‘너의 A.Idea가 보여’ , 2021 인공지능 학습용 데이터 기반 서비스 공모전

- 아이디어 기획서 -

1 AI 서비스 명칭

ㅇ 피싱헌터 (인공지능기반 대면편취 전기통신금융사기 예방 시스템)

2 활용 인공지능 학습용 데이터

출처	데이터 명	데이터 정보	메타 데이터	활용 알고리즘
AI HUB	한국인 감정 인식을 위한 복합 영상	50만장의 레이블링이 완료된 표정 데이터	성별, 나이대, 업로더 감정 정보, 업로더 배경 정보, Annotation A bounding box 좌표, Annotation B bounding box 좌표, Annotation C bounding box 좌표,	표정인식
Kaggle	Face Mask Detection	853장 마스크 착용, 미착용 이미지	name, pose, truncated, occluded, difficult, Bounding Box	마스크 추적
Oxford University	Hand Data Set	13,050 손 동작 데이터셋	point of bounding box	통화 유무 추적
마이 데이터 사업	계좌정보 - 거래내역	개인 금융 거래데이터	거래 일시(일자), 거래 유형(코드) 거래구분, 거래 금액	금융데이터 분석
마이 데이터 사업	대출상품정보 - 기본정보	개인 금융 거래데이터	대출차주명, 대출일	
마이 데이터 사업	대출팡품정보- 잔액정보	개인 금융 거래데이터	대출 원금	
마이데이터사업	보험정보	보험 대출상품 기본정보 및 잔액정보	대출 실행일, 총 대출 금액, 대출 합계금액	
마이데이터사업	카드정보	카드 대출정보	단기대출목록, 장기대출목록, 단기대출이용일시, 단기대출이용금액, 장기대출일시, 장기대출이용금액	

3 핵심내용

금융 거래 기록과 이미지 처리 인공지능 알고리즘을 결합하여 ATM부스에서 일어날 수 있는 전기통신금융사기에 대하여 선제적 예방체계 구축

4 제안배경 및 목적

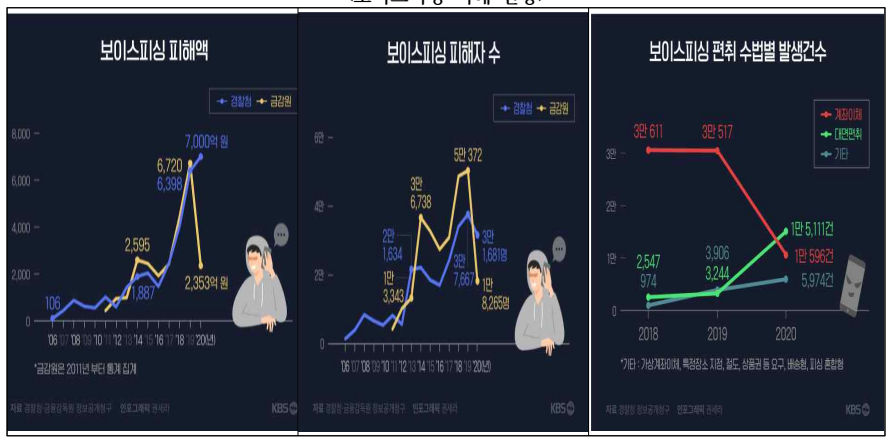
□ 추진배경

ㅇ 추진배경

- 경찰청 자료에 따르면 ‘20년 **보이스피싱 피해액은 역대 최고금액 7,000억원 달성**
- 피해자 수 또한 꾸준히 증가하는 추세이며, **‘20년 기준 31,681명의 피해자 발생**
- **대면편취*로 인한 보이스피싱 피해 발생 건수가 지속적으로 증가 중이며, 이 경우 피해 구제에 어려움이 있기 때문에 사전적 대응체계 구축 필요**

