P R O J E C T D O C U M E N T

Project Design Brief

Project Name	BGP라우팅 데이터 분석 LLM 기술 개발

6조

202002567 진효겸
202002506 손봉우
202002518 양준혁

지도교수: 이영석 교수님 (서명)

Document Revision History

Rev#	Date	Affected Section	Author
1	2023/03/06		홍길동

Table of Contents

List of Figure

그림 목차 항목을 찾을 수 없습니다.

1. 프로젝트 주제 이름

BGP 라우팅 데이터 분석 LLM 기술 개발

2. 대상 이해당사자 (stakeholder)

- 통신사 네트워크 운영 및 엔지니어링 팀 (SK텔레콤, KT, LG유플러스)
  - BGP 데이터를 실시간 모니터링하고 네트워크 상태를 유지해야 하는 기술 엔지니어 및 관리자
  - 네트워크 장애 감지 및 경로 최적화를 수행하는 팀
- 보안 팀
  - BGP 하이재킹(라우트 탈취) 및 기타 네트워크 공격을 탐지하고 대응하는 보안 전문가
  - 라우팅 이상 감지 및 취약점 분석을 수행하는 보안 연구자
- 정부 및 규제 기관 (KISA, 과학기술정보통신부)
  - 국가 인터넷 백본 안정성을 유지하기 위한 모니터링 담당 기관
  - 인터넷 트래픽 흐름 및 BGP 이상 탐지를 연구하는 기관
- 대학 및 연구기관
  - 인터넷 라우팅 및 BGP 관련 연구를 수행하는 연구자 및 대학원생
  - BGP 경로 변경이 네트워크 성능 및 보안에 미치는 영향을 분석하는 연구기관

3. 이해당사자의 고충(pain point) 또는 니즈(needs)

- 통신사 네트워크 운영 및 엔지니어링 팀
  - BGP 데이터를 분석할 때, 기존 툴들은 복잡한 명령어 및 설정을 요구하여 사용

이 어려움
  - 실시간 라우팅 변화 감지를 위한 자동화된 모니터링 시스템 부족
  - 과거 BGP 데이터를 활용하여 라우팅 이슈의 원인을 분석하는 과정이 어려움
  - 데이터가 많아도 시각화 기능이 부족하여 직관적인 분석이 어려움

- 보안 팀 (SOC, CSIRT)
  - BGP 하이재킹 등의 보안 위협이 발생했을 때, 기존 툴로는 탐지 및 대응이 느림
  - 대량의 BGP 로그 데이터를 수동으로 분석하는 것은 비효율적이며 시간이 오래 걸림
  - 실시간 경로 변화를 자동 감지하고, 이상 징후를 분석하는 기능이 필요함

- 정부 및 규제 기관 (KISA, 과기정통부)
  - 국가 단위의 인터넷 경로 안정성을 유지하기 위해 BGP 이상 탐지 시스템 필요
  - 특정 기간 동안의 BGP 변화 데이터를 추적하는 것이 어렵고 수작업이 많음
  - 통신사와의 협업을 위해 표준화된 데이터 및 분석 리포트 제공 필요

- 대학 및 연구기관
  - 대량의 BGP 데이터를 다룰 때, 기존 분석 방식은 비효율적이며 계산량이 많음
  - 연구 목적에 맞게 데이터를 자유롭게 가공하고, 원하는 형태로 분석하는 것이 어려움
  - 다양한 시각화 기능을 활용하여 BGP 트렌드를 쉽게 분석하고 논문 등에 활용할 필요가 있음

4. 이해당사자의 이유

- 통신사 네트워크 운영 및 엔지니어링 팀
  - 운영 효율성 증가: 자동화된 분석 및 시각화를 통해 라우팅 장애 해결 시간을 단축
  - 네트워크 안정성 보장: 실시간 BGP 데이터 분석을 통해 장애 및 성능 문제를 빠르게 감지
  - 기존 분석 도구의 단점 보완: 기존 솔루션은 복잡하고 직관적이지 않음, LLM 기반 인터페이스로 쉽게 분석 가능하도록 개선

- 보안 팀 (SOC, CSIRT)
  - 보안 위협 감지 속도 향상: BGP 하이재킹 및 DDoS 공격을 빠르게 탐지하고 대응
  - 자동화된 이상 탐지 기능 확보: 실시간으로 이상한 경로 변경을 감지하고 알림 제공
  - 과거 데이터 활용 가능: 기존 보안 시스템과 연계하여 과거 BGP 데이터를 통해 공격 패턴을 분석 가능

- 정부 및 규제 기관 (KISA, 과기정통부)
  - 국가 인터넷 인프라 보호: 통신사 및 주요 네트워크 경로의 안정성 모니터링
  - 신속한 위기 대응: BGP 경로 변화를 감지하여 인터넷 장애 발생 시 빠른 대응 가능
  - 정책 수립을 위한 데이터 분석: 국내외 BGP 트렌드를 분석하여 정책 결정에 활용

- 대학 및 연구기관
  - 연구 효율성 향상: 복잡한 BGP 데이터 분석을 쉽게 수행하여 연구에 집중 가능
  - 다양한 데이터 활용: RIPE 및 RouteViews 데이터를 활용하여 글로벌 트렌드 분석 가능
  - 시각화를 통한 인사이트 도출: 데이터 분석 결과를 직관적으로 표현하여 연구 및 논문 작성에 활용 가능

5. 프로젝트 수행자의 의도

현재 BGP(Border Gateway Protocol) 데이터는 네트워크 엔지니어와 보안 전문가들에게 필수적인 분석 대상이지만, 기존 분석 도구들은 사용이 어렵고 실시간 대응이 어렵다는 한계가 있다. 특히, SKT 및 KT와 같은 통신사 내부에서는 대량의 BGP 데이터를 효율적으로 분석하고 시각화할 수 있는 사용자 친화적인 솔루션이 부족하다.

