

## 프로젝트 요약서

# 보 고 서

프로젝트명 : 사용자 음성을 활용한 서비스 사용자 인증 및 접근  
제어 시스템 개발

교과목명	기업사회맞춤형프로젝트	
담당교수	임대운	
팀명	SIN(Shield INformation)	
팀원	학 번	이 름
	2014112081	정세인
	2017112154	웅웬딩 호영
	2018112013	이서연
	2018112042	송승민

제출일자: 2020년 7월 4일

보고서 목차

설계과제명	사용자 음성을 활용한 서비스 사용자 인증 및 접근제어 시스템 개발
주요기술용어 (2~7개 단어)	음성인식, gmm, 보안, 암호화, 랜덤텍스트, 접근권한
<div>1. 목표</div> <p>현재 사용자 인증 및 접근에서의 음성 인식이 인증 수단으로 이용되고 있다. 음성인식을 통한 인증 방식은 다른 인증 수단에 비해 편리하다는 장점이 있는 반면에, 사용자 음성 위조·변조 등 기술한계로 인해 보안에서 취약해질 수 있다는 문제점을 지닌다. 본 설계에서는 기존 사용자 음성을 활용한 사용자 인증의 보안취약점을 개선하고 보완하기 위해 추진한다.</p> <div>2. 수행 내용</div> <p>본 과제에서는 사용자의 목소리를 인증매체로 사용하면서 기존의 인증방법 보다 더 강화된 보안을 목표로 한다.</p> <p>회원가입 시 음성인증을 위한 음성 인식 인증 기능을 추가하였다. 사용자는 기존 아이디와 패스워드를 통하여 로그인할 수도 있고, 아니면 아이디와 음성 인식 기능으로 로그인을 할 수 있다. 사용자는 이 둘 중 하나를 선택할 수 있다.</p> <p>랜덤 텍스트를 생성하여 사용자가 그 텍스트를 말하고 해당 텍스트가 맞고 목소리 일치율이 넘어야 인증이 성공한 것으로 해서 음성인증 보안을 고도화하였다.</p> <p>frontend를 nodejs와 reactjs framework를 이용하여 UI를 개선하였고, 예제 서비스인 은행 시스템을 구현하였다. 인증을 성공하여 접근 권한을 부여받은 사용자는 이 은행 시스템을 이용할 수 있다. 데이터베이스(mysql)를 연결하여 회원 가입한 사용자의 음성과 아이디 및 패스워드를 저장하였다.</p> <div>3. 수행 결과</div> <p>사용자는 기본 정보인 아이디와 패스워드, 이메일 등을 입력하여 회원가입이 가능하다. 이에 더하여 사용자는 정보와 마찬가지로 목소리 또한 저장하여 음성 인식 인증 기능을 추가할 수 있다. 로그인 시, 사용자는 아이디와 패스워드로 로그인이 가능하며, 음성 인식 인증 기능이 추가된 사용자는 아이디와 음성 인식으로도 로그인이 가능하다. 아이디 비밀번호로 로그인하는 것은 기존과 동일하게 데이터베이스에 저장된 내용들을 비교하여 로그인이 가능하다. 아이디, 음성인식으로 로그인을 할 때, 사용자는 먼저 아이디를 입력하고 음성 인식을 진행한다. 음성 인식 시, 랜덤 텍스트가 생성되며 사용자는 그 랜덤 텍스트를 그대로 따라 읽으면 된다. 만약 따라 말한 랜덤 텍스트가 일치하고, 데이터베이스에 저장된 목소리와 방금 목소리와 일치한다면 사용자는 로그인에 성공하여 접근 권한을 부여받게 된다. 접근 권한을 부여받은 사용자는 은행시스템을 이용할 수 있다.</p> <div>4. 결과 분석</div> <p>본 프로젝트의 결과물은 기존의 아이디와 패스워드뿐만 아니라 목소리를 인증 매체로 활용한다는 점에서 보안의 측면을 높일 수 있다. 이는 카드 번호나 비밀번호 등 복잡하고 외워야 하는 기존의 방식과 달리 사용자의 목소리를 인증 매체로 사용한다면 간단함은 물론이고, 고유의 생체 인증이기 때문에 더욱 보안이 뛰어난 효과를 기대할 수 있다.</p> <p>또한 보안 부분에서 랜덤 텍스트를 생성하여 사용자가 말한 단어를 비교하여 일치할 경우에만 접근 권한을 부여하기 때문에 음성 녹음, 유출을 통한 피해를 방지할 수 있으며, 음성 파일 암호화와 음성 파일 경로 암호화, gmm파일 경로 암호화, 비밀번호 암호화를 통하여 보안을 고도화하여 향상된 보안 성능을 기대할 수 있다.</p>	

1. 서론
- 1.1 문제 정의
- 1.2 설계 주제 및 목적
2. 배경
- 2.1 관련 기술의 동향
- 2.2 관련 기술의 수요 및 전망
3. 요구사항 분석
- 3.1 기능 요구 조건
- 3.2 성능 규격 조건
4. 제한요소
- 4.1 동작환경
- 4.2 개발환경
- 4.3 개발비용
- 4.4 사회성
5. 설계
- 5.1 설계목표
- 5.2 설계안
- 5.3 평가 항목과 평가 방법
- 5.4 대안 분석
6. 구현
- 6.1 구현 방법
- 6.2 구현 도구

## 7. 결과

### 7.1. 결과물 설명

### 7.2. 결과물 분석

### 7.3. 기대성과

## 8. 작업 진행 방법

### 8.1. 작업 분담 구조

### 8.2. 설계 일정 및 역할 분담

### 8.3. 예산집행내역

## 9. 결론

### 9.1 결론

### 9.2 결과 분석

### 9.3 향후 계획 및 일정

## 10. 참고문헌

## 1. 서론

### 1.1 문제 정의

현재 사용자 인증 및 접근에서의 음성인식이 인증 수단으로 이용되고 있다. 음성 인식을 통한 인증 방식은 다른 인증 수단에 비해 편리하다는 장점이 있는 반면에, 사용자 음성 위조·변조 등 기술한계로 인해 보안에서 취약해질 수 있다는 문제점을 지닌다. 본 설계에서는 기존 사용자 음성을 활용한 사용자 인증 및 접근제어 시스템의 보안취약점을 개선하고 보완할 방안을 제시하고 이를 구현한다.

