# 다크 웹에서 실시간 악성 URL 탐지시스템 연구

이종우[1], 정태연[2], 강원희[3],박태수[4],유동영[5]
[1] [2] [3] [4]홍익대학교 소프트웨어융합학과 학부생
[5]홍익대학교 소프트웨어융합학과 교수
any4time@naver.com,jty84373786@gmail.com,kwh4748@naver.com,
xkdlffpshf@naver.com, ydy@hongik.ac.kr

# A Research of Real-time Malicious URL Detection System in Dark Web

Jong-Woo Lee[1], Tae-Yeon Jeong[2], Won-Hee Kang[3], Tae-Su Park[4],
Dong-Young Yoo[5]
[1] [2] [3] [4] [5]Dept. of Software and Communications Engineering, Hongik University

요 약

본 논문에서는 DarkWebGuard라는 실시간 악성 URL 탐지 시스템을 소개하고, 그 개발에 사용된 도구와 알고리즘에 대해 논의합니다. DarkWebGuard는 머신러닝을 기반으로 하며, 인터넷 보안에 대한 현재의 요구를 충족시키기 위해 개발되었습니다. 이 시스템은 사용자와 시스템을 보호하기 위해 악성 URL을 실시간으로 탐지하고 분류합니다.

## 1. 서론

최근 몇 년간 인터넷의 보급으로 인해 악성 URL에 대한 위협이 커지고 있습니다. 이에 따라 사용자 및 시스템 보호의 필요성이 증대되고 있습니다. 본 논문에서는 이러한 환경 변화에 대응하여 DarkWebGuard라는 실시간 악성 URL 탐지 시스템을 소개합니다. DarkWebGuard는 현존하는 보안 시스템과는 다르게 머신러닝 알고리즘을 기반으로 한다는 특징을 가지고 있으며, 이를 통해 보다 효과적인 악성 URL 탐지 및 분류를 가능케 합니다.

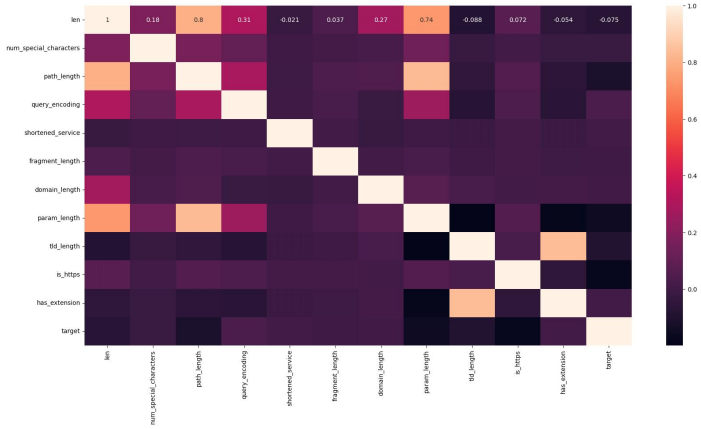
## 2. 데이터 엔지니어링 및 전처리

데이터 엔지니어링 및 전처리는 DarkWebGuard 시스템의 핵심적인 부분으로, 실시간 및 배치 데이터의 효율적인 수집과 처리가 필요합니다. 먼저, 데이터 엔지니어링팀은 Kaggle의 Malicious URLs Dataset을 주 데이터셋으로 선정하였습니다. 이 데이터셋은 다양한 악성 URL을 포함하고 있으며, 이를 기반으로 모델을 학습시키기 위해 사용됩니다.[1]

또한, UNB의 2016 URL Dataset과 Mendeley의 웹페이지 분류 데이터셋과 같은 보조 데이터셋도 활용됩니다. 이 보조 데이터셋은 다양한 형태의 URL을 포함하고 있어 DarkWebGuard 모델의 다양성과 일반화에 도움이 됩니다.

데이터 전처리 과정에서는 데이터셋의 정제와 특성 추출이 수행됩니다. 정제 과정에서는 데이터의 중복 제거, 누락된 값 처리 등이 이루어지며, 특성 추출 단계에서는 URL의 길이, 특수 문자 수, 경로 길이 등과 같은 특성들을 추출합니다.

이러한 작업은 Python과 Pandas를 사용하여 수행되며, 웹 크롤링을 통해 추가적인 데이터를 수집하고 정제하는 작업도 이루어집니다. 최종적으로, 전처리된 데이터셋은 훈련, 검증 및 테스트 세트로 분할되어 모델 학습에 활용됩니다.




(그림 1) 특성 간 상관 관계 히트맵

(그림1)은 데이터의 다양한 특성 사이의 상관계수를 색상의 강도로 나타낸 시각적 도구입니다.