*피해자가 현금 인출 후 보이스피싱 범죄자에게 대면으로 직접 인출한 금액을 전달하는 형태의 전기통신금융사기

<보이스피싱 피해 현황>



□ 필요성

ㅇ 전기통신금융사기피해 예방 현황

- (은행권) 빅데이터기반 악성 프로그램 탐지기술, 스미싱 차단 등 차세대 기술 기반 금융보안 활용체계 확립 중
- (경찰 및 지자체) 노인 계층 등 보이스 피싱 취약 계층에 대한 예방 교육과 간담회, 범인 검거 기여자에 대한 표창 등을 통해 신고활성화 문화 조성
- (금융당국) 제도개선을 통한 신규 보이스피싱 방법에 대한 처벌 강화 및 피해구제 근거 강화 및 **금융회사등의 보이스피싱 모니터링시스템·전사적 방지체계 의무화 추진**

ㅇ 전기통신금융사기피해 예방 한계점

- 은행권에서 빅데이터를 활용한 **보이스피싱 대응체계***를 구축하였으나, 문자 형태의 스미싱으로 한정됨

*인공지능 기반 보이스피싱 차세대 모니터링 시스템

- **제도의 사각지대인 대면편취와 같은 전기통신금융사기피해는 꾸준히 증가하는 반면 예방 및 보호체계가 미비**
- 지자체 및 경찰당국에서는 오프라인 및 온라인 예방 교육을 통한 경각심을 심어주고 있으나, 전기통신금융사기피해 사례는 지속적으로 증가

ㅇ 필요성

- 2019년 까지 누적 피해액은 2조 3천 937억원이며 이 중 피해자가 돌려받지 못한 피해액은 1조 7000억원
- 피해 금액대비 피해 구제금액을 고려했을 때, 보이스피싱은 선제적 예방체계가 필수적임
- 특히 피해구제 제도의 사각지대에 있는 대면편취형 보이스피싱에대한 예방체계 도입이 시급함
- 경찰청 자료에 따르면 전체 보이스피싱 발생 건수 중 **대면편취 피해건수의 비율이 2019년 8.6%에서 2021년 8월까지 73.8%로 급증함**
- 대면편취 피해사례가 주로 발생하는 ATM기계는 장소 특성상 은행 직원의 통제가 불가하여 상대적으로 위험 노출도가 높음

□ 목적

ㅇ ABCDS*기술을 통하여 대국민 보이스피싱 사전예방체계를 구축하여 안전한 금융 생태계 구축

*인공지능(AI), 블록체인(Block chain), 클라우드(cloud), 빅데이터(Big data), 보안(Security)

ㅇ 대면편취형 보이스피싱 피해 예방체계를 빅데이터 분석 및 인공지능 모델들을 결합하여 구축함으로 24시간 대국민 금융 보안체계 수립

- (영상처리) 가명처리된 인공지능 학습용 데이터를 활용하여 보이스피싱 피해자의 표정을 분석하고, 피해 위험도를 산출하는 인공지능모델 개발
- (금융데이터 분석) 대출기록, 입출금 내역 등 마이 금융데이터 분석을 통한 보이스피싱 피해 위험도 분석 및 시각화 시스템 구축
- (스마트 ATM 인공지능 SW) 영상처리 및 금융데이터 분석 모델을 결합하여 고액 인출이 이뤄지는 현장에서 활용 가능한 인공지능 SW 개발

ㅇ 팀은, 해당 경진대회를 통한 후속지원을 통해 실제 사업화를 추진할 예정임

5 세부내용

□ 서비스 세부 내용

ㅇ 서비스 아이디어 개요

- ATM은 비대면 채널 특성상 은행 직원의 통제가 불가하여, 상대적으로 위험노출도가 높음
- 정부기관을 사칭하며 전화를 끊지 못하도록 협박하고 고액 현금 인출 및 송금을 유도하는 수법을 실질적으로 차단하는 서비스가 전무함
- 기존 ATM에 내장되어있는 CCTV 영상 데이터를 기반으로 고객 표정/통화여부 등 영상정보를 통해 보이스피싱 위험도를 산출하여 피해를 사전예방하는 모델 개발
- 금융위 마이데이터 사업 지원을 통해 개인 금융거래데이터를 확보, 이를 바탕으로 보이스피싱 위험도를 산출하여 사전예방하는 모델 개발
- 영상 데이터 기반 모델, 개인 금융데이터 모델을 최종 결합하여 보이스피싱 위험 여부를 판단하는 최종 인공지능 소프트웨어 개발

