One-class SVM 알고리즘을 이용한 안드로이드 API의 이상치 탐지 시스템

이지은[1], 최유준[1], 신용태[2]
[1]숭실대학교 컴퓨터학과 석사과정
[2]숭실대학교 컴퓨터학부 교수
lhsgsse10@soongsil.ac.kr, pathfinder357@soongsil.ac.kr, shin@ssu.ac.kr

Android API anomaly Detection System Using One-class SVM algorithm

Ji-Eun LEE[1], Yu-Jun Choi[1], Yong-Tae Shin[2]
[1]Dept. of Computing, Soongsil University
[2]School of Computing, Soongsil University

요 약

스마트폰 발전으로 인한 SNS(Social Network Service), 웹 검색 및 활용 등 편리함과 유용성을 가져다 주었지만 안드로이드 APP의 개방성으로 인하여 프로그램의 원칙적 특성을 악용한 취약점이 발생하고 있다. 이를 대응하는 해결방안으로 API에 대한 요청 데이터를 모듈을 통하여 로그 값을 수집한다. 수집된 데이터는 로그 값을 시간을 기준으로 라벨링하여 이상치 탐지 알고리즘인 OCSVM의 이상치 평균으로 사용하여 실시간 데이터 영향을 받는 하이퍼파라미터 C 와 r 값을 Grid Search 기법을 통해 조정함으로써 최적의 파라미터 값을 찾는 시스템을 제안한다.

1. 서론

2023년 1월 카카오톡의 LOCO 프로토콜을 악용해 오픈 채팅방 참여 이용자의 카카오톡 프로필 ID, 실명, 카카오톡 로그인에 쓰이는 이메일 주소, 전화번호 등의 개인정보를 추출하는 과정을 담은 글이 논란이 되었다. 이는 API의 특징인 'API는 이용자 요청에 응답한다'는 프로그램의 원칙적 특성을 악용하여 발생한 공격이라 추측했다. 이처럼 실시간으로 데이터를 주고받는 서비스를 지원하는 안드로이드 API의 취약점을 분석하고 그에 대응할 수 있는 해결방안으로 이상치 탐지 기법이 있다.

따라서 본 논문에서는 API 요청 데이터를 모듈을 이용하여 데이터의 로그 값을 수집하고 수집된 데이터의 로그 값을 시간을 기준으로 라벨링하여 이상치 평균으로 사용한다. 이때 데이터들이 정상적인 요청인지 비정상적인 요청인지를 OCSVM 이상치 탐지 기법 알고리즘을 통하여 학습한다. OCSVM은 밀도 함수 기반 이상치 탐지 기법으로 확률 밀도 함수 모델링을 기반으로 모델의 성능을 높이려면 데이터 분포를 알아야 한다. 그러나 수집된 데이터들은 실시간 데이터임으로 데이터의 분포가 일정치 않다. 때문에 OCSVM의 하이퍼파라미터 중 데이터 분포의 경계를 결정하는데에 영향을 준다는 문제점이 발생한다. 이를 해결하기 위해서는 Grid Search 기법을 사용하여 통하여 최적의 하이퍼파라미터 조합을 찾는 시스템을 제안한다.

2. 관련 연구

본 장에서는 안드로이드 APP에서 쓰이는 텍스트 파일 형식의 종류와 정상 데이터와 이상 데이터로 구성된 학습 데이터가 주어졌을 때, 이상 데이터를 탐지해줄 OCSVM 알고리즘의 동작원리와 이 알고리즘에 기준 하이퍼파라미터 값을 조정할 Grid Search 기법을 살펴본다.

2.1 텍스트 파일 형식

안드로이드 APP에서 로그를 수집한 텍스트 파일 형식은 실시간 데이터를 주고받는 서비스를 지원하는 안드로이드 APP에서 발생된 API 호출 및 데이터 흐름을 텍스트 파일 형식으로 저장하여 데이터 전처리 및 분석의 효율성을 높여준다. 이러한 텍스트 파일 형식은 다음과 같이 로그 수집 방법에 따라 로그 형식을 구분할 수 있다.

2.1.1 CSV(Comma-Separated Values)

쉼표(,)로 구분된 값 형식으로, 각 로그 메시지마다 시간, 태그, 메시지 등의 정보를 쉼표로 구분하여 저장한다. CSV 형식은 일반적으로 데이터 분석 도구에서 쉽게 읽을 수 있는 형식이다.

