시스템 정의서

(Genesis) 조

<table>
<tr><td rowspan="2">시스템 명칭</td><td colspan="3">(국문) 메일가드</td></tr>
<tr><td colspan="3">(영문) MailGuard</td></tr>
<tr><td rowspan="4">팀원</td><td>학번</td><td>이름</td><td>전공</td></tr>
<tr><td>2023078075</td><td>고재현</td><td>소프트웨어학부 인공지능전공</td></tr>
<tr><td>2021041067</td><td>심수민</td><td>소프트웨어학과</td></tr>
<tr><td>2021041072</td><td>전영우</td><td>소프트웨어학과</td></tr>
<tr><td colspan="4">시스템에 대한 요약</td></tr>
<tr><td>시스템 설명</td><td colspan="3">작품은 사용자에게 수신된 이메일이 악성 행위로 이어질 수 있는 이메일인지 검증하고 알려주는 PC용 응용프로그램이다.</td></tr>
<tr><td>개발 목적</td><td colspan="3">이 시스템은 사용자가 수신한 이메일의 제목, 본문, 첨부파일등을 분석하여 피싱 및 스미싱 여부 및 악성코드 감염 가능성을 사전에 검증하는 것을 목적으로 한다.</td></tr>
<tr><td>핵심
사용자</td><td colspan="3">1. 개인용 이메일 서비스 사용자:
네이버, 다음, Gmail(지메일), Nate, Hotmail, Yahoo(야후) 등 다양한 포털 사이트나 웹 서비스에서 제공하는 무료 이메일 서비스를 사용하는 사용자

2. 기업/조직용 이메일 사용자:
특정 기업이나 조직의 도메인(예: @company.co.kr)을 사용하는 사용자

3. 특수 계정 사용자:
특정 단체에서 발급한 이메일 주소를 사용하는 사용자</td></tr>
</table>

운영 방식	1. 이 시스템은 PC 환경에서 동작하도록 설계된다. 사용자가 이메일 또는 첨부파일을 업로드하면 시스템은 두단계로 악성 여부를 판별한다. 2. 1차 검증: 이메일 제목과 본문을 분석하여 피싱 또는 스미싱 가능성을 평가한다. 3. 2차 검증: 첨부파일을 정적으로 분석, 조회(VirusTotal API)등을 활용하여 악성여부를 판별한다. 4. 사용자는 브라우저에서 이메일 파일 또는 첨부파일을 업로드한다. 시스템은 백엔드 서버에서 AI 및 분석 모듈을 호출하여 실시간 검사를 수행한다.
작품의 주요 기능	1. 사용자의 이메일에 대한 실시간 검진 현황을 제공한다. 2. 이메일별 안전, 의심, 경고 표시 제공한다. 3. 이메일 검진 결과를 보고서 형식으로 제공한다. 4. 악성메일로 의심되는 이메일의 첨부파일 클릭 시 경고 알림창을 제공한다. 5. 사용자가 검진을 원하는 메일을 등록하는 기능 제공한다.
기타 개발시 고려사항	1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 개인정보 보호법 을 준수해야 한다. 2. 프로그램에서 수집한 개인정보가 외부에 유출되지 않도록 암호화 기능 등을 통하여 보안 수준을 높여야 한다. 3. 다양한 종류의 이메일 서비스(네이버 메일, gmail, 다음 메일 등)에서 적용이 가능해야 한다.

기타사항	*** 논문 및 특허** 1. 이메일의 첨부 파일에서 악성 코드 검출 방법 및 그 장치 https://patents.google.com/patent/KR100743372B1/ko 2. DB化 및 사례기반추론 알고리즘 적용을 통해 공격성향과 집단의 특성을 프로파일링 가능성 https://koreascience.kr/article/JAKO201509057414567.pdf *** 상용된 SW 제품** 1. 네이버 클라우드 플랫폼 https://www.ncloud.com/product/security/fileSafer#detail 제공 기능 : Hash Filter 및 File Filter 이용한 메일 첨부된 파일의 악성코드 감염 여부 확인 후 감염 시 다운로드 차단 기능 제공 2. EG-Platform http://hudas.co.kr/page/sub3_1.html 제공 기능: DB 기반 스팸 차단 기본 기능, 첨부파일과 URL에 숨겨진 신종 랜섬웨어 검출, 반송 없는 메일 발신,대량 메일 발송 시도 차단 등 기능 제공 *** API** https://www.virustotal.com/gui/home/upload 구글의 자회사. 바이러스, 웜 트로이 등을 검사하고 막는 사이트. 여러 개의 백신 엔진으로 검사하여 결과를 보여주고, 여러 개 파일 검사하는 사이트. 악성코드 검사할 수 있는 API를 제공함. https://virustotal.github.io/yara/ 멀웨어 연구자들이 멀웨어 샘플을 식별하고 분류하는데 도움을 주기 위한 도구. 텍스트 또는 바이너리 패턴을 기반으로 멀웨어에 대한 설명을 생성할 수 있다.