### 1.2 설계 주제 및 목적

서비스 인증을 하기 위한 여러 방법이 제시되면서 그 중 하나로 음성 인식을 예로 들 수 있다. 음성인식 서비스를 제공하기 위해서는 각각의 사용자를 구분하며 보안을 지킬 수 있어야 한다. 이번 설계 주제는 이러한 보안 이슈를 해결하기 위해 사용자 음성을 사용한 서비스 사용자 인증 및 접근제어 시스템 개발을 주제로 한다.

기존 음성 인식을 통한 인증방식은 사용자 음성 위조·변조 등 기술한계로 인해 보안에서 취약해질 수 있다는 문제점을 지닌다. 이 설계에서는 사용자 인증을 통해 이를 해결하고자 한다. 첫째, 사용자는 사전에 서비스 시스템에 계정을 생성하고 인증 수단(음성 인식)을 등록한다. 둘째, 사용자는 서비스 이용 시 등록된 인증 수단을 활용하여 인증값을 생성하여 서비스 시스템에 제시한다.

셋째, 서비스 시스템은 사용자 음성 인식 기반 인증 및 접근제어 시스템을 활용하여 사용자가 제시한 인증값에 대한 검증을 실시한다. 또한 사용자 인증 및 접근제어 시스템의 결과 값에 따라 서비스 시스템은 사용자의 서비스를 사용할 수 있도록 접근 권한을 부여한다.

위의 방법을 차례로 거치며 이를 통해 음성인식을 통한 보안 문제를 해결하고자 한다.

## 2. 배경

### 2.1 관련 기술의 동향

음성은 사람의 의사전달 수단으로서 언어정보, 화자정보, 감정정보, 건강상태, 발생환경 등과 같이 여러 가지 정보를 포함한다. 음성기술은 음성을 가공하여 실생활에 활용하기 위한 모든 기술들을 포함하며, 음성코딩, 음성인식, 화자인식, 음성이해, 음성강화, 음성합성 등이 있다. 음성을 제한된 채널을 통하여 효율적으로 전송하기 위한 음성코딩(Speech Coding)을 음성정보처리의 기본이라 할 수 있으며, 최근에 대중화된 휴대폰의 요소기술의 하나이다.

이 중에서 음성 인식 기술은 일상생활에서 사람들 사이의 음성언어를 사용하여 정보기기를 제어하거나 정보 서비스를 받을 수 있도록 말과 글을 처리하기 위한 생체인식 기술의 한 분야로 음성신호에 내재되어 있는 정보를 분석하여 글자나 문장을 바꾸어준다.

국내 음성 인식 기술 시장은 IT 산업의 새로운 인터페이스 및 차세대 인터페이스 기술로 각광을 받으면서 2000년대 들어 업체 수의 증가로 인한 경쟁 심화와 정부의 지원사업 감소, 시장 수요 위축 등 악재가 겹치면서 침체의 길로 접어들었다. 현재 국내의 주요 음성 인식 업체들은 수익을 내는데 급급한 모습을 보이며, 일부 업체들은 회사를 정상적으로 유지하는 데에도 심각한 어려움을 겪고 있는 것으로 알려졌다.

그러나 음성 인식 기술은 차세대 사용자 인터페이스 기술의 핵심요소로서 선진국의 연구기관 등에서 21세기 정보화 사회를 선도할 주요 유망 기술로 선정되고, 기술개발 및 음성 DB 자원 확보에 대규모 투자가 되고 있다.

### 2.2 관련 기술의 수요 및 전망

<국내>

－공항: 인천공항

2019.09 인천공항에 음성인식 키오스크(KIOSK·무인 정보단말기) 도입하였다. 전세계 공항 최초 시범 서비스 도입을 목표로 'AI(인공지능) 기반 음성 인식 스마트 사이니지 구축사업'을 착수하였다. 12월께 1터미널 출국장 6개소 도입하였다. 노약자와 시각장애인에게 도움 될 것이다. 스마트 사이니지는 음성 인식(STT) 기술에 인공지능 기술을 접목해 여객들의 반복적인 요청사항을 학습함으로써 음성 인식 및 안내의 정확도를 높인 것이 특징이다. 음성 인식을 보안에 사용하려면, 정확도가 높아야 한다. 인증 수단으로 음성 인식을 활용하여 보안을 강화할 수 있다.