2.1.2 JSON(JavaScript Object Notation)

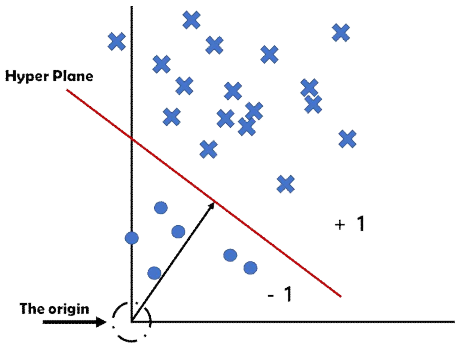
JavaScript 객체 표기법을 이용한 형식으로, 각 로그 메시지를 JSON 객체로 표현한다. JSON 형식은 데이터를 구조적으로 표현할 수 있으며, 다양한 프로그래밍 언어에서 사용되는 표준 데이터 교환 형식이다.

2.1.3 SQLite

안드로이드에서 기본적으로 제공되는 데이터베이스 관리 시스템으로, 로그 메시지를 데이터 베이스에 저장하여 관리할 수 있다. SQLite 형식의 로그는 SQL Query를 이용하여 데이터를 추출할 수 있다.

2.2 OCSVM (One-class Support Vector Machine)

OCSVM 알고리즘이란 비지도 이상치 탐지 알고리즘 중 하나로 하나의 클래스만 존재하는 데이터셋에서 다른 클래스(이상치)를 탐지하는 데에 사용된다. 동작 원리로는 다음(그림 1)과 같다.



(그림 1) OCSVM 동작 원리

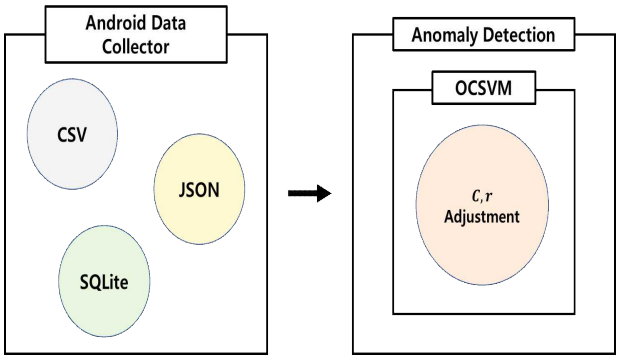
데이터들을 N차원의 좌표축으로 뿌린 후, 원점과의 거리를 기준으로 Hyper Plane을 그어 Claasification(분류)하는 원리로 이는 원점을 기준으로 하기에, 조건에 따라 데이터가 많아도 Class가 1개이다. 그렇게 찾은 하나의 클래스(정상 클래스)를 대표하는 결정 경계는 정상 클래스의 중심이 되는 영역으로 설정되며, 다른 클래스(이상치)는 이 결정 경계 밖에 존재하게 된다.

2.3 Grid Search 기법

하이퍼파라미터 최적화에 사용되는 일반적인 기법 중 하나로 가능한 모든 하이퍼파라미터 조합을 시도하여 최적의 조합을 찾는 방법이다. 동작 원리로는 각 하이퍼파라미터의 가능한 값을 정의하고, 이 값들을 조합하여 그리드를 형성한다. 그리드는 모든 가능한 하이퍼파라미터 조합을 나열하는 표 형태를 가지며 각 조합마다 모델을 학습하여 검증 데이터에서의 성능을 평가한다.

3. 제안

OCSVM 알고리즘은 비지도 학습 기법으로 레이블이 없는 데이터셋에 적합한 기법이다. 텍스트 파일 형식 데이터는 대부분 레이블이 없는 데이터이기 때문에 OCSVM 알고리즘을 적용하기에 적합하다. OCSVM 알고리즘은 밀도 함수 기반(density-based) 이상치 탐지 기법으로 확률 밀도 함수 모델링을 기반으로 하기 때문에 데이터 분포를 알아야 모델의 성능을 높일 수 있다. 그러나 제안하는 Android Data Collector에 수집되는 데이터는 실시간으로 주고받는 메시지 형식의 데이터임으로 데이터 분포가 일정치 않다는 문제점이 있다. 따라서 OCSVM의 하이퍼파리미터 중 데이터와 OCSVM 경계 사이의 거리를 제어하는 C와 RBF 커널 함수의 폭을 제어 조정하는 γ에 영향을 준다는 문제점이 있다. 이를 해결하기 위해 Grid Search 기법을 사용하여 최적의 하이퍼파라미터 조합을 찾는 시스템(그림 2)을 제안한다.



(그림 2) 제안하는 시스템 구조

3.1 Android Data Collector

로그는 각 로그 메시지마다 시간, 로그 레벨, 태그, 메시지 등의 정보를 담고 있는 ADB(Android Debug

Bridge)를 통해 로그 메시지를 수집한다.

