINT 2**기능 동작 과정**

- 01 이미지 파일을 업로드 하면 OCR을 이용해 사진 속 글자를 반환
- 02 서버는 위험 키워드와 레이아웃, 직인을 종합적으로 분석
- 03 분석 결과를 토대로 문서 위조 위험도를 판단
- 04 사용자에게 탐지 결과와 위험도 판단 근거를 제공



OpenCV, OCR, 레이아웃 탐지로 문서 위조 여부를 판단하고 위험도를 제공합니다.

문서 위조 위험도

68% 위조 문서일 가능성이 있습니다.
주의 깊게 확인해주세요.

01 위조 위험도를 **직관적으로 표시**하고,
색상을 통해 **사용자가 쉽게 인지할 수 있도록 합니다.**

문서 위조 위험도

73% 위조 문서일 확률이 높습니다.
보이스피싱 등 범죄 목적으로 위조된 문서일 가능성이 높습니다.

02 위조 판단 근거를 **사용자가 알 수 있도록 설명합니다.**

위조 의심 항목

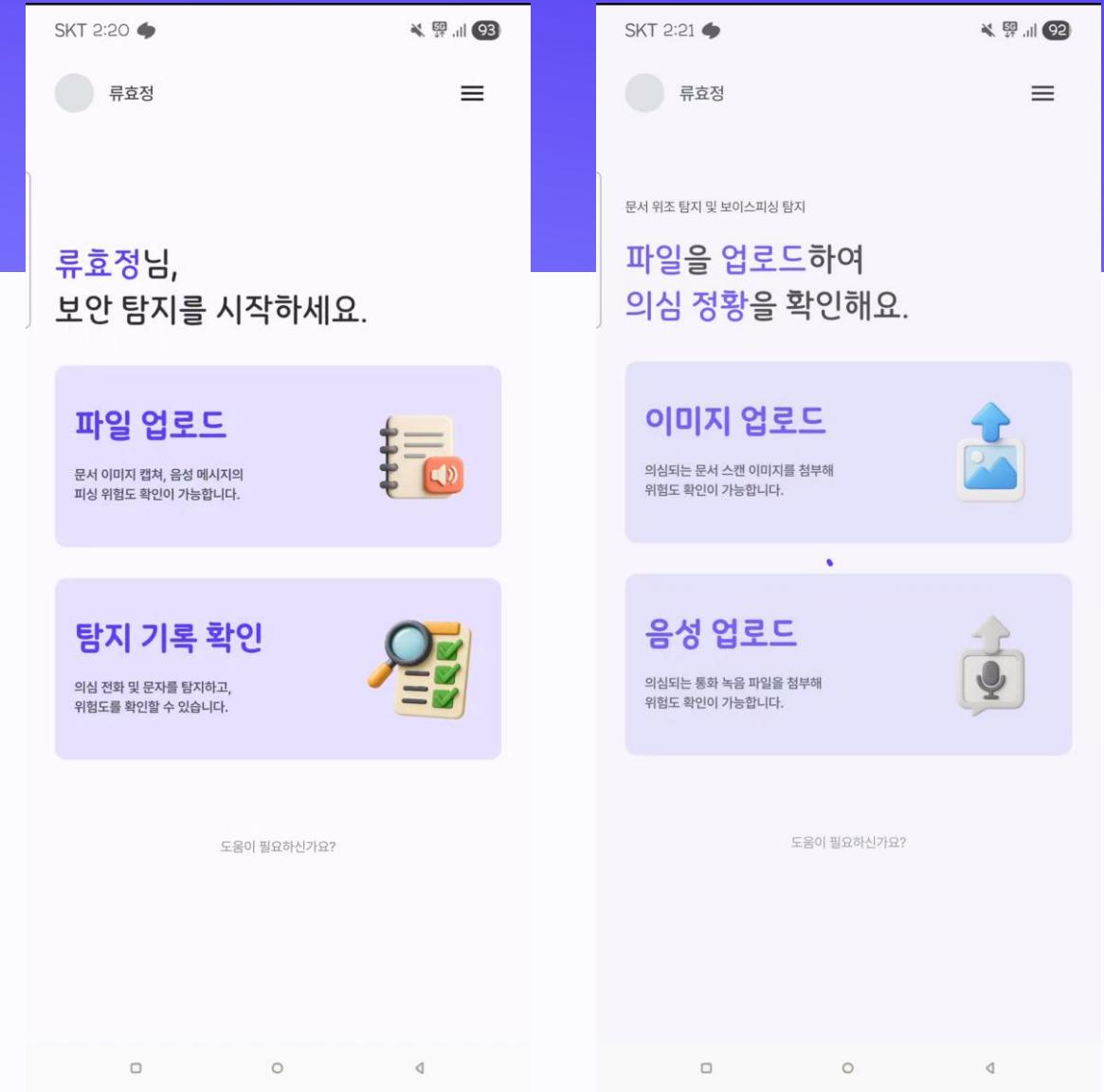
- ⓘ 직인 탐지 영역 2개 발견됨.
- ⓘ 위조 키워드 감지: 총 점수 0.7
- ⓘ 문서 레이아웃이 비정상적으로 감지되었습니다.