－유통: CJ대한통운

2019.04 택배기사와 매일 동행하며 필요한 정보를 실시간으로 안내해주고 고객 문의에 즉시 답변을 해주는 택배기사용 인공지능(AI) 가상비서가 등장하였다. 음성 인식(STT), 음성합성(TTS), 자연어처리(NLP) 등 다양한 AI 기술을 융-복합해 사용자 환경에 최적화하였다. 하루 동안 이뤄지는 택배 프로세스를 작업자의 관점에서 9단계로 세분화해 분석한다. 작업 단계별, 시간대별로 택배기사에게 가장 필요한 데이터, 검색 빈도가 높은 자료, 정확도와 효율성을 높일 수 있는 정보들을 빅데이터화하여 가상비서에 학습시킨다. 텍스트로 받은 내용을 고객 의도 및 문의 유형에 따라, 가상비서가 스스로 판단해 음성 또는 텍스트로 변환해, 최적화된 답변을 제공하는 하이브리드 대화 기술을 적용했다. 이에 따라 배송 일정, 상품 종류, 착불 요금 입금 계좌 등 문의 문자가 올 경우 가상비서가 택배기사를 대신해 고객에게 답장을 보낸다. 배송 일정 변경, 위탁 배송지 지정, 방문 시 주의사항 등 요청사항이 인입될 경우 음성과 푸시 알림을 통해 택배기사에게 안내한다. 유통 산업에서 쓰인 것처럼, 모바일 단말에서도 음성 인식을 이용한 보안을 적용할 수 있고, 빅데

이터를 학습시켜 인증과 가용성 측면에서 높은 효율성을 보일 수 있는 보안 방법이다.

－보험: 신한생명

2018.09 신한생명은 음성 인식(STT) 솔루션을 도입하여, 챗봇 시스템과 직원교육(맞춤형 영업 가이드, 영업 우수사례 발굴 및 영업코칭 활성화)에 활용할 예정이다. STT로 통화 내역의 음성과 일을 텍스트 데이터로 전환해주는 시스템을 적용하여, 빅데이터를 기반으로 고객 상담 품질과 영업 효율성 개선했다. 직원 교육과 같은 회사 내부자료와 고객 상담에서 나오는 고객 정보는 정보 보호가 필요한 부분이다.

－보험: DB손해보험

DB손해보험은 아이폰 'Siri'와 연계해 목소리로 긴급출동 서비스를 접수 받는다. 음성 인식 긴급출동 서비스를 한 번 설정 후에는 앱이 실행되지 않은 상태에서도 Siri에 '긴급출동'이라고 음성 명령을 하면 바로 긴급출동을 신청하는 화면이 실행된다.

<해외>

－본인인증: 캐나다 매뉴라이프

캐나다의 매뉴라이프는 미국 소프트웨어 회사 '뉘앙스'(Nuance)와 협력해 음성 인식 기반 본인인증 시스템을 도입했다. 매뉴라이프는 자연 언어이해 및 음성 생체인식 기술을 통해 발음, 강조, 악센트 등을 포함한 100개가 넘는 고유한 음성 특성을 분석해 개개인의 목소리 특성만으로 고객의 본인 여부를 인증한다. 목소리가 비밀번호를 대체하기 때문에 인증에 걸리는 시간을 줄이는 효과가 있다.

－고객의 스트레스 수준 정보 제공: 미국 메트라이프

미국의 메트라이프는 콜센터 상담원과 고객 간의 대화 시 인공지능이 고객의 감정을 분석해 콜센터 상담원들에게 고객의 스트레스 수준 정보를 제공한다. 고객의 감정은 대화 속도, 대화 중 일시 중지, 대화량, 목소리의 톤 및 피로도 등을 측정해 분석. 고객의 감정 상황에 따라 말을 멈추거나, 시작하거나, 동조감을 표시하도록 화면에 제시하면서 최초 민원 통화 해결은 3.5%, 고객 만족도는 13% 향상됐고 평균 통화시간은 절반으로 단축된다.

－정신 및 감정적 반응 식별: 이스라엘 네메시스코(Nemesysco)사

이스라엘 네메시스코(Nemesysco)사는 계층형 음성분석(Layered Voice Analysis: LVA) 기술을 통해, 숨겨진 정서적 신호를 감지해 대상의 정신 상태와 정서적 반응을 정확히 이해, 다양한 유형의 스트레스 수준, 인지 과정 및 감정적 반응을 식별해낸다. 또 '정서 다이아몬드'(Emotional Diamond) 개념을 개발해 LVA가 감지한 복잡한 정서적 반응을 시각화된 심리 분석으로 제공하고 이를 바탕으로 보험사거나 사기 의도가 있을 확률을 예측 가능하다.

위와 같은 국내외 해외 사례를 통해, STT를 이용한 사용자 인증 및 접근제어 시스템을 인증, 기밀성, 무결성, 가용성 측면에서 효과적으로 만들 수 있다.

### 3. 요구사항 분석

#### 3.1 기능 요구 조건

본 설계의 목표를 달성하기 위해 다음의 기능적 요구들이 필요하다.

사용자 음성을 활용한 서비스 사용자 인증 및 접근 제어 시스템

- 사람의 목소리를 인식하는 마이크
- 사용자 계정 생성 및 인증 수단(음성 인식) 등록
- 사용자 목소리 저장하는 데이터베이스
- 기 등록값과 입력받은 음성을 비교하는 기능(검증)
- 비교 결과에 따라 접근 권한 부여
- 음성 인식된 내용을 문자 데이터로 전환 처리하는 기능
- PC 또는 모바일 단말에서 운용
- 예제 서비스(예 은행, 쇼핑몰 등)에서 활용

#### 3.2 성능 규격 조건

본 설계의 목표를 달성하기 위해 사용자 음성을 활용한 서비스 사용자 인증 및 접근 제어 시스템은 다음의 성능을 만족해야 한다.

