Journal of Korea Multimedia Society Vol. 23, No. 11, November 2020(pp. 1396-1405)
https://doi.org/10.9717/kmms.2020.23.11.1396

다중 머신러닝 알고리즘을 이용한 악성 URL 예측 시스템 설계 및 구현

강홍구[†], 신삼신[††], 김대엽[†††], 박순태[††††]

Design and Implementation of Malicious URL Prediction System based on Multiple Machine Learning Algorithms

Hong Koo Kang[†], Sam Shin Shin[††], Dae Yeob Kim[†††], Soon Tai Park[††††]

ABSTRACT

Cyber threats such as forced personal information collection and distribution of malicious codes using malicious URLs continue to occur. In order to cope with such cyber threats, a security technologies that quickly detects malicious URLs and prevents damage are required. In a web environment, malicious URLs have various forms and are created and deleted from time to time, so there is a limit to the response as a method of detecting or filtering by signature matching. Recently, researches on detecting and predicting malicious URLs using machine learning techniques have been actively conducted. Existing studies have proposed various features and machine learning algorithms for predicting malicious URLs, but most of them are only suggesting specialized algorithms by supplementing features and preprocessing, so it is difficult to sufficiently reflect the strengths of various machine learning algorithms. In this paper, a system for predicting malicious URLs using multiple machine learning algorithms was proposed, and an experiment was performed to combine the prediction results of multiple machine learning models to increase the accuracy of predicting malicious URLs. Through experiments, it was proved that the combination of multiple models is useful in improving the prediction performance compared to a single model.

Key words: Malicious URL, Prediction, Multiple Machine Learning, Web Threat