03 탐지 결과를 **이미지 위에 표시해**
사용자가 알기 쉽도록 합니다.

OpenCV, OCR, 레이아웃 탐지로 문서 위조 여부를 판단하고 위험도를 제공합니다.

POINT 3 시연 영상 내용

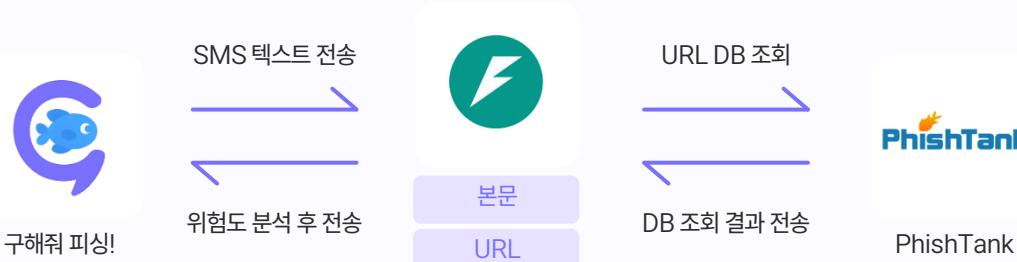
- 01 사용자가 업로드할 이미지를 선택하면 OCR을 이용해 사진 속 글자를 반환
- 02 서버는 위험 키워드와 레이아웃, 직인을 종합적으로 분석
- 03 분석 결과를 토대로 문서 위조 위험도를 판단
- 04 사용자는 탐지 위험도와 사진 원본, 직인 탐지 결과, 판단 근거 확인 가능



본문과 URL을 분리해 키워드 및 링크 분석을 통한 위험 알림을 제공합니다.