- 마이크의 목소리 인식률 : 90% 이상
- 사용자 목소리 인식할 때의 시스템 반응시간 : 0.3ms 이하
- 등록값과 입력받은 음성 비교 시 비교오차율 : 1% 이하
- 음성 인식 내용의 문자 데이터화 처리 정확도 : 98%
- 사용자 계정을 저장하는 데이터베이스의 존재
- 사용자 목소리를 저장하는 충분한 데이터베이스 공간의 존재
- PC 또는 모바일 단말에서 운용 가능하도록 하는 접근성
- 서비스에서의 활용도 및 사용자가 느끼는 편리함 증대

### 4 제한요소

본 설계에서 고려해야할 중요한 제한요소들을 동작환경, 개발환경, 개발비용, 사회성 순서로 다음에 기술하였다.

#### 4.1 동작환경

본 설계 대안 생성 및 선택에 영향을 줄 만한 사항을 다음과 같다.

서비스에 등록되지 않은 사용자는 음성인증 시 접근권한을 부여받을 수 없다.  
서비스에 등록되지 않은 사용자는 자신의 계정을 등록 할 수 있다.  
서비스에 등록된 사용자는 음성인증 시 다른 사람의 계정에 접근할 수 없다.  
서비스에 등록된 사용자는 부여된 접근권한 이외의 권한을 가질 수 없다.  
음성 위.변조 프로그램을 이용하여 사용자의 계정에 접근할 수 없다.

#### 4.2 개발환경

음성 인식 방법은 크게 화자독립(Speaker-Independent), 화자종속(Speaker-Dependent), 화자 인증(Speaker-Verification)으로 나눌 수 있다. 이러한 음성 인식 방법 중 보안에 관련된 것을 화자종속과 화자인증이다. 두 가지 방법 공통으로 화자의 음성 데이터를 기 사용 시의 음성 인식 알고리즘을 사용하여 획득했던 음성 데이터와 비교를 통해서 결과를 도출하는 방법을 사용하고 있는데. 이 방법에 시간이 많이 걸리고 작업하기 힘들지만 정확도 높은 정점이 하나이다.

이는 음성 인식을 하기 위해서 마이크를 통해서 들어온 음성은 프리엠프, 아날로그-디지털 컨버터, 로직 등의 음성 인식에 필요한 과정을 통해서 디지털 데이터화되고 외부 메모리에 저장되어 있는 기기 사용 시 추출된 음성 특성 데이터와 중앙 처리장치 혹은 마이크로 컨트롤러(MCU)에 의해 비교/연산되어지고, 그 결과 값 즉 사용자의 진실 여부를 외부에 전달하게 된다.

이러한 음성 인식 과정에서 음성 인식율에 가장 큰 영향을 끼치는 요인을 마이크를 통해 입력된, 인식해야할 음성 외에 첨가되는 주위의 노이즈이다. 또한 화자의 목소리 변화도 음성 인식율에 많은 영향을 준다. 이런 문제들을 최대한 노이즈를 줄기 위해서 좋은 마이크, 목소리에 큰 문제가 없는 사용자 또한 조용한 환경에서 권한다.

#### 4.3 개발비용

필요한 부품 또는 자재의 구입예산은 동국대학교 산학연계 캡스톤디자인 교과목의 지원금(100만원)을 한도로 한다.

#### 4.4 사회성

본 설계에 의한 음성 인식을 통해서 사용자 인증을 하면, 단일 기기를 사용할 때의 보안/인증 절차보다 한 단계 더 강도 높은 사용자 인증을 수행하는 효과가 있으며 편리성을 높여지게 된다. 최근에 클라우드 서비스를 사용할 때 가장 큰 문제점은 바로 보안 위협인데 이 중에서 사용자 인증, 자격 증명이 하나이다.

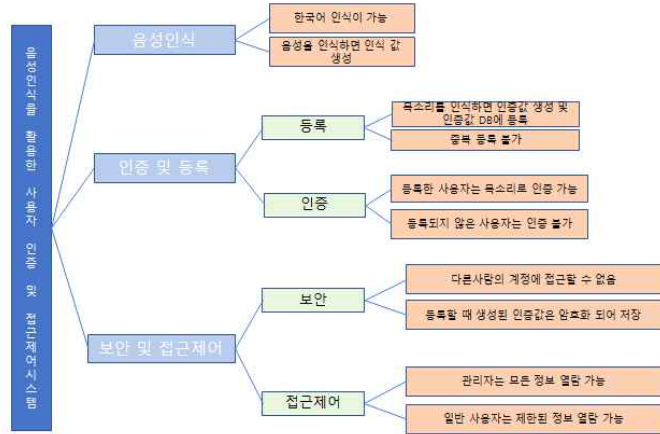
예를 들면 합법적인 사용자, 운영자 혹은 개발자로 가정한 공격자를 데이터를 읽고 수정하고 삭제할 수 있다. 또한 제어 및 관리 기능을 통해서 전공 중인 데이터를 엿보거나 합법적인 소스를 가정보록 악의적인 소프트웨어를 배포할 수 있다. 이들과 같은 더 많은 문제가 존재되어 있으며 결과적으로 ID, 자격 증명 또는 키 관리자 제대로 되지 않으면 데이터에 대한 무단 액세스를 허용하게 되고 조직이나 최종 사용자에서 치명적인 피해를 입힐 수 있다.

이 보안 문제들을 정확히 해결하려면 쉽지 않은 일이라고 판단한다. 여러 방법중에서 생체 인증을 위한 음성 인식을 통해서 대표적이다. 다만 예방 제어는 최대한 모든 경계선에 적용될 것을 권고한다. 조직은 매니지드, 공유, 퍼블릭 환경 등에서도 취약점을 검색해야 한다.

