고령자 음성 모니터링 서비스를 위한 보안 요구사항 도출 및 개인정보보호 기반 시스템 설계

박지영°†, 최원영†, 김이든, 배준영, 이다영*
강원대학교 컴퓨터공학과
a24cc410s@kangwon.ac.kr, sable@kangwon.ac.kr, rladlems103@kangwon.ac.kr,
kaan03@naver.com, dayoung08@kangwon.ac.kr

Security Requirement Elicitation and Privacy-Aware System Design for an Elderly Voice Monitoring Service

Jiyeong Park°†, Wonyeong Choi†, Yideun Kim, Junyoung Bae, Dayoung Lee*
Department of Computer Science and Engineering, Kangwon National University

요 약

고령자 음성 모니터링 서비스는 일상 대화를 통해 건강 상태를 추적할 수 있다는 점에서 활용 가능성이 높지만, 음성 데이터가 민감정보이자 개인 식별 가능 정보를 포함할 수 있어 보안과 개인정보보호가 필수적이다. 특히 AI가 피보호자의 음성을 수집하고 이를 보이스 스펙트럼 이미지로 변환하여 치매 위험도를 판별하는 서비스에서는 음성 원본뿐 아니라 스펙트럼 이미지와 분석 결과 역시 보호되어야 한다. 본 논문은 독거 고령자의 음성 응답을 수집하고 보호자가 결과를 확인하는 서비스를 대상으로, 보안 요구사항을 도출하고 이를 반영한 개인정보보호 기반 시스템 설계를 제안한다. 공개 보안 지침을 바탕으로 입력 검증, 인증 및 권한 분리, 상태 전이 안정성, 민감정보 보호, 파일 처리, 오류 처리의 여섯 범주로 요구사항을 재구성하고, 인터페이스 명세 기반 퍼징 절차를 통해 이를 검증한다. 이를 통해 본 논문은 설계 단계부터 보안과 개인정보보호를 반영한 보안 내재화 설계 사례를 제시한다.

1. 서론

고령화가 심화되면서 독거 고령자의 건강 상태를 일상적으로 확인할 수 있는 원격 모니터링 기술의 필요성이 커지고 있다. 특히 치매는 조기 진단이 중요하지만, 독거 고령자 자발적 검사가 어렵고 기존 텍스트 기반 선택형 진단은 지속적 활용에 한계가 있다. 이에 따라 서비스가 먼저 사용자에게 접근해 건강 상태를 확인하는 방식이 필요하다. 또한 음성은 반복 수집이 쉽고 발화 속도, 억양, 휴지, 말 더듬기, 응답 지연 등 다양한 단서를 포함하므로 고령자 대상 디지털 헬스케어의 유망한 입력 매체로 주목받고 있다. 최근 연구들도 음성 바이오마커가 인지 저하와 건강 상태 변화를 반영할 수 있음을 보고하였다[1].

그러나 음성 기반 건강 모니터링 서비스는 건강정보와 식별 가능 정보가 결합된 민감한 서비스이므로 높은 수준의 보안과 개인정보보호가 요구된다. 헬스케어 분야 선행 연구에서도 인증, 접근통제, 정보 보호, 개인정보 처리가 핵심 과제로 제시되었으며[2], 보안 내재화 설계(Secure-by-Design)는 이를 초기 설계 단계에서 반영할 것을 강조한다[3, 4]. 특히 본 서비스는 음성을 보이스 스펙트럼 이미지로 변환하고, AI 모델의 판별 결과를 보호자 앱에 제공하므로, 음성 원본뿐 아니라 스펙트럼 이미지와 분석 결과도 보호 대상이 된다.

본 논문은 고령자 음성 모니터링 서비스를 위한 보안 요구사항을 도출하고, 이를 반영한 개인정보보호 기반 시스템 설계를 제안한다. 또한 공개 보안 가이드라인을 바탕으로 요구사항을 정리·구체화하고, 인터페이스 명세 기반 퍼징 절차를 통해 인터페이스 수준의 보안성을 검증한다[5, 6]. 이를 통해 음성 기반 건강 모니터링 서비스의 보안 중심 설계 사례를 제시한다.