POINT 1

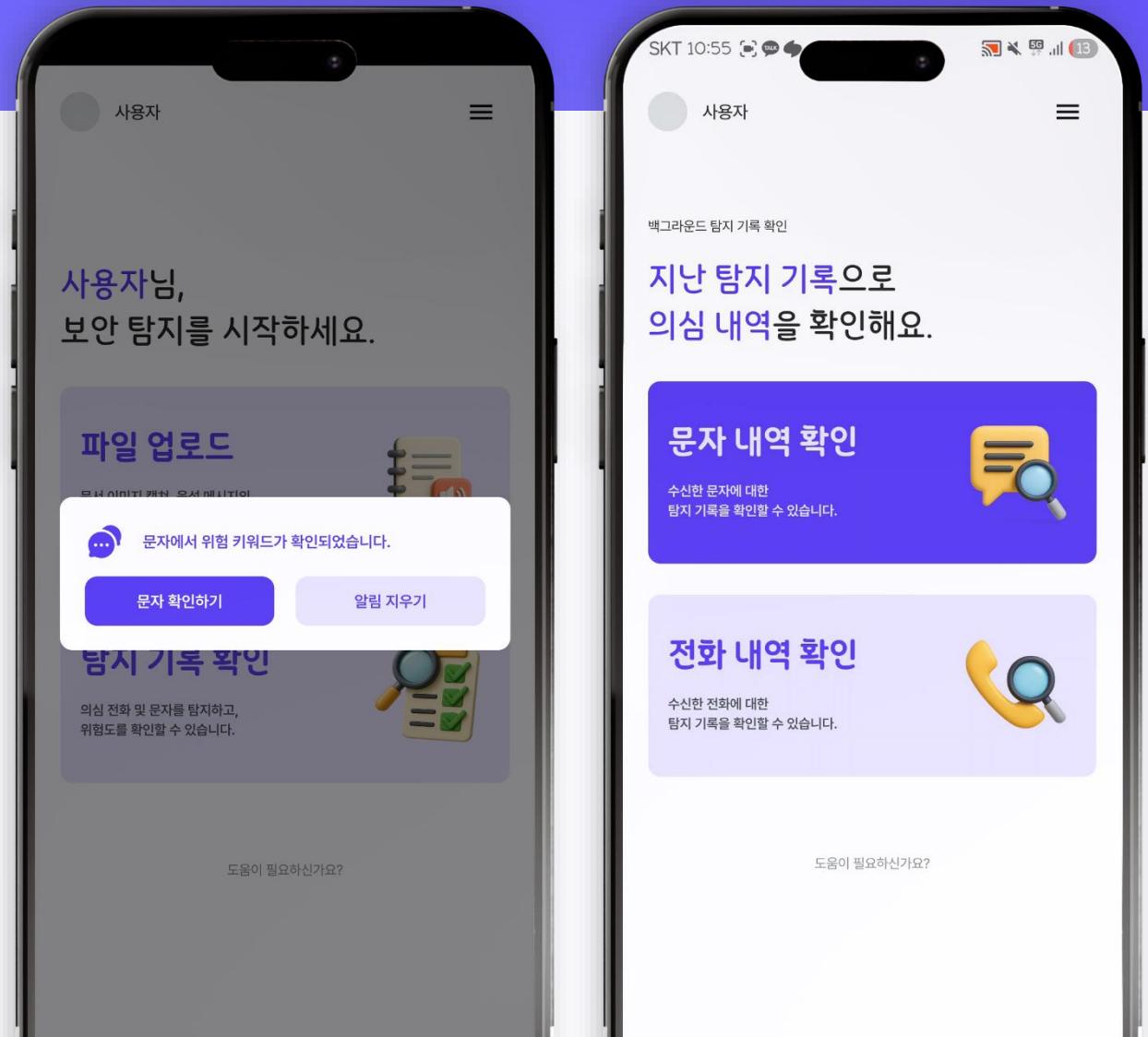
기능 구조도



POINT 2

기능 동작 과정

- 01 문자를 수신하면 앱이 자동으로 감지하여 분석 시작
- 02 서버는 텍스트 내용을 분석하며, URL 존재 시 URL 검사
- 03 결과를 토대로 스미싱 위험도를 판단
- 04 위험도가 기준치 이상일 경우 사용자에게 알림



본문과 URL을 분리해 키워드 및 링크 분석을 통한 위험 알림을 제공합니다.

01 검색 기능을 통해 원하는 링크, 키워드 등을 찾을 수 있습니다.

원하는 내역을 검색하세요.

01030904435 PM 09:34
[국민은행] 보안등급 향상을 위한 긴급 업데이트가 필요합니다.
24시간 이내 미 업데이트시 계좌가 정지됩니다.

01030904435 PM 09:32
안녕하세요 대구지방검찰청입니다. 의심계좌확인으로 인해 연락드렸는데 혹시 계좌 확인 가능하실까요?

02 주요 의심 키워드를 눈에 보기 쉽게 표기합니다.