ㅇ 서비스 절차

① 출금매체(통장, 카드 등) 투입 및 거래 계좌 인식시 고객 금융거래내역 데이터 분석

② 위험거래의 경우, 위험도 분석에 앞서 마스크 등 얼굴을 가리는 요소를 탐지

③ 손 위치와 입모양, 표정을 인식하여 위험도 산출 및 고객 안내

<서비스 활용 절차>

ㅇ 서비스 구현 가능성

- 기존의 표정인식은 **서양인 중심 인공지능 학습용 데이터 기반으로 진행되어, 한국인을 대상으로한 데이터가 부족하여 성능이 저조하였음**
- **데이터 댐 사업으로 AI HUB에 약 50만장의 레이블링이 완료된 한국인 감정 데이터가 구축되었으며, 이를 바탕으로 아이디어 실현 가능성 확보**
- ATM에 별도의 카메라 등 하드웨어를 설치하지 않고 기존 방범용 CCTV를 활용할 수 있으므로 비용적인 측면에서도 실현 가능성 확보
- 고객별 ATM 이용한도 및 계좌 거래내역을 이미 은행 전산시스템을 통해 관리하므로 출금 한도 등 계좌에 대한 데이터를 활용 가능할 것으로 판단
- 또한, 이미 금융권에서 FDS*를 적용하여 위험도를 측정하고 있으므로 추후 이를 융합한다면 더욱 신뢰성있는 서비스로 확장 가능할 것으로 예상

*FDS: Fraud Detection System (이상거래 탐지 시스템)

ㅇ 다양한 입상 및 연구경험을 통한 공신력 있는 팀의 기술력

< 팀 역량 >

팀원	담당	연혁
김영민	Real Time object detection(Mask, Hand Shape) & 최종 AI 모델	· **前 서울대학교 차세대융합기술연구원 컴퓨터비전 및 인공지능 연구실 연구원** · 청년 공공 빅데이터 인턴십 2기 수료 · 빅데이터 동아리 BOAZ 16기 분석 · **CCTV를 이용한 Object Couting AI모델 개발 (블랙스톤 벨포레)** · 조난자 데이터셋 구축 및 AI 모델 개발(NIA) · 차상 탑재 가능한 ADAS 트램 알고리즘 개발 (KRRI) · 고성능&고지속성 경전철 타이어 헬스 모니터링 프로젝트(KAIA) · **KIPS (정보처리학회) 논문 등재** - YOLOv5와 모션벡터를 활용한 트램 - 보행자 충돌 예측방법 연구 · **KCC2021 (정보과학학회) 논문등재** - 딥러닝과 Optical flow를 활용한 보행자 사고 방지 모델 외 3편 · **KIPS(정보처리학회) 특별 원고 논문 등재** - Optical Flow 추정 기술 및 최신 동향 · **특허출원** - 데이터 분석 장치 및 방법, 이상 예측 장치 및 방법, 컴퓨터 프로그램 · **특허출원** - 객체 모션정보를 활용한 자율주행 장치의 충돌 예상 경고시스템 및 방법 · **특허출원** - 드론을 활용한 조난자 수색 영상 AI학습 데이터 구축 · KCC2021 주니어/학부생 분야(스마트시티) 최우수 논문상 · KED 2021 산업 빅데이터 플랫폼 경진대회 우수상
여지민	마이데이터 분석모델 & 최종 AI 모델	· **現 서울대학교 차세대융합기술연구원 컴퓨터비전 및 인공지능 연구실 연구원** · 청년 공공 빅데이터 인턴십 2기 수료 · 前 행정안전부 국가기록원 복원관리과 - **국가기록원 데이터분석 업무 수행** (정량적 데이터 분석을 통한 기록물 훼손 등급 예측) · **국가 이미지 처리를 통한 시청각 데이터 메타데이터 추출 연구 수행**
양동재	사업화 & 최종 AI 모델	· **前 서울대학교 창업캠프** 플랜트 325에서 Vib 플랫폼 Full Stack 개발 · **前 보건복지부 의료정보정책과 2021년도 신규 R&D사업 기획**
		· 외교부 산하 Asia Economic Community Forum에서 **국제 포럼 및 MAU 국제 학술제 기획 및 운영** · 청년창업네트워크 프리즘 - K-ICT창업 멘토링 기획, 운영 , **초기 스타트업 심사역, 서울대학교 창업 네트워크 세션 기획 및 운영** · 충남 공공데이터 활용 창업경진대회 입상 · 제 7회 대한민국 SW융합 해커톤 대회 입상 · 인공지능 학습용 데이터 활용 아이디어 공모전 장려상 수상 · 청년 공공 빅데이터 인턴십 2기 수료
곽윤경	UI/UX & Real Time Object Detection	· **前 국민은행 IT서비스개발부 디지털서식관리시스템 담당** · 빅데이터 분석 연합동아리 BOAZ 17기 · 제스처(수어)인식 기반 그래픽 변환 연구 진행