## 5. 설계

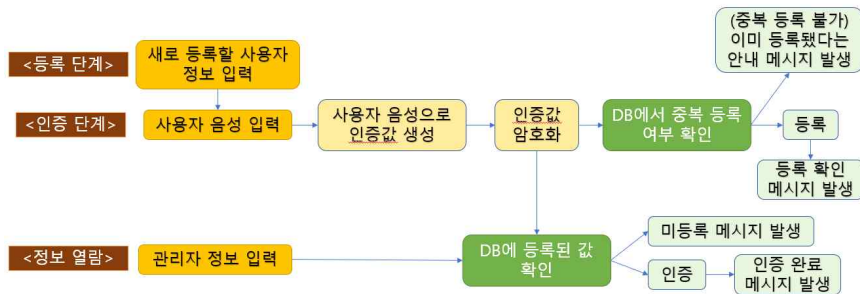
### 5.1 설계목표

#### <목적나무>



### 5.2 설계안

#### <설계도>



### 5.3 평가 항목과 평가 방법

평가항목	평가기준	근거 (보통기준)	평가점수				
			아주미흡 (1)	미흡 (2)	보통 (3)	우수 (4)	아주우수 (5)
월별 API 사용 비용	만원	20	80	50	20	10	5

평가항목	평가기준	근거 (보통기준)	평가점수				
			아주미흡 (1)	미흡 (2)	보통 (3)	우수 (4)	아주우수 (5)
다수의 사용자처리 (목적)	명 수	2000	20	40	60	80	100
DB서버의 네트워크 액세스 (목적)	%	50	20	40	60	80	100
Micro를 통한 물품 정보입력 (목적)	%	50	20	40	60	80	100

평가항목	평가기준	근거 (보통기준)	평가점수				
			아주미흡 (1)	미흡 (2)	보통 (3)	우수 (4)	아주우수 (5)
DB와의 연동 (목적)	%	50	20	40	60	80	100
다양한 방식의 물품 정보저장 및 검색 (목적)	%	50	20	40	60	80	100
설치 편의성 (동작환경제한요소)	%	50	20	40	60	80	100

평가항목	평가기준	근거 (보통기준)	평가점수				
			아주미흡 (1)	미흡 (2)	보통 (3)	우수 (4)	아주우수 (5)
개발편의성 (개발환경 제한요소)	%	50	20	40	60	80	100
User Interface 개발 편의성 (개발환경 제한요소)	%	50	20	40	60	80	100
개발후 유지보수 (개발환경 제한요소)	%	50	20	40	60	80	100

평가항목	평가기준	근거 (보통기준)	평가점수				
			아주미흡 (1)	미흡 (2)	보통 (3)	우수 (4)	아주우수 (5)
경제성 (제한요소)	%	50	20	40	60	80	100

평가항목	평가기준	근거 (보통기준)	평가점수				
			아주미흡 (1)	미흡 (2)	보통 (3)	우수 (4)	아주우수 (5)
일정 (제한요소)	일수	10	20	40	60	80	100

#### 5.4 대안 분석

이 설계는 naver STT에서 제공해준 API으로 대안으로 개발을 진행해 온 프로젝트다. 기존 설계에서 오픈 소스를 이용하여 개발하지만 현재 상황을 보면 오픈 소스로 개발하는 작업이 어려울 것이다. 물론 오픈 소스로 개발하는 작업과 비교하면 REST API로 개발하는 작업이 쉽지만 소스 상속을 받아서 개발하기 불가능하므로 보안 고도화하기는 어려워서 아까운 점이 하나이다. 즉 사용자부터 음성 데이터를 받아서 API 서버를 보낸 다음에 분석 결과만 받아서 사용자를 인증한다.

	가중치	대안1	대안2	대안3
개요		Micro, Javascript, Node.js, Access를 사용한 재고관리	Micro, Javascript, Node.js, SQL Server를 사용한 재고관리	Micro, Javascript, Node.js, MySQL을 사용한 재고관리
다수의 사용자처리 (목적)	5%	Access를 사용하므로 다량의 데이터 및 다수의 사용자를 동시에 처리하는데 어려움이 있다. (점수: 50)	SQL 서버를 사용하므로 다량의 데이터와 다수의 사용자를 처리하는데 효과적이다. (점수: 100)	MySQL 서버를 사용하므로 다량의 데이터와 다수의 사용자를 비교적 잘 처리할 수 있다. (점수: 80)
DB서버의 네트워크 액세스 (목적)	5%	Access를 사용하므로 네트워크 연결을 통한 데이터 삽입, 삭제, 업데이트가 어렵다. 데이터의 분산 저장, 처리가 어렵다. (점수: 60)	네트워크 연결을 통한 데이터 삽입, 삭제, 업데이트가 가능하다. SQL서버를 사용하여 데이터의 분산처리 기능이 우수하다. (점수: 100)	네트워크 연결을 통한 데이터 삽입, 삭제, 업데이트가 가능하다. MySQL을 사용하여 데이터의 분산처리가 가능하다. (점수: 90)
Micro를 통한 물품 정보입력 (목적)	10%	Micro와 응용 프로그램간의 연동이 어렵다. (점수: 60)	Javascript 과 Micro 소프트웨어간에 연동이 용이하다. (점수: 100)	Javascript와 Micro 소프트웨어가 연동하는데 어려움이 있다. (점수: 70)
DB와의 연동 (목적)	5%	Access는 Visual Basic과 연동을 위한 기능을 잘 제공하고 있다. (점수: 100)	Microsoft SQL을 사용하므로 Node.js와 연동이 상대적으로 쉽다. (점수: 70)	DB와 Node.js를 연동하므로 연동이 상대적으로 쉽다. (점수: 90)
다양한 방식의 물품	5%	Access는 기능에 제한이 있다.	SQL Server가 다양한 기능을 제공하여 고급	무료배포용이지만 다양한 DB기능을 제공하고