2. 시스템 설계

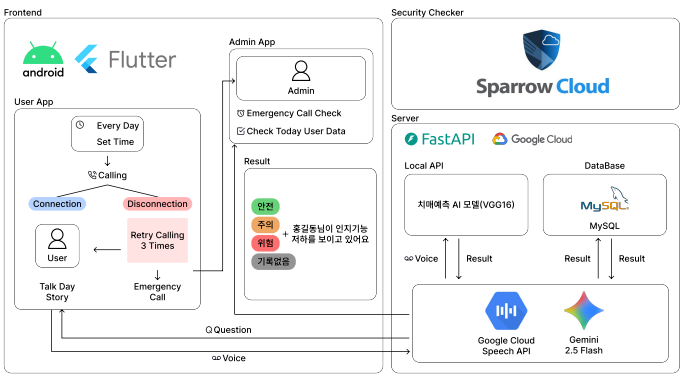


그림 1: 고령자 음성 모니터링 서비스의 전체 시스템 아키텍처

본 연구의 대상 시스템은 독거 고령자의 음성 응답을 수집하고, 이를 AI 기반으로 분석하여 보호자가 결과를 확인할 수 있도

†) 박지영과 최원영은 공동 제1저자입니다.
*) 본 논문은 2026년도 과학기술정보통신부 및 정보통신기획평가원의 'SW중심대학사업'(2025-0-00058)과, 2026년도 교육부 및 강원특별자치도의 재원으로 강원RISE센터의 지원을 받아 수행된 '지역혁신중심 대학지원체계(RISE)'(2026-RISE-10-002)와, 2026년도 정부(과학기술정보통신부)의 재원으로 한국인터넷진흥원(KISA) '정보보호전문인력양성(정보보호특성화대학) 사업'의 지원을 받아 수행된 연구결과입니다.

록 설계된 고령자 음성 모니터링 서비스이다. 시스템은 피보호자용 앱, 보호자용 앱, 서버, 데이터베이스, 음성 분석 모듈로 구성되며, 그림 1, 2, 3는 전체 구조와 주요 처리 흐름을 나타낸다.

피보호자용 앱은 AI 기반으로 생성된 질문을 인앱 전화 방식으로 제시하고 음성 응답을 수집하며, 보호자용 앱은 피보호자 목록, 진단 결과, 리포트 조회 기능을 제공한다. 서버는 사용자 연결, 음성 분석, 결과 저장 및 조회를 담당한다.

음성 데이터는 전처리를 거쳐 보이스 스펙트럼 이미지로 변환된 뒤, AI hub에서 "인지기능 장애 진단 음성/대화" 데이터와 함께 공개된 VGG16 기반 분류 모델의 입력으로 사용하였다[7, 8].

또한 본 시스템은 원본 멜 스펙트로그램을 비가역적 윤곽선 중심 시각 표현으로 변환하여 직접 복원을 어렵게 하였으며, 분석 결과는 서버와 데이터베이스를 거쳐 보호자 앱에 AI 점수와 보이스 스펙트럼 이미지 형태로 제공되며, 음성 원본은 폐기된다.



그림 2: AI 기반 질문 생성과 인앱 전화 기반 음성 수집 과정



그림 3: 보이스 스펙트럼 기반 치매 판별 흐름

3. 보안 요구사항 도출

본 서비스는 음성 원본, 보이스 스펙트럼 이미지, AI 진단 결과, 보호자-피보호자 연결 정보 등 민감한 데이터를 함께 처리한다. 특히 음성 데이터는 건강 상태 추론의 근거가 되는 동시에 개인 식별 가능성을 포함할 수 있고, 스펙트럼 이미지와 AI 진단 결과 역시 원본 음성으로부터 생성된 건강 관련 파생 정보이므로 동일한 수준의 보호가 필요하다.

표 1: 고령자 음성 모니터링 서비스를 위한 보안 요구사항

구분	보안 요구사항
입력 검증	모든 입력은 형식과 범위가 검증되어야 하며, 비정상 요청과 누락 필드는 서버에서 차단되어야 함.
인증/권한	보호자와 피보호자의 역할에 따라 접근 권한을 구분하고, 승인된 관계에서만 결과 조회와 관리 기능을 허용해야 함.
상태 전이	보호자-피보호자 연결, 음성 업로드, 결과 조회와 같은 다단계 요청은 정의된 상태와 순서를 만족할 때만 처리되어야 함.
민감정보 보호	음성, 스펙트럼 이미지, 진단 결과, 식별 정보의 저장 · 전송 · 조회 범위를 최소화해야 함.
파일 처리	업로드 음성 파일과 분석 과정의 임시 파일은 안전하게 처리되어야 하며, 분석 후 삭제하거나 최소 기간만 유지해야 함.
오류 처리	오류 발생 시 내부 구현 정보가 외부에 노출되지 않아야 하며, 클라이언트에는 필요한 수준의 오류만 반환해야 함.