ㅇ 서비스 아이디어의 창의성

- 마이 금융 데이터와, 표정을 분석하여 보이스피싱 피해 위험도에 대한 정확한 산출이 가능
- GT값*을 갖는 금융 데이터를 지속적으로 생성, 이를 통한 인공지능 알고리즘 고도화

*학습하고자 하는 데이터의 원본 혹은 실제 값

- 대면편취형 보이스피싱의 피해사례가 증가하는 추세에 신뢰할 수 있는 해결책

□ 활용 데이터 및 AI 모델

ㅇ 데이터 정의

출처	데이터 명	데이터 정보	메타 데이터	활용 알고리즘
AI HUB	한국인 감정 인식을 위한 복합 영상	50만장의 레이블링이 완료된 표정 데이터	성별, 나이대, 업로더 감정 정보, 업로더 배경 정보, Annotation A bounding box 좌표, Annotation B bounding box 좌표, Annotation C bounding box 좌표,	표정인식

Kaggle	Face Mask Detection	853장 마스크 착용, 미착용 이미지	name, pose, truncated, occluded, difficult, Bounding Box	마스크 추적
Oxford University	Hand Data Set	13,050 손 동작 데이터셋	point of bounding box	통화 유무 추적
마이 데이터 사업	계좌정보 - 거래내역	개인 금융 거래데이터	거래 일시(일자), 거래 유형(코드) 거래구분, 거래 금액	금융데이터 분석
마이 데이터 사업	대출상품정보 - 기본정보	개인 금융 거래데이터	대출차주명, 대출일	
마이 데이터 사업	대출팡품정보-잔액정보	개인 금융 거래데이터	대출 원금	
마이데이터사업	보험정보	보험 대출상품 기본정보 및 잔액정보	대출 실행일, 총 대출 금액, 대출 합계금액	
마이데이터사업	카드정보	카드 대출정보	단기대출목록, 장기대출목록, 단기대출이용일시, 단기대출이용금액, 장기대출일시, 장기대출이용금액	

ㅇ 데이터 Preprocessing Pipeline

- 전체 데이터에 대하여 개인정보 보호법에 의거한 가명처리를 명확히 진행 후 활용 예정
- (금융데이터) 빅데이터 탐색적 분석방법 기법을 활용하여, 보이스피싱 피해 여부 분석에 필요한 성질들을 추출
- (이미지 처리 데이터) 높은 성능을 달성하기 위하여, 전체 데이터 중 목적에 필요한 부분만 추출 및 전처리하여 개발 진행
- 사업화 이후, 금융 데이터등의 개인정보보호에 만전을 기하기 위해 개인정보보호 보험 가입 예정