01083781266 PM 11:13
http://192.168.1.100/banking/login

01030904435 PM 10:10
[국민은행] 보안등급 향상을 위한 긴급 업데이트가 필요합니다.
24시간 이내 미 업데이트시 계좌가 정지됩니다.

01030904435 PM 10:06
http://192.168.1.100/banking/login

01030904435 PM 10:05
http://192.168.1.100/banking/login

01030904435 PM 09:34
[국민은행] 보안등급 향상을 위한 긴급 업데이트가 필요합니다.
24시간 이내 미 업데이트시 계좌가 정지됩니다.

01030904435 PM 09:32
안녕하세요 대구지방검찰청입니다. 의심계좌확인으로 인해 연락드렸는데 혹시 계좌 확인 가능하실까요?

01023335317 PM 08:42
즉시 송금 부탁드리겠습니다. 가급적 빠른 확인을 부탁드립니다.

03 최신순, 위험도순, 번호순으로 탐지 목록을 정렬하고, 필터를 통해 원하는 조건의 내역만을 확인 가능합니다.

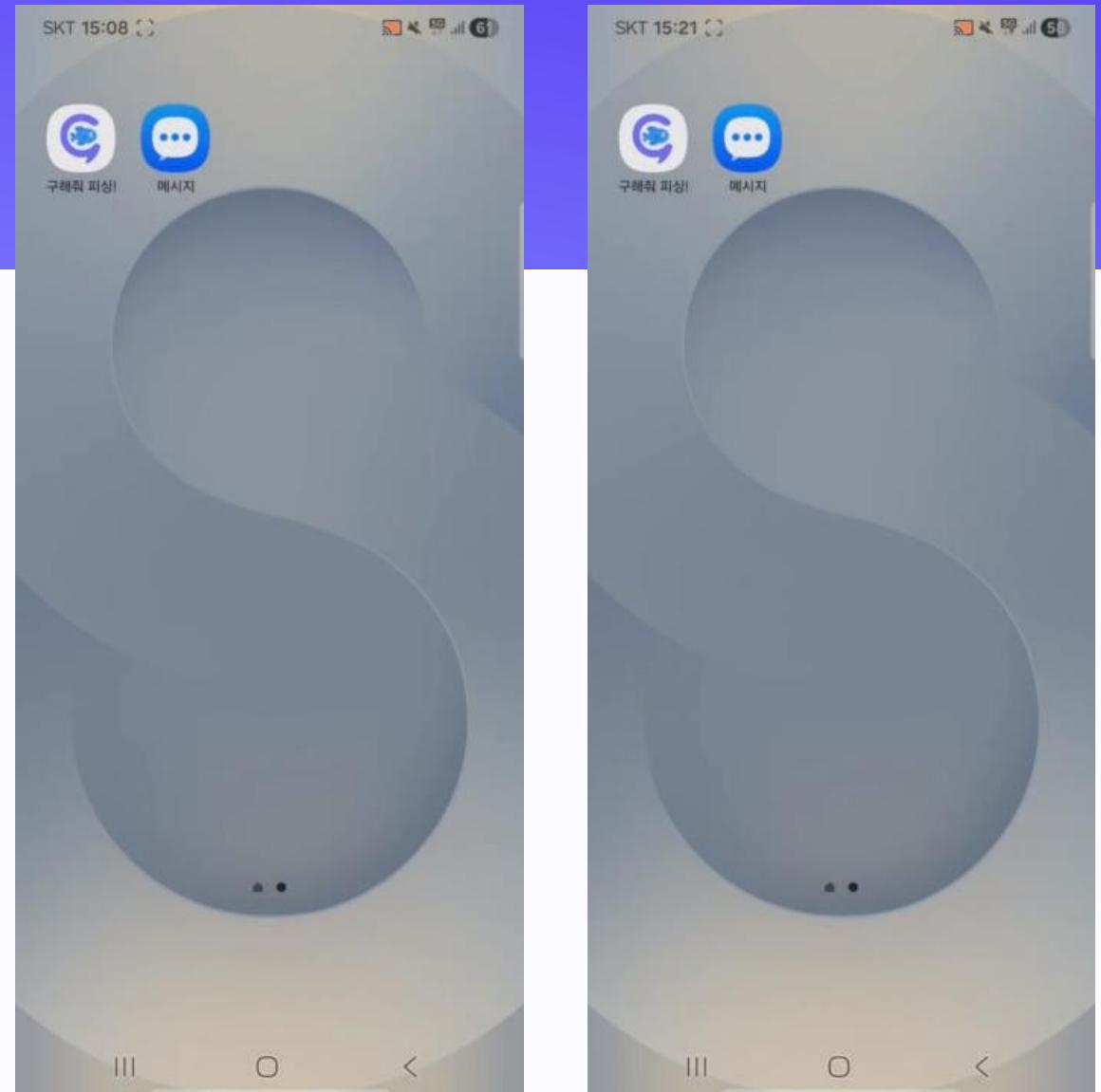
최신순
위험도순
번호순

본문과 URL을 분리해 키워드 및 링크 분석을 통한 위험 알림을 제공합니다.

POINT 3

시연 영상 내용

- 01 문자를 수신 하면 앱이 자동으로 감지하여 분석 시작
- 02 서버는 텍스트 내용을 분석하며, URL 존재 시 URL 검사
- 03 결과를 토대로 스미싱 위험도를 판단, 위험 탐지 시에 알림
- 04 탐지 결과 확인 버튼을 누르면 결과 페이지로 이동



