사이버수사관 모니터링업무 보조시스템

AJOU SOFTCON 2021-1

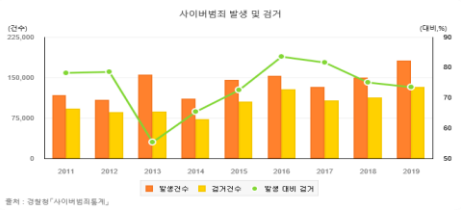
팀 명 5조

팀 원 김홍주, 이승환, 이정현, 전지원

지도교수 손태식

멘 토 최욱 (테스트웍스)

개발 동기 및 목적

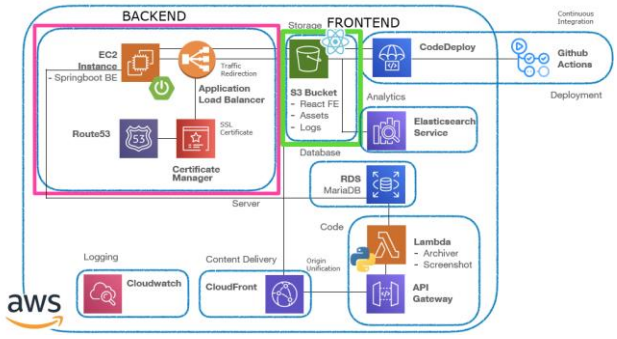


출처 : 경찰청 「사이버범죄통계」

위 차트는 경찰청에서 제공한 연간 사이버 범죄 발생 및 검거율입니다. 사이버범죄의 발생 건수는 매년 증가하고 있지만 사이버 수사대의 인력 부족과 수사에 적합한 도구가 주어지지 않아 검거율은 갈수록 낮아지고 있는 추세입니다.
이에 반복적이고 비효율적으로 수행되는 인터넷 게시글 모니터링 업무의 자동화로 사이버범죄 수사 업무의 효율성을 제고하기 위해 이번 작품을 개발하게 되었습니다.
또한 사이버수사대 내의 증거 보존 툴의 부재로 인해 수사 중 원본 게시물이 삭제될 경우 수사 진행에 차질이 생기는 경우가 있습니다. 이에 게시물이 삭제된 경우 원활한 수사 진행이 가능하도록 원본 게시글을 보존해주는 웹 아카이버를 개발하였습니다.

주요 기술

본 프로젝트는 여러 기능들을 독립적으로 구축하여 배포하는 MSA(Micro Service Architecture) 방식으로 설계되었습니다.
Backend, Frontend, AWS Api Gateway의 크게 3개의 영역에서 api 호출을 통해 동작합니다.



Backend는 Springboot로 로그인 기능과 사이트의 게시물을 수집하는 크롤링 기능을 담당하며 AWS EC2 서비스를 이용해 구축하였습니다. 이때 EC2의 HTTP 포트 사용으로 인한 Frontend와의 상호작용 문제를 해결하기 위해 AWS Route53에서 도메인을 구입해 SSL 인증서를 발급받아 Application Load Balancer를 이용해 EC2에 장착하였습니다.
Frontend는 React를 사용하였고 AWS S3를 이용해 서버리스 구조로 동작하며 사용자와의 상호작용을 담당합니다.
AWS Lambda Function에 게시물 아카이빙 및 스크린샷 기능을 Python으로 작성하였고 이를 Api Gateway에서 호출해 동작합니다.
Database는 MariaDB를 사용하였고 저장된 첩보 데이터를 시각화하기 위해 ElasticSearchService를 이용하였습니다.
CloudFront는 EC2, S3, Api Gateway의 3개의 Origin이 달라 발생한 CORS 문제를 해결하기 위해 Origin을 통합하는 목적으로 사용하였습니다.
서비스 배포는 AWS Code Deploy를 사용하였습니다.

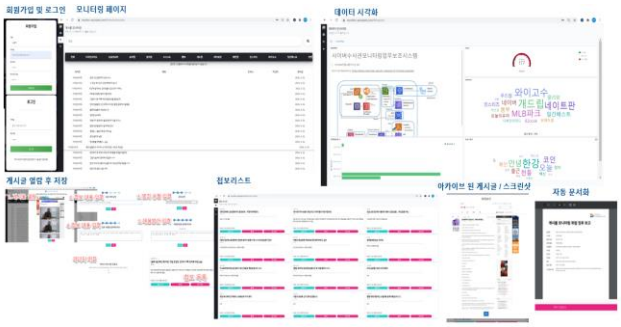
개발 내용

사이버 수사관의 모니터링 업무 효율 향상을 목적으로 한 본 프로젝트에서 제공하는 핵심 기능은 다수의 커뮤니티 게시물 동시 모니터링과 증거물 보존을 위한 웹 아카이버 입니다.

세부 기능은 다음과 같습니다.
1. 회원가입 및 로그인 기능
사용자별 첩보 데이터 관리를 위해 회원가입 및 로그인 기능을 개발하였습니다.
2. 게시물 수집 기능
키워드를 입력하면 접속률을 기준으로 선정한 국내 15개의 커뮤니티 사이트에서 게시물을 가져와 사이버수사관이 하나의 페이지에서 여러 사이트 모니터링을 효과적으로 수행할 수 있도록 개발하였습니다.
3. 게시물 아카이빙 및 스크린 샷 기능
게시물이 삭제된 경우를 대비해 만든 기능으로, 문제가 되는 게시물에 대해 수사를 진행하기 위해 첩보로 저장할 시 원본 게시물의 HTML과 Asset들을 S3에 저장해 언제든지 게시물을 확인할 수 있게 합니다. 또한 아카이빙 시 전체 페이지에 대한 스크린 샷을 촬영해 저장합니다.
4. 첩보물 저장 기능
모니터링 중 허위사실 유포 등 수사가 필요한 게시글 발견 시 첩보 내용, 대응방안 등의 수사내용을 입력한 후 저장하며 첩보 리스트에서 열람 및 삭제 등 관리 가능합니다.
5. 첩보물 자동 문서화 기능
문서 작업에 소요되는 시간 단축을 위해 저장된 첩보물에 대해 자동 PDF 문서화 및 다운로드 기능을 제공합니다.
6. 데이터 시각화 기능
범죄유형 인사이트 도출을 위해 첩보 개수, 출처 사이트와 검색 키워드 순위, 날짜 별 저장된 첩보 수 등의 정보를 제공합니다.

결과 및 분석

사이버수사관이 허위사실 유포 등의 위법 게시물을 모니터링 하기 위해 키워드를 입력하면15개의 사이트에서 키워드가 포함된 게시물을 크롤링해 제공합니다. 모니터링 중 수사가 필요한 게시물 발견 시 수사내용을 입력하면 아카이빙 된 데이터 및 게시글 스크린샷과 함께 첩보 리스트에 저장됩니다. 첩보 리스트에서는 수사내용 및 아카이빙 된 게시글 확인, 자동 문서화, 삭제 등의 기능을 제공합니다. 또한 수사 인사이트 도출을 위해 저장된 첩보 데이터에 대한 시각화를 제공합니다.



사이버 수사대에서 본 프로젝트의 결과물을 사용하게 된다면 수사 업무의 효율이 상승하여 사이버 범죄 검거율 증가에 도움이 될 것으로 예상됩니다.

Domain: www.monitor-assistant.com
git: https://github.com/cyber-security-capstone-21-1/monitor-assistant