### 3.모델 개발 및 평가

DarkWebGuard의 핵심적인 부분은 머신러닝 모델의 개발과 평가입니다. 이를 위해 머신러닝 라이브러리인 Scikit-learn과 XGBoost[2]를 사용하여 기본적인 모델을 개발하고, TensorFlow와 Keras를 활용하여 딥러닝 모델도 개발됩니다.

모델의 평가는 교차 검증을 통해 이루어지며, 이를 통해 모델의 일반화 능력을 평가할 수 있습니다. 성능 메트릭스를 계산하여 모델의 정확도, 정밀도, 재현율 등을 평가하고, GridSearchCV와 RandomSearchCV를 사용하여 하이퍼파라미터를 튜닝합니다. 이러한 과정을 통해 최적의 모델을 선정하고, 최종 모델을 선택하여 성능을 검증합니다.[3]

### 4. 실시간 분석 및 응답

DarkWebGuard 시스템은 사용자의 URL 입력을 실시간으로 분석하고, 결과를 즉각적으로 반환해야 합니다. 이를 위해 Flask 또는 FastAPI와 같은 웹 프레임워크를 사용하여 API를 개발하고, Redis를 데이터베이스로 활용합니다.

데이터베이스에 저장된 URL은 모델에 입력으로 제공되고, 모델은 실시간으로 URL을 분석하여 악성 여부를 판단합니다. 이후, 분석 결과를 사용자에게 반환하여 사용자의 보호를 위해 경고를 제공합니다.[4]

### 5. 시스템 통합 및 개선

DarkWebGuard 시스템의 통합과 개선은 사용자가 모델의 분석 결과를 쉽게 활용할 수 있도록 하는 것을 목표로 합니다. 먼저 REST API를 사용하여 개발된 머신러닝 모델을 웹 서비스나 애플리케이션과 통합합니다. 이를 통해 사용자는 URL을 입력하고 분석 결과를 받아볼 수 있습니다.

동시에 Prometheus와 Grafana와 같은 도구를 활용하여 시스템의 성능과 모델의 응답을 실시간으로 모니터링[5]하여 성능 저하나 장애를 빠르게 감지하고 대응합니다. 또한 모델의 성능 데이터와 사용자 피드백을 분석하여 모델을 지속적으로 조정하고 개선하여 사용자에게 더 나은 보호를 제공할 수 있도록 합니다.

### 6. 결론

본 논문에서는 XGBoost 기법을 활용한 다크웹 사이트에 대한 실시간 탐지 시스템을 제안합니다. XGBoost는 그라디언트 부스팅 기반의 머신러닝 알고리즘으로, 고차원의 데이터와 복잡한 패턴을 처리하는 데 효과적입니다. 이를 통해 다크웹의 다양한 특성을 식별하고, 악성 사이트를 실시간으로 감지하여 사용자를 보호하는 시스템을 구축할 수 있습니다.

본 연구에서는 개발된 시스템은 잠재적으로 위험한 특성을 가진 다크웹 사이트를 탐지하는 데 효과적인 방법 중 하나입니다. 이러한 특성은 급격한 URL 주소 변경, 의심스러운 트래픽 패턴, 암호화된 데이터 교환 등을 포함할 수 있습니다. 이러한 특성을 기반으로 하는 탐지 시스템은 보다 정확하고 신속하게 악성 다크웹 사이트를 식별할 수 있습니다.

### 참고문헌

[1] Jongkwan Kim, Minhae Jang, Suna Lim, Myongsoo Kim, "A Study on the Detection Method of Malicious URLs based on the Internet Search Engines using the Machine Learning," The Transactions of The Korean Institute of Electrical Engineers, vol. 70, no. 1, pp. 114-120, January 2021.

[2]Suyun Park, "Malicious Insider Detection Using Boosting Ensemble Methods," Journal of the Korea Institute of Information Security & Cryptology, vol. 32, issue 2, pp. 267-277, 2022.

[3]강준구, 김대형, 박수태, "다중 머신러닝 알고리즘을 이용한 악성 URL 예측 시스템 설계 및 구현," 멀티미디어학회논문지, 제23권, 제11호, 1396-1405쪽, 2020년

[4]Youngjun Kim, Jaewoo Lee, "Development of a Malicious URL Machine Learning Detection Model Reflecting the Main Feature of URLs," Journal of The Korea Institute of Information and Communication Engineering, vol. 26, no. 12, pp. 1786-1793, December 2022.

[5]Swaroop Chitlur, Kornel Csernai, "Maintaining Machine Learning Model Accuracy Through Monitoring," DoorDash Engineering Blog, May 20, 2021.