ㅇ 인공지능

- 인공지능 모델은 아래의 마스크 착용 여부 및 통화 유무 여부 확인 알고리즘, 표정인식 알고리즘, 마이데이터 분석 모델을 결합하여 보이스피싱 피해 여부를 포착함
- 마스크 착용 여부 및 통화 유무 여부 확인 알고리즘
  · 실시간 이미지 분류 시스템에 높은 성능을 보이는 YOLOR모델과 YOLOv4-CSP모델의 테스트 알고리즘을 만든 후 적합한 모델 선정 예정
- 표정인식 알고리즘

· 보이스피싱 위험도는 ATM에 내장된 카메라를 통해 데이터를 클라우드에 탑재된 AI 소프트웨어에 전송하여 위험도를 계산하는 방식

· 보이스피싱 피해자 예방을 위한 AI 알고리즘은 표정 인식 개발 중 가장 성능이 높다고 평가되는 알고리즘을 후보군으로 하여 테스트할 예정

· 테스트 결과 학습용 데이터셋에 가장 높은 효율을 보이는 모델을 최종 모델로 선정하여 개발 예정

· 추후 GT값을 갖는 데이터셋 구축을 병행하며, 해당 데이터 기반 Fine Tuning*을 진행, 고도하 예정

*사전학습 된 모델을 활용하여 새로운 모델을 학습하는 과정을 말함

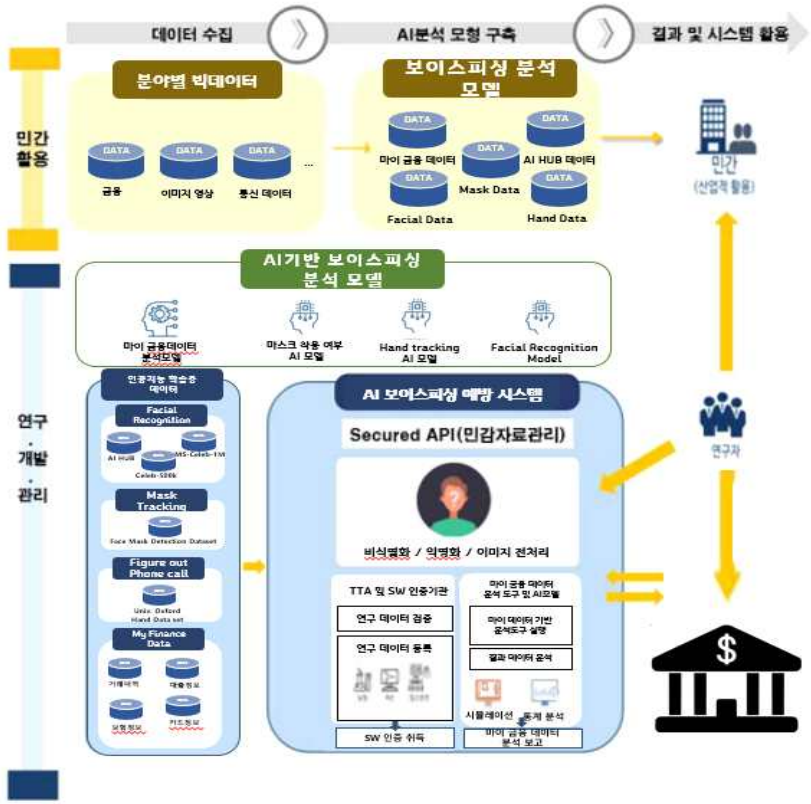
<표정인식 인공지능 학습 알고리즘 성능평가>

모델	논문
Multi-task EfficientNet-B2	Facial Expression And Attributes Recognition based on multi-task learning of lightweight neural networks
DAN	Distract your attention: Multi-head cross attention Network for Facial Exrpession Recognition
SL+SSL in-panting-pl	Using Self-Supervised Auxiliary Tasks to Imporve Fine-Grained Facial Representation
Distilled Student	Leveraging Recent Advances in Deep Learning for Audio-Visual Emotion Recognitnion
ARM (ResNet-18)	Learning to Amend Facial Expression Repersentation Via De-Albino and Affinity
SL+SSL puzzling	Using Self- Supervised Auxilary Task to imporve Fine-Grained Facial Representation