기존의 BGP 분석 방식은 명령어 기반의 복잡한 절차를 요구하며, 실시간 감지 및 과거 데이터 활용이 제한적이다. 또한, 네트워크 장애나 보안 위협(BGP 하이재킹 등)이 발생했을 때, 이를 빠르게 탐지하고 대응하기 어려운 문제가 있다.

이에 따라, 우리는 LLM(대형 언어 모델, Large Language Model) 기술을 활용하여 누구나 자

연어 질의를 통해 손쉽게 BGP 데이터를 분석하고 시각화할 수 있는 시스템을 개발하려고 한다. LLM을 적용하면 사용자가 "최근 한 달간 KT의 국제 BGP 경로 변화 추세를 보여줘"와 같은 질의를 던졌을 때, 복잡한 명령어나 SQL을 직접 작성하지 않고도 원하는 데이터를 분석하고 시각화할 수 있다.

또한, RIPE 및 RouteViews 데이터를 활용하여 실시간 데이터뿐만 아니라 과거 데이터까지 분석할 수 있도록 하여, 장기적인 네트워크 변화 트렌드와 이상 징후를 쉽게 탐지할 수 있는 기능을 제공할 것이다. 이를 통해 통신사 네트워크 운영팀, 보안팀, 정부 기관 및 연구기관이 보다 효과적으로 BGP 데이터를 활용하고, 네트워크 운영 및 보안 대응을 최적화할 수 있도록 지원하는 것이 목표이다.

6. 탐구 내용 및 기대 결과

탐구 내용

1. LLM 기반 자연어 질의 시스템 구축
   - 사용자가 자연어로 BGP 데이터 분석을 요청하면, 이를 SQL 쿼리 또는 분석 코드로 변환하여 실행하는 기능을 구현한다.
   - 예: "KT의 BGP 경로 변화 추세를 시각화해줘" → 내부적으로 적절한 분석 코드 실행 후, 결과 반환

2. 실시간 및 과거 BGP 데이터 분석 기능 개발
   - RIPE 및 RouteViews 데이터를 활용하여 과거 BGP 데이터를 조회 및 분석할 수 있도록 구현한다.
   - 실시간으로 BGP 경로 변경을 수집하고, 이상 탐지 기능을 적용하여 라우팅 변화 및 보안 위협(BGP 하이재킹 등)을 감지한다.

3. BGP 데이터 시각화 대시보드 개발
   - 네트워크 엔지니어 및 보안 전문가가 쉽게 데이터를 분석하고 해석할 수 있도록 인터랙티브 대시보드를 개발한다.
   - 시각화 요소: BGP 경로 변화 그래프, 트래픽 흐름 히트맵, 지리적 시각화, 경로 변경 타임라인 등

4. 이상 탐지 및 네트워크 이벤트 분석 기능

- BGP 경로의 급격한 변경이나 특정 IP 대역의 이상 트래픽이 감지될 경우, 자동으로 경고 및 분석 리포트를 생성하는 기능을 추가한다.
- 특정 기간 동안의 BGP 이벤트(라우트 변경, 피어 다운 등)를 분석하여 네트워크 장애의 원인을 추적할 수 있도록 지원한다.

기대 결과

1. 사용자 친화적인 BGP 분석 시스템 제공
   - 네트워크 전문가가 아니어도 LLM을 활용하여 BGP 데이터를 쉽게 분석할 수 있도록 한다.
   - 자연어 입력을 통해 BGP 경로를 조회하고, 과거 데이터를 분석하며, 실시간 이벤트를 감지하는 기능을 제공한다.

2. 실시간 및 과거 데이터 분석 가능
   - RIPE 및 RouteViews 데이터를 활용하여 장기적인 BGP 트렌드 분석이 가능하도록 한다.
   - 실시간 데이터를 수집하여 네트워크 운영 및 보안팀이 즉각적인 대응을 할 수 있도록 지원한다.

3. 네트워크 장애 및 보안 위협 탐지 강화
   - BGP 하이재킹, 경로 변경, 특정 AS(Autonomous System) 이상 탐지 등 보안 관련 이슈를 자동 감지할 수 있도록 한다.
   - 탐지된 이상 현상을 정리하여 경고 알림 및 보고서를 자동 생성하는 기능을 포함한다.

4. 시각화를 통한 데이터 인사이트 제공
   - 복잡한 네트워크 데이터를 쉽게 해석할 수 있도록 대시보드에서 다양한 시각화 기능을 제공한다.
   - BGP 경로 변화 및 네트워크 이벤트를 직관적으로 분석할 수 있도록 한다.

5. 정량적/정성적 달성 지표
   - 정량적 지표
     - LLM 기반 질의 응답 정확도 80% 이상 달성
     - 실시간 BGP 데이터 수집 및 분석 속도 5초 이내 응답 가능
     - 과거 데이터 분석 지원 범위 최소 1년치 이상
   - 정성적 지표

- 네트워크 엔지니어 및 보안 전문가가 기존 분석 방식보다 편리하다고 평가할 것
- 제공된 시각화 기능이 데이터 분석에 실질적인 도움이 되는지 피드백 반영

7. 프로젝트 관련 학습 계획

학습할 내용	기간	역할 분담

8. 프로젝트 관련 현장방문 / 인터뷰 / 관찰 계획

조사할 내용	기간	역할 분담