3.2 Anomaly Detection

Grid Search 기법을 사용하여 데이터와 OCSVM 경계 사이의 거리를 제어하는 C와 RBF(Radical Basis Function)커널 함수의 폭을 제어하는 γ의 파라미터 값을 사용하여 최적의 파라미터 값을 찾는다. 데이터와 OCSVM 경계 사이의 거리를 제어하는 C 값은 다음 (식 1)과 같다.

$$\min_{w} \frac{1}{2}\|w\|^2 + \frac{1}{vl}\sum_{i=1}^{l}\xi_i - \rho \qquad \text{(식 1)}$$

$$\text{subject to:}$$

$$(w \bullet \phi(x_i)) \geq \rho - \xi_i \qquad \text{for all } i = 1, \ldots, l$$

$$\xi_i \geq 0 \qquad \text{for all } i = 1, \ldots, l$$

위 수식에서 수집된 데이터의 로그 값(ρ)은 메시지마다 시간을 기준으로 라벨링하여 데이터에서 수집된 시간 값들 중 변환하는 데이터의 이상치 평균으로 한다. ρ값을 (그림 1)의 원점(The Origin)으로 지정하고 지정한 원점과 Hyper Plane 간의 거리가 최대한 멀어지도록 ρ값을 빼줌으로써 최소화 문제를 만족할 때에서의 ρ가 최대가 되도록 한다. Hyper plane 바깥에 있는 비정상적인 데이터군들 또한 각각의 평균을 구하여 Hyper plane에 최대한 멀어지게 하는 것을 목적으로 둔다.

(식 1)을 통해 표본 데이터 간의 유사도를 측정하는 값을 정의한다. 이렇게 수집된 데이터의 폭을 제어하고 고차원으로 변환해주는 RBF 커널 함수를 이용한다. RBF 커널 함수를 구하는 식은 다음(식 2)과 같다.

$$k_{RBF}(x_1, x_2) = \exp(-\gamma\|x_1 - x_2\|^2) \qquad \text{(식 2)}$$

위 수식에서 수집된 데이터 간 유사도를 측정하는 값(γ)을 구하고 원에 가장 가까운 x_k의 Support Vector를 통해 R^2(반지름)을 계산하고 수집된 데이터가 가질 수 있는 Support Vector의 최소 개수(vl)를 구하는 커널 함수를 Android Data Collector의 텍스트 데이터에 대한 확률분포를 정의하는 변환함수 커널로 정의한다.

따라서 (식 1)과 (식 2)를 통하여 메시지 형태로 송수신되는 데이터의 분포를 예측하고 데이터 간의 유사도를 측정한다. 이를 통해 전체 요청 데이터 중 정상적인 데이터와 비정상 데이터에 대한 분포를 계산하고 Hyper Plane 구간을 Support Vector로 계산된 γ의 기준선으로 계산하는 방식을 제안한다.

위와 같은 방법을 통해 API의 실시간 데이터를 시간을 기준으로 라벨링하여 변환하는 데이터의 이상치 평균을 OCSVM의 원점을 기준으로 두고 로그를 수집하는 Android Data Collector를 이용하여 텍스트 메시지에 대한 확률분포를 정의하는 변환함수의 커널로 정의함으로써 위 시스템을 통해 실시간 데이터에 영향을 주는 하이퍼파라미터의 최적 값을 찾아 기존 이상치 탐지의 문제점을 보완할 수 있다.

4. 결론

Android Data Collector에서 수집된 데이터는 실시간 데이터임으로 데이터 분포가 일정치 않다는 문제점을 위 시스템을 통해 해결할 수 있다. 하지만 수집된 데이터를 제안하는 시스템에 적용하기 위해서는 텍스트 데이터를 이상치 스코어를 통해 사용해야 하기 때문에 데이터의 마스킹에 대한 문제점이 발생할 수 있는 한계점을 가지고 있다. 따라서 향후 연구에서는 수집된 데이터에서 이상치 스코어를 사용하여 데이터셋에서 이상치를 식별하면 해당 이상치를 검토하여 민감한 정보가 관련된 경우 해당 정보를 마스킹하는 연구 분석을 통해서 본 연구의 한계점을 개선할 것이다.

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음" (IITP-2023-2020-0-01602)

참고문헌

[1] Anh Khoi NGO HO, Nicolas RAGOT, Document Classification in a non-stationary environment: A One-Class SVM Approach, International Conference on Document Analysis and Recognition, 2013

[2] Ming Zhang, Boyi Xu, Jie Gong, An Anomaly Detection Model based on One-class SVM to Detect Network Intrusions, International Conference on Mobile Ad-hoc and Sensor Networks, 2015