이에 본 연구에서는 공개 보안 가이드라인을 참고하여 서비스 구조에 적합한 보안 요구사항을 도출하였다[3, 4]. 도출된 요구사항은 입력 검증, 인증 및 권한 분리, 상태 전이 안정성, 민감정보 보호, 파일 처리 안전성, 오류 처리의 여섯 범주로 정리하였다. 표 1은 고령자 음성 모니터링 서비스에 필요한 주요 보안 요구사항을 정리한 것이다. 각 성공률은 해당 검증 항목에 대해 생성된 전체 테스트 요청 중 보안 요구사항을 만족한 응답의 비율로 산정하였다.

4. 실험

본 연구에서는 3장에서 도출한 보안 요구사항이 실제 서비스 인터페이스 수준에서 적절히 반영되는지 확인하기 위해 OpenAPI 명세 기반 보안 검증 절차를 적용하였다. 검증 대상은 사용자 인증, 보호자–피보호자 연결, 음성 업로드, 분석 결과 조회 등 핵심 인터페이스이다.

검증에는 Schemathesis와 RESTler를 함께 활용하였다[5, 6]. Schemathesis는 OpenAPI 명세를 기반으로 Coverage, Fuzzing, Stateful 단계를 수행하며, 본 실험에서는 전체 22개 operation을 대상으로 두 차례 실행하여 각각 3,233개와 2,480개의 테스트 케이스를 생성하였다[5]. Coverage 단계에서는 전체 API를 점검하고, Fuzzing 단계에서는 다양한 입력을 통해 검증 누락과 스키마 위반 가능성을 확인하며, Stateful 단계에서는 이전 응답값을 활용한 연계 시나리오를 수행하였다. RESTler는 요청 간 의존관계를 반영하는 상태 기반 API 퍼징 도구로, 본 실험에서는 총 22개 요청 집합과 20개의 의존성을 기준으로 상태 기반 시퀀스를 확장하며 다단계 API 흐름을 점검하였다[6].

검증 결과는 다음과 같다.

- **입력 검증:** 비정상 입력, 누락 필드, 타입 불일치, 경계값 변형 요청은 모두 적절히 차단되어 기본적인 입력 검증 체계가 안정적으로 동작함을 확인하였다.
- **인증 및 권한 분리:** 인증 정보 없이 보호 자원에 접근하거나 다른 역할의 권한으로 요청하는 경우는 모두 차단되어 권한 분리 정책이 정상적으로 적용됨을 확인하였다.
- **상태 전이:** 리소스 생성 후 조회 · 수정 · 삭제, 세션 생성 후 하위 자원 접근, 코드 · 토큰 교환 이후 후속 요청과 같은 연계 흐름에서 승인되지 않은 관계 형성이나 비정상 상태 전이는 관찰되지 않았다.
- **민감정보 보호:** 퍼징을 통해 응답 수준에서 과도한 정보 노출이 없는지 점검하였으며, 설계 단계에서는 원본 멜 스펙트로그램을 비가역적 시각 표현으로 변환하고, 음성 원본은 분석 후 폐기하며, 스펙트럼 이미지와 진단 결과의 저장 · 전송 · 조회 범위를 최소화하였다.
- **파일 처리:** 비정상 파일 업로드와 잘못된 파일 관련 입력은 모두 차단되었으며, 업로드 파일과 임시 파일은 분석 후 삭제하거나 최소 기간만 유지하도록 설계하였다.
- **오류 처리:** 내부 구현 정보나 스택 트레이스의 직접 노출은 관찰되지 않았으며, 오류 응답은 일관된 형태로 안전하게 반환되었다.

종합하면, 입력 검증, 인증 및 권한 분리, 상태 전이, 파일 처리, 오류 처리 측면에서는 명세 기반 퍼징을 통해 인터페이스 수준의 안정성을 확인하였다. 반면 민감정보 보호는 인터페이스 응답 점검만으로 충분히 검증하기 어려워, 본 연구에서는 응답 최소화와 비가역적 파생 표현 활용 등 설계상의 보호 조치를 함께 제시하였다. 즉, 본 실험은 시스템 전반의 보안성을 완전하게 입증한 것이 아니라, 도출한 보안 요구사항이 인터페이스 수준에서 일관되게 반영되고 있음을 확인한 것으로 볼 수 있다.