정보저장 및 검색 (목적)		(점수: 60)	기능 개발에 편하다. (점수: 100)	있다. (점수: 90)
설치 편의성 (동작환경제한요소)	5%	Access는 보급형 PC나 사양이 떨어지는 PC에서도 잘 동작하여 학생 수준의 사용에 용이하다. (점수: 100)	SQL 서버 구축용으로 고사양의 PC가 필요하다. (점수: 70)	Javascript를 사용하므로 Windows가 아닌 PC에서도 사용가능하다. MySQL은 중급형 PC환경에서 무난히 돌릴수 있다. (점수: 90)
개발편의성 (개발환경제한요소)	15%	Access를 사용하므로 DB 학습 및 개발기간을 단축시킬수 있다. Visual Basic을 사용하므로 Access와 의 연동하여 동작하는 예제를 쉽게 얻을 수 있어 개발에 편리하다. (점수: 100)	Nodejs과 SQL 서버를 사용하며 이 개발도구들이 익숙하지만 관련 예제가 적거나 이해가 어려워 개발이 어려울 수 있다. (점수: 70)	Nodejs와 MySQL을 사용한 개발이 익숙하지 않지만 관련 예제가 많아 개발에 무리가 없다. (점수: 90)
User Interface 개발 편의성 (개발환경제한요소)	5%	Visual Basic을 사용하므로 User Interface 개발에 용이하다. (점수: 90)	HTML, Javascript를 통한 User Interface 개발이 어렵다. (점수: 80)	Javascript의 개발도구 (Visual Studio Code)를 사용한 User Interface 개발방법을 학습해야 하지만 예제가 많고 상대적으로 쉬워 개발에 무리가 없다. (점수: 80)
개발후 유지보수 (개발환경제한요소)	5%	Visual Basic을 사용하기 때문에 개발후 유지보수에 상대적으로 어려움이 있다. (점수: 80)	Javascript을 사용하기 때문에 유지보수에 상대적으로 쉽다. (점수: 100)	Javascript를 사용하기 때문에 유지보수가 상대적으로 쉽다. (점수: 100)
경제성 (제한요소)	25%	Visual Basic, Access 모두 교내 컴퓨터에 인스톨되어 있어 비용은 Micro구입비용 외에 추가로 들지 않는다. (점수: 100)	Micro구입비용과 SQL 서버 구축비용이 추가로 필요하다. (점수: 70)	Javascript는 무료 개발도구가 다양하고 MySQL은 무료이기 때문에 Mrcio구입비용 외에 추가 비용이 필요하지 않다. (점수: 100)
일정 (제한요소)	15%	15일 (점수: 100)	20일 (점수: 80)	15일 (점수: 90)
총합	100%	88	81	90

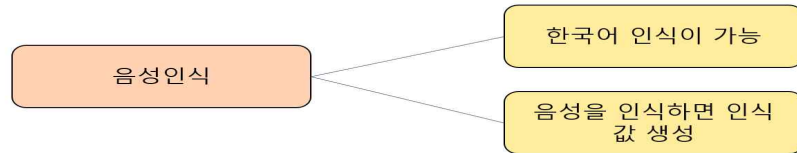
위 표에 의하여 최종 대안은 대안 3으로 결정하였다.

## 6. 구현

### 6.1 구현 방법

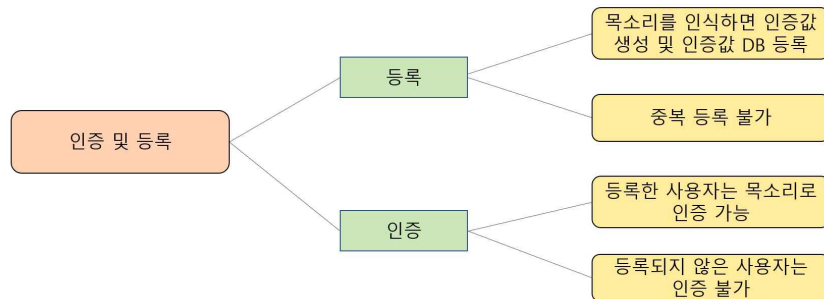
다음은 개발할 프로그램의 시스템 구조에 대한 구현방법이다.

#### <음성인식>



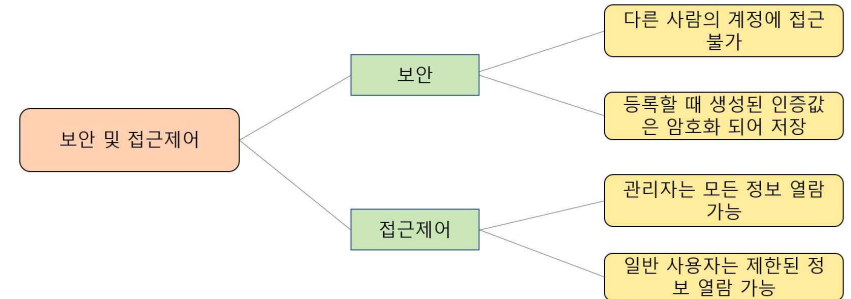
- naver STT API를 사용하여 음성인식을 진행한다. 먼저 사용자의 음성을 받아서 naver STT API로 보내 음성인식을 진행하여 인식값을 다시 전달받는다. 이런 과정을 통하여 음성인식과정을 수행한다.