2025 SOFTWARE ENGINEERING
UI FLOW DESIGN



BUSINESS FEASIBILITY

지속 가능한 상생 비즈니스 모델로 안전을 잇다

개인의 앱 사용 경험이 모여 사회 전체를 지키는 집단 면역 체계를 구축하고,
참여 기업과 공공의 이익이 선순환하는 구조를 만듭니다.

비즈니스 모델 구조도

위조 문서
데이터 제공탐지 기술
제공수사 공조
정책 자문신종 피싱
데이터 공유

AFTER DEVELOPMENT

하나의 앱으로 안전한 디지털 라이프를 꿈꾸다.

개인의 스마트폰을 넘어, 사회 전체를 지키는 통합 안전 플랫폼으로 확장합니다.

모두의 경험을 하나로 모아 더 안전한 대한민국을 만듭니다.

KEYWORD 1

#전문화

신종 범죄 예측, 개인 맞춤형



DEV 데이터 분석, 모델 재학습

수집된 데이터를 분석하여
아직 알려지지 않은 신종 패턴 예측

사용자별 취약점을 분석하고
맞춤형 경고 제공

KEYWORD 2

#플랫폼화

가족의 일상을 지키는 안전 플랫폼



DEV 정확도 향상 및 다양성 확보

디지털 취약계층의 피싱 위험을
가족 구성원이 원격으로 관리, 보호

카카오톡, 이메일, SNS 메시지 등
다양한 소통 경로들까지 탐지 범위를 넓힘

KEYWORD 3

#공익실현

기관 협력을 통한 집단면역 체계 구축



DEV Database 구축

수집된 피싱 데이터를
공공/수사기관에 제공, 데이터 허브 구축

국가적 피싱 범죄 근절을 위한
사회적 시스템을 형성

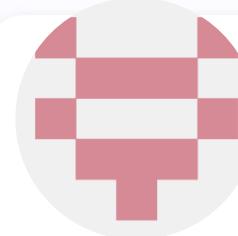
‘구피’를 만든 팀원들을 소개합니다.