5. 결론

본 논문은 고령자 음성 모니터링 서비스를 대상으로, 음성 기반 디지털 헬스케어 서비스에 필요한 보안 요구사항을 도출하고 이를 개인정보보호 중심의 시스템 설계에 반영하였다. 대상 서비스는 피보호자의 음성을 수집하여 보이스 스펙트럼 기반 AI 모델로 분석하고, 보호자에게 결과를 제공하는 구조를 가진다. 이에 따라 입력 검증, 인증 및 권한 분리, 상태 전이 안정성, 민감정보 보호, 파일 처리 안전성, 오류 처리의 여섯 범주로 보안 요구사항을 정리하고, 서비스 구조와 인터페이스 설계에 반영하였다.

또한 OpenAPI 명세 기반 검증 절차를 통해 인터페이스 수준에서 해당 요구사항이 일관되게 반영되는지를 확인하였다. 그 결과 비인가 접근과 승인되지 않은 관계 형성은 관찰되지 않았으며, 입력 검증과 오류 처리 또한 안정적으로 동작하였다. 민감정보 보호 측면에서는 인터페이스 응답 수준의 정보 노출을 점검하는 한편, 원본 음성을 비가역적 파생 표현으로 전환하고 제공 범위를 제한하는 설계 원칙을 제시하였다. 이는 고령자 대상 음성 모니터링 서비스에서 보안 내재화 설계의 필요성을 보여준다.

본 연구의 의의는 대규모 운영 환경에서의 보안성을 완전하게 증명한 데 있지 않다. 오히려 음성, 파생 스펙트럼 이미지, AI 진단 결과처럼 서로 다른 민감 정보가 결합되는 서비스에서, 보안 요구사항을 사전에 구조화하고 이를 설계와 인터페이스 검증까지 연결하였다는 데 의미가 있다. 이러한 접근은 기능 구현 이후 취약점을 보완하는 방식보다 설계 초기 단계에서 주요 위협을 식별하고, 접근 통제, 정보 최소화, 비정상 요청 차단과 같은 보호 조치를 선제적으로 반영할 수 있다는 점에서 보안적으로 유용하다. 또한 이러한 절차는 유사한 민감정보 처리 시스템에도 적용 가능한 보안 설계 기준으로 활용될 수 있다는 점에서 실무적 유용성이 있다.

다만 본 연구는 보안 요구사항 도출과 인터페이스 수준 검증에 초점을 두었으므로, 상용 서비스와의 정량 비교, 서버 내부 저장 구조와 장기 운영 환경의 보안성, 원본 음성과 파생 정보 간 개인정보보호 효과의 정량적 비교까지는 다루지 못하였다. 향후 연구에서는 실제 운영 환경을 반영한 장기 보안성 검증, 내부 저장소 및 운영자 권한 통제 분석, 민감정보 최소화 정책의 효과 비교를 포함하여 보다 실질적인 개인정보보호 보장 수준을 평가할 필요가 있다. 또한 상용 서비스와의 비교를 통해 접근 통제, 정보 최소화, 결과 제공 방식의 차이를 체계적으로 분석함으로써, 고령자 대상 디지털 헬스케어 서비스에 적합한 보안 설계 원칙을 더욱 정교화할 필요가 있다.

참고 문헌

[1] G. Fagherazzi *et al.*, "Voice for health: The use of vocal biomarkers from research to clinical practice," *Digit. Biomark.*, vol. 5, no. 1, pp. 78–88, 2021.

[2] L. H. Iwaya *et al.*, "Security and privacy for mhealth and uhealth systems: A systematic mapping study," *IEEE Access*, vol. 8, pp. 150081–150112, 2020.

[3] Cybersecurity and Infrastructure Security Agency, "Shifting the balance of cybersecurity risk: Principles and approaches for secure by design software," tech. rep., CISA, 2023.

[4] OWASP Foundation, "Owasp api security top 10 – 2023." OWASP Project Page, 2023. Accessed: 2026-04-10.

[5] Z. Hatfield-Dodds and D. Dygalo, "Deriving semantics-aware fuzzers from web api schemas," in *Proc. ICSE-Companion*, pp. 345–346, 2022.

[6] V. Atlidakis *et al.*, "Restler: Stateful rest api fuzzing," in *Proc. ICSE*, pp. 748–758, 2019.

[7] AI Hub, "인지기능 장애 진단 음성/대화." https://aihub.or.kr/aidata/34103, 2021. Accessed: 2026-04-10.

[8] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *Proc. ICLR*, 2015.