※ 가장 높은 성능의 알고리즘(State-of-the-Art)를 평가하는 Paperswithcode 기준 상위6개를 선정

- 마이데이터 분석 모델
  · 사용자의 금융데이터를 활용하여, 금융 거래 내역의 변동을 분석, 보이스피싱 의심 행위 패턴을 파악
  · 마이데이터 사업에서 제공하는 개인 금융데이터를 기반으로 탐색적 분석을 실시하여 보이스피싱 피해 위험도 산출에 적합한 변수 추출 예정
- 데이터 공정성
  · 인공지능 SW 학습 시 정상군 데이터와 비 정상군 데이터의 비율을 추적 관리하여 인공지능 알고리즘 성능에 대한 공정성과 성능에 대한 신뢰도를 입증할 예정

<서비스 모델 아키텍처>



6 기대효과

□ 사회적 기대효과

ㅇ 개인

- 보이스피싱 사전적 대응체계에 기인한 사전예방을 통해 안전한 금융거래 활성화 및 피해 예방 프로세스 확립
- 법·제도의 사각지대에 있는 대면편취형 전기통신금융사기에 대하여 피해사례 감소 효과

ㅇ 사회

- 인공지능 SW는 표정의 주요 포인트, 개인 금융 기록의 갑작스러운 변화 등을 파악, 피해사례와 비교 분석하여 금융사기 여부를 인지하는 방식으로
  - 정부기관 사칭의 고전적 방식은 물론 대출사기 등 첨단화·교묘화하는 보이스피싱 범죄의 선제적 차단이 가능하여 인공지능 SW가 활성화 될 경우 보이스피싱 피해예방에 상당한 효과가 있을 것으로 전망
- 금융 분야 인공지능 학습용데이터 구축
  - 금융 보안분야 고품질 인공지능 학습용데이터 구축을 통하여 금융 보안분야 D.N.A.(Data-Network-AI)생태계 강화

□ 경제적 기대효과

- 2008년부터 현재까지 전기통신 금융사기로 인한 피해액은 총 3조에 달하며 대부분의 자금이 해외로 유출 됨
- ABCDS기술을 통해 전기통신 금융사기를 사전에 예방하여 국민 소득에 대한 해외 유출을 예방 및 피해 구제금액 감축

□ 산업적 기대효과

ㅇ 금융 업계

- ABCDS기술을 바탕으로 스미스 피싱, 보이스 피싱 등에대한 지속적 관리를 통해 소비자들에게 '차세대 금융 보안 선도 기업' 브랜드 이미지 구축

※ 분량제한은 없으며, 공모요강에 적시된 평가항목을 참고하여 작성하여 주시기 바랍니다.
(상세 설명을 위해 도표, 스케치 등 별도파일 추가 가능)

참고1 전기통신금융사기 방지대책 추진현황

□ 전기통신금융사기 현황

○ 전기통신금융사기는 인터넷, 전화 등 전기통신을 이용하는 금융사기의 일종으로,

○ 보이스피싱으로 불리는 피싱부터 해킹 까지 유형이 다양하며, 범죄방식과 피해양상이 확대 및 다변화 되고 있음

○ 경찰청에서 집계한 피해액 추이를 살펴보면 2006년에는 106억원에서 2020년 7,000억원으로 증가함

□ 문제점

○ 전기통신금융사기의 피해규모가 확대되고 있음에도, 피해자가 피해구제를 신청하여 피해금을 환급받는 비율은 2015년부터 2020년 간 평균 30%로 나타나고 있음

| 2015년~2020년 연도별 피해현황 및 피해금 환급률 |

(억원, 건, %)