김민서

@Kimmminseo1104

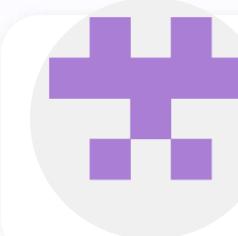
22012286, 컴퓨터공학과



박윤호

@nini4746

22012124, 컴퓨터공학과



윤찬익

@ychoik

22212125, 컴퓨터공학과

BACK

SERVER/APPLICATION

APP/FUNCTIONALITY

- 앱.서버 WebSocket/HTTP 연결 설정
- 연결/인증 오류 디버깅 및 수정
- PCM 기반 음성 캡처, 전송 로직 구현 지원

SERVER

- FastAPI 기반 백엔드 골격 설계
- Clova gRPC STT 연동 및 WebSocket 구현
- 이미지 업로드 API, 주요 기능 함수 파이프라인 구성

BACK

SERVER/DB/MACHINE LEARNING

SERVER/DB

- JWT 기반 로그인 및 유저 인증 로직 구현
- 스미싱·보이스피싱 탐지 API와 서버 파이프라인 구현
- 크론탭·PhishTank 기반 피싱 사이트 DB 자동 갱신
- 유저 Database 구현

ML/AI

- 피싱 사이트 탐지 모델 학습
- 피싱 탐지 위한 키워드 기반 모델, koBERT 모델 학습

BACK

SERVER/AWS

SERVER

- 네이버·카카오 OAuth 기반 소셜 로그인 연동 구현
- 음성-텍스트 변환을 위한 비동기 Callback API 구현

AWS

- Ubuntu 기반 EC2 서버 구성 및 서비스 배포 환경 구축
- Nginx를 통한 HTTPS 적용 및 도메인 설정
- PM2 기반 프로세스 관리·배포·로그 운영 체계 구축
- WebSocket 활용 실시간 로그 모니터링 시스템 구현

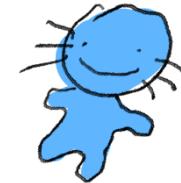
‘구피’를 만든 팀원들을 소개합니다.



김성현

@Ahrasblue

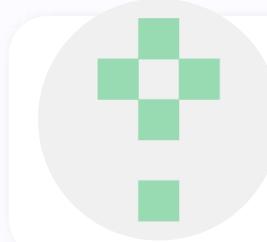
22010958, 컴퓨터공학과



류효정

@YEOL0520

22112144, 정보통신공학과



최현수

@NockDu

22112102, 컴퓨터공학과

FRONT APP/UI/SERVER

APP/UI,FUNC

- 전화/문자 알림 카드, 회원가입 및 메인 페이지 구현
- 파일 업로드, 기록 및 내역 확인을 위한 메뉴 페이지 구현
- 회원 가입 기능, 서버로 가입한 회원 정보 전송 기능 구현
- 문자 수신 시 위험도 계산 및 알림카드 팝업 기능 구현
- 어플리케이션 주요 기능 테스트 지원

SERVER

- 위조 문서 레이아웃 분석 기능 구현

FRONT APP/UI/SERVER

APP/UI,FUNC

- 어플리케이션 기본 구조 구성 및 리팩토링 수행
- 어플리케이션 주요 기능 함수 구현, 테스트 수행 및 디버깅
- PCM 활용 WebSocket 실시간 통신, 기타 API 통신

UI

- 어플리케이션 UI, 로고, PPT 디자인

SERVER

- OpenCV를 활용한 직인 탐지 기능 구현

FRONT APP/UI/SERVER

APP/UI,FUNC

- 타이틀 페이지, 로그인 페이지 구현
- 음성 및 이미지 업로드 결과 페이지 구현
- 로그인, 소셜 로그인, 자동 로그인 기능 구현
- 위험도순, 번호순, 최신순 등 다양한 기준별 정렬 구현
- SMS 로컬 저장 및 출력 기능 구현

SERVER

- OCR, 의심 키워드 판별 기능 구현

사용자를 위한
실시간 피싱 탐지 어플리케이션

구해줘 피싱

컴퓨터공학과

김민서 김성현 박윤호

윤찬익 최현수

정보통신공학과

류효정

