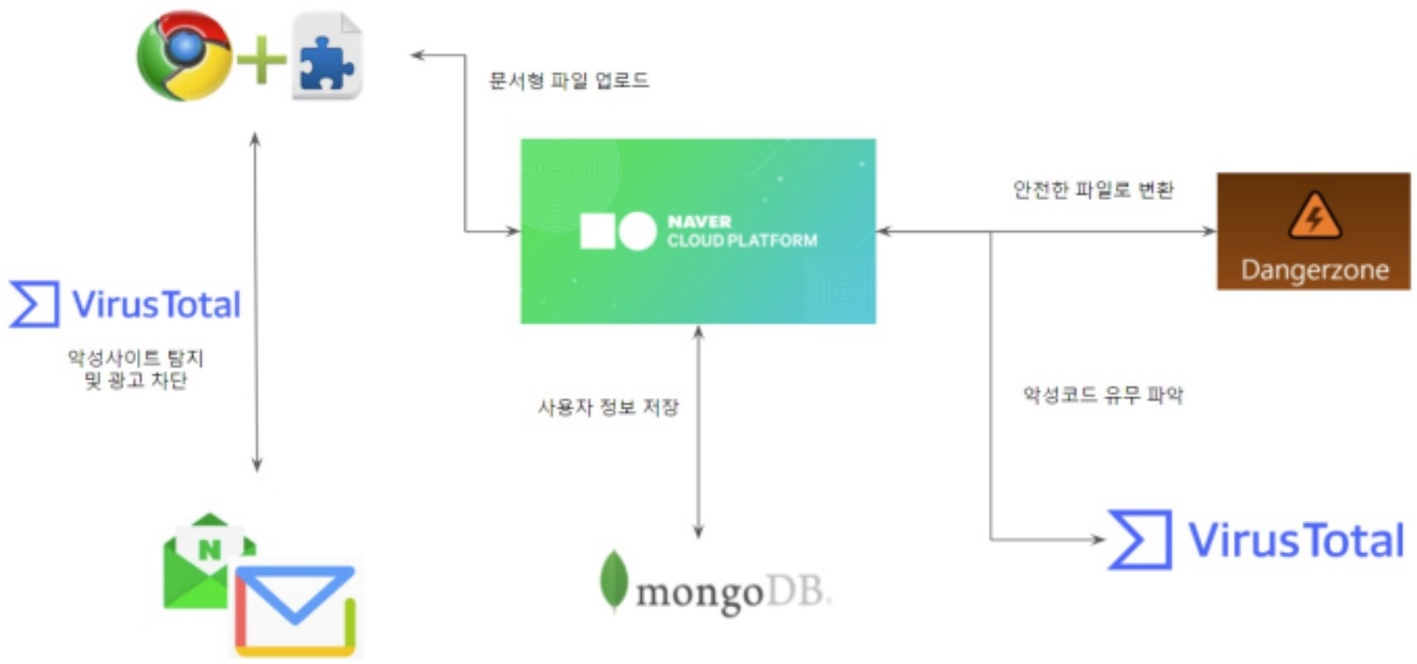
3. 주요 구성 및 설계

그림 1 설계도



아이디어를 구현하기 위한 설계도는 위와 같으며 총 3부분으로 나뉜다. 안전한 파일로 변환하고 악성 코드 리스트 보고서를 반환하는 부분, MongoDB를 통해 사용자를 관리하는 부분, mail 내에 존재하는 URL을 검사하고 공격 벡터로 사용될 수 있는 배너형 광고를 차단하는 부분이다.

악성 파일을 안전한 파일로 변환하는 부분에서 Dangerzone Open source에 HWP 확장자를 추가한 docker container를 Naver Cloud에서 생성한 Ubuntu server 18.04 LTS 운영체제 위에서 운영한다. CDR 기법으로 변환한 파일뿐만 아니라 VirusTotal API를 이용해 변환하려는 파일이 가진 악성코드 리스트의 보고서를 사용자에게 전달한다.

변환한 파일과 보고서가 다른 사용자에게 전달되는 것을 방지하기 위해 MongoDB를 사용해 사용자 정보를 관리한다.

마지막으로 EasyList에서 제공하는 URL을 Chrome Extension API를 사용해 배너형 광고를 차단하고 VirusTotal API과 Chrome Extension API를 사용해 메일로 전달되는 URL을 검사하고 위험도를 제공한다.

Python의 pyhwp 모듈과 wkhtmltopdf 모듈을 사용해 HWP 파일을 PDF 파일로 바꾸는 것이 가능하다. Chrome extension API와 VirusTotal API를 활용해 배너형 광고를 차단하고 악성 파일과 URL을 검사하고, Chrome extension으로 사용자에게 제공한다. 이를 바탕으로 본 프로젝트의 제작하고 시현한다.