#### <인증 및 등록>



- 등록에서는 전달받은 인식값을 Node js와 mySQL을 사용하여 데이터베이스에 등록한다. 이때 중복 등록은 불가능하다. mySQL 데이터베이스에 등록된 사용자는 목소리로 인증이 가능하며, 등록되지 않은 사용자는 인증서비스를 사용할 수 없다.

#### <보안 및 접근제어>



- 랜덤 텍스트, 경로 암호화 등을 이용하여 보안을 강화한다. 일반적으로 다른 사람의 계정에는 접근이 불가능해야 할 것이며, 등록할 때 생성된 인증값은 암호화하여 저장되어 있어야 한다. 또한 인증 절차를 거치고 난 후, 사용자는 정보에 접근 가능해야 할 것이고 인증에 따른 사용자가 누구인가에 따라 제한된 정보를 열람 가능한지 아니면 모든 정보에 대해 열람 가능한지를 구분하여 접근제어를 한다.

### 6.2 구현 도구

음성 인식 절차에는 naver STT API를 사용할 것이며, 인증 절차를 거친 사용자 정보는 Micro, javascript와 nodejs, mySQL을 사용하여 데이터베이스에 저장할 것이다. 보안 관련해서는 랜덤 텍스트, 경로 암호화 등을 사용하여 보안을 좀 더 고도화하고, 이에 따라 접근제어를 최대한 정확하게 할 것이다. javascript와 nodejs 등은 무료로 사용 예제들이 많아 쉽게 사용하고 접근할 수 있으며, naver STT API는 부분적으로 유료로 지원받은 금액 내에서 해결하도록 할 것이다.

## 7. 결과

### 7.1. 결과물 설명

본 프로젝트에서는 사용자 인증방식을 보여줄 수 있는 간단한 웹페이지를 개발하여 로그인 기능을 통해 사용자의 계정을 생성하고 음성 인식 기능이 작동되는 모습을 보여 준다. 다음은 본 프로젝트의 구현된 결과물이다.

#### <기본 페이지 화면>



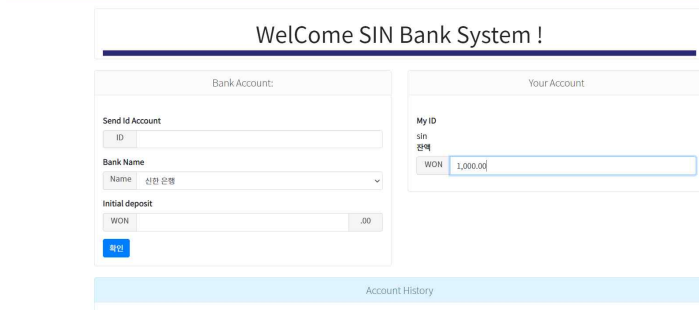
Sign in with Voice를 클릭하면 나오는 페이지이다. 유저는 음성 인식 기능으로 로그인할 아이디를 입력하여 아이디 체크를 누른다.



Developed By SIN Team 2020- 01

아이디 체크를 눌러 해당 아이디가 음성 인식 기능이 추가된 아이디로 확인이 되면 다음과 같은 페이지가 뜬다. 회원 가입할 때와 마찬가지로 랜덤 텍스트가 생성되며, 유저는 그 랜덤 텍스트를 그대로 따라 읽어서 로그인을 하면 된다.

## <서비스 페이지>



Developed By SIN Team 2020- 01

로그인이 성공하여 접근 권한이 부여됐다면 해당 서비스인 은행 시스템을 이용할 수 있다. 유저는 송금 등 은행 업무를 볼 수 있다.

## 7.2. 결과물 분석

본 프로젝트의 결과물은 MySQL을 사용하므로 다량의 데이터와 다수의 사용자를 비교적 잘 처리할 수 있으므로 다수의 사용자처리 부분에서 우수하고, 네트워크 연결을 통한 데이터 삽입, 삭제, 업데이트가 가능하며 MySQL을 사용하여 데이터의 분산처리가 가능하므로 DB서버의 네트워

크 액세스 부분에서 우수하다. 데이터베이스와 Node.js를 연동하므로 연동이 상대적으로 쉽기 때문에 DB와의 연동 부분에서 우수하다. 또한 MySQL은 무료배포용이지만 다양한 데이터베이스 기능을 제공하고 있다. Javascript를 사용하므로 Windows가 아닌 PC에서도 사용가능하며 MySQL은 중급형 PC환경에서 무난히 돌릴 수 있으므로 동작 환경 제한요소 부분에서 우수하다. 그리고 Nodejs와 MySQL, Javascript 경우 관련 예제가 많아 개발에 무리가 없으므로 개발환경 제한요소 부분에서 우수하다. Javascript를 사용하기 때문에 유지보수가 상대적으로 쉬워 유지보수 부분에서 우수하다. Javascript는 무료 개발도구가 다양하고 MySQL은 무료이기 때문에 경제성 부분에서 우수하다.

전체적으로 평가항목 부분에서 우수한 것을 볼 수 있다. 이러한 것을 바탕으로 본 프로젝트의 결과물은 편의성, 유지보수, 경제성 등 이러한 부분에서 만족스럽게 구현이 되었다.