구분	2015년	2016년	2017년	2018년	2019년	2020년
피해금(A)	2,444	1,924	2,431	4,440	6,720	2,353
피해건수	57,695	45,921	50,013	70,218	72,488	25,859
환급액(B) (환급률 : B/A)	822 (33.6)	423 (22.0)	598 (24.6)	1,011 (22.8)	1,915 (28.5)	1,141 (48.5)

자료: 감사원 감사보고서, 『전기통신금융사기 방지대책 추진실태』, 2020, p.9. ; 금융감독원 보도자료

※ **금융감독원 집계는 「통신사기피해환급법」 적용 대상이 아닌 '대면 편취형'으로 인한 피해는 집계에서 제외하고 있으므로, 피해금이 하락한 것으로 명시 됨**

□ 개선방안

○ 정부는 '전기통신금융사기 방지대책 협의회'를 설치하여 보이스피싱 범죄에 대한 대응에 착수함

○ 보이스피싱 방지 앱 활성화 및 범부처 차원의 협력 강화 등 보이스피싱 피해 규모를 줄이기 위해 다방면에서 적극 노력 중

○ 디지털 뉴딜의 일환으로 전자금융사고에 대해 금융회사 등 책임 강화*

* (현행) 공인인증서 위·변조 등 특정한 기술적 사고에 한해서만 배상 책임
(개선) 이용자가 미허용한 전자금융거래에 대해 책임, FDS(Fraud Detection System) 강화

○ 피해방지를 위해서 민간·통신·수사당국 모두의 협력이 필수적인 만큼 이들의 보이스피싱

방지의무를 법에 명시

- 금융회사등의 보이스피싱 모니터링시스템·전사적 방지체계 의무화 추진

참고2 산출물 관리 및 평가를 통한 사업화 추진 계획(안)

□ 산출물

○ 요구사항 분석서, SW설계서, 소스코드 등에 대한 산출물 등을 문서화하여 관리 지속적 관리 실시 예정

○ AI소프트웨어 보급확산 시 성능에 신뢰도를 제시하기 위해 TTA 인증 및 CE 인증 등을 준비할 예정

○ 해당 인증제도를 취득하기 위한 산출물에 대한 지속적 관리 필요

<AI 소프트웨어 개발에 따른 산출물 관리계획 방안>

단계	활동	산출물	산출시기
분석	요구사항 정의	요구사항분석서 (자체 분석)	요구분석 완료후 2주
	아키텍처 정의		
	요구사항 분석		
설계	개략설계	설계서	상세설계 완료 후 2주
	상세설계		
구현 및 테스트	테스트 준비	시험평가계획서	구현 완료 후 4주
	구현	프로그램 소스코드	개발 완료시
	통합시험	시험평가결과서	테스트 완료 후 1주
	지침서 작성	사용자 메뉴얼	테스트 완료 후 3주
완료	개발 완료	최종보고서	과제종료시

□ 품질 관리 계획

○ 시스템 검증 계획

- 성능평가

· 개발 2차년도 기점 연차별 R&D 결과물의 성능평가를 위해 TTA*등 공인시험기관을 통해 정량적 목표치 달성여부에 대한 검증을 실시하여 품질 성능을 제시할 예정

*「소프트웨어산업진흥법」 제13조에 의거하여 소프트웨어 품질을 인증하는 기관

· 인공지능 정확도 이외의 부분에서 성능평가 필요시 외부 전문기관(금융기관)을 통해 평가 진행 예정

<성능평가 계획>

* 인공지능의 객관적 성능 검증을 위해 공인인증 기관인 TTA에 개발 2차년도 이후부터 매년 시험을 의뢰 함, 통과 기준은 매년 초 설정한 정량적 목표치를 넘으면 통과로 정의 예정

* 평가는 TTA에서 무작위 Sampling을 통하여 데이터를 인공지능 알고리즘에 넣어, 정답 여부를 평가함

* 인공지능 알고리즘에 넣을 때 마다 서버에 로그가 생성되고, 그 생성된 로그와 인공지능 파일 모델의 hash값을 제공함으로써, 인공지능으로 판독했다는 정보를 TTA에 재공하고, 통과 여부와 서버의 로그, 파일 모델 등의 정보를 모두 통합하여 TTA에서 인증서를 발급 할 예정