## 7.3. 기대성과

기존의 아이디와 패스워드뿐만 아니라 목소리를 인증 매체로 활용한다는 점에서 보안의 측면을 높일 수 있다. 인터넷쇼핑을 예로 들면 인터넷쇼핑은 결제수단이 점점 간편화되어 예전엔 OTP 번호와 카드 정보 등을 입력해야 했다면 지금은 간편 비밀번호만을 통해 결제를 진행할 수 있다. 만약 간편 비밀번호가 노출이 되면 누구나 상대방의 기기로 인터넷 결제를 진행할 수 있다. 하지만 사용자의 목소리를 인증 매체로 사용한다면 간편 비밀번호와 같이 간단 하지만 더욱 보안이 뛰어난 효과를 기대할 수 있다.

또한 보안부분에서 랜덤 텍스트를 생성하여 사용자가 말한 단어를 비교하여 일치할 경우에만 접근 권한을 부여하기 때문에 음성 녹음, 유출을 통한 피해를 방지할 수 있으며, 음성 파일 암호화와 음성 파일 경로 암호화, gmm파일 경로 암호화, 비밀번호 암호화를 통하여 보안을 고도화하여 향상된 보안 성능을 기대할 수 있다.

## 8. 작업진행 방법

### 8.1. 작업 분담 구조



## 8.2. 설계 일정 및 역할 분담



## 8.3. 예산집행내역

회의비 - 200,000원

## 9. 결론

### 9.1 결론

현재 사용자 인증으로 비밀번호, 지문, 홍채인식 등 비밀번호 뿐 아니라 사용자의 고유한 생체 정보를 인증수단으로 사용하는 사례가 점차 증가하고 있다. 본 프로젝트에서는 음성인식을 통한 인증방식을 인증 수단으로 채택하여 사용자를 간단하게 인증하며 또한 사용자가 다른 누군가의 계정 정보에 접근할 수 없도록 보안 측면으로도 신경을 썼다.

사용자가 로그인 시에 음성정보를 등록하면 서버에서는 WAV파일에 사용자 목소리의 특징을 뽑아내는 MFCC파일을 생성하게 되고 생성된 MFCC파일을 이용해 gmm파일을 생성하여 저장하게 된다. 사용자의 목소리에 따라 특징이 서로 다르기 때문에 gmm파일의 값이 달라지게 되고 때문에 어떤 사용자가 다른 사용자의 계정에 음성인식을 통해 접근하려고 하는 경우 생성된 gmm파일의 인증값이 달라지게 되고 계정 인증에 실패하게 된다. 이를 통해 음성 인식을 통한 서비스 인증의 보안 문제를 해결하였다.

또한 서비스를 인증 중인 사용자의 목소리를 녹음하거나 사용자의 목소리 파일을 해킹하여 서비스를 인증하려는 해킹방식에 대비하기 위하여 인증시 필요한 Text가 랜덤으로 생성되어 매번 로그인 시 마다 화면에 나타나는 랜덤한 텍스트를 읽어야 하도록 설정했다.

마지막으로 사용자의 계정 정보, 또는 목소리파일, gmm파일 등등을 직접적으로 해킹하는 것을 방지하기 위해 사용자의 계정 정보는 암호화 되어 DB에 저장되게 되고 또한 gmm파일과 사용자의 목소리가 담긴 wav파일은 경로를 암호화하여 파일의 위치를 찾을 수 없도록 설정했다.

## 9.2 결과 분석

본 프로젝트의 결과물은 기존의 아이디와 패스워드뿐만 아니라 목소리를 인증 매체로 활용한다는 점에서 보안의 측면을 높일 수 있다. 이는 카드 번호나 비밀번호 등 복잡하고 외워야 하는 기존의 방식과 달리 사용자의 목소리를 인증 매체로 사용한다면 간단함은 물론이고, 고유의 생체 인증이기 때문에 더욱 보안이 뛰어난 효과를 기대할 수 있다.

또한 보안 부분에서 랜덤 텍스트를 생성하여 사용자가 말한 단어를 비교하여 일치할 경우에만 접근 권한을 부여하기 때문에 음성 녹음, 유출을 통한 피해를 방지할 수 있으며, 음성 파일 암호화와 음성 파일 경로 암호화, gmm파일 경로 암호화, 비밀번호 암호화를 통하여 보안을 고도화하여 향상된 보안 성능을 기대할 수 있다.

단점으로 AI로 생성된 fake voice를 통한 목소리 흉내를 감지할 수 없다는 부분이 있지만 이는 향후 더 발전된 방법이나 기술을 통하여 해당 문제를 해결할 수 있을 것이다. 그래도 위에서 살펴본 것과 같이 전체적으로 본 프로젝트의 결과물은 편의성, 유지보수, 경제성 등 이러한 측면에서 우수하며, 만족스러운 구현이다.

## 9.3 향후 계획 및 일정

향후 본 프로젝트의 보안 부분을 조금 더 강화할 예정이다. 보안 측면을 신경을 쓰긴 했지만, 예를 들어 AI로 생성된 fake voice를 통해 사용자의 목소리를 흉내를 내는 경우 이를 감지할 수 없다. 해당 문제를 해결하기 위해 fake voice detection 부분을 추가하여 목소리가 위.변조된 부분을 검증하면 더욱 보안이 강화된 인증 서비스를 구현할 수 있을 것이다.

## 10. 참고문헌

[1] CLOVA Speech Recognition API(CSR) ,네이버 음성인식 API 사용 설명서

[2] Google Speech Recognition API(GSR) , 구글 음성인식 API 사용 설명서

[3]

<https://appliedmachinelearning.blog/2017/11/14/spoken-speaker-identification-based-on-gaussian-mixture-model-s-python-implementation/> ,파이썬 gmm파일 추출

[4] <https://scikit-learn.org/stable/modules/generated/sklearn.mixture.GaussianMixture.html> ,파이썬 gmm파일 추출 관련 라이브러리