참고3 서비스 시스템 구성 및 서비스 절차 세부계획

□ 위험도 산출 공식

○ 위험도는 전화 여부 가중치와 표정의 당황함과 불안함에 대한 확률 가중치와 이상거래데이터 위험 탐지를 모두 더한 값으로 한다.(전문가에 의해 수치 조정 가능)

$$risk = w_{call} + w_{\mathrm{expression}} + w_{abnormal}$$

○ 전화 여부의 가중치는 전화를 받고 있는 상태면 0.3을 받고 있지 않으면 0.1로 설정

$$w_{call} = \begin{cases} 0.3 & call \\ 0.1 & no\,call \end{cases}$$

○ 불안 표정 인식은 모델이 표정이 당황함으로 인식할 확률과 불안함으로 인식할 확률을 더한 값에 0.3을 곱함

$$w_{\mathrm{expression}} = (P_{\mathrm{embarrassment}} + P_{\mathrm{unrest}}) \times 0.3$$

○ 이상거래데이터는 이상거래 점수(x_{score})에 0.4를 곱함

$$w_{abnormal} = x_{score} \times 0.4$$

○ 이상 거래 데이터는 다음과 같은 항목을 고려(전문가에 의해 항목 조정 가능)

$$x_{score} = x_1 + x_2 + x_3$$

1. 여수신정보(x_1)

ATM 출금 금액 > ATM 이용 당일 기준 한달 전 ATM 출금 데이터의 Q3+1.5*IQR 일 경우
: 0.4점

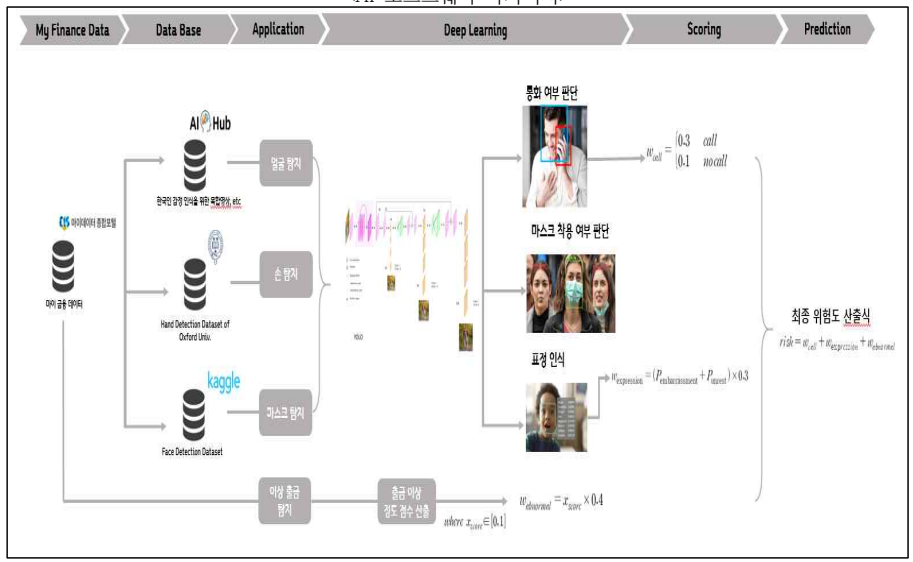
2. 보험 정보(x_2)

ATM 이용 당일 or ATM 이용 당일 포함 3일 전까지 받은 대출 금액 > ATM 이용 당일 기준 6개월 or 1년 전 받은 대출 금액 데이터의 Q3+1.5*IQR 일 경우
: 0.3점

3. 카드 정보(x_3)

ATM 이용 당일 or ATM 이용 당일 포함 3일 전까지 받은 대출 금액 > ATM 이용 당일 기준 6개월 or 1년 전 받은 대출 금액 데이터의 Q3+1.5*IQR 일 경우
: 0.3점

<AI 소프트웨어 아키텍처>



<서비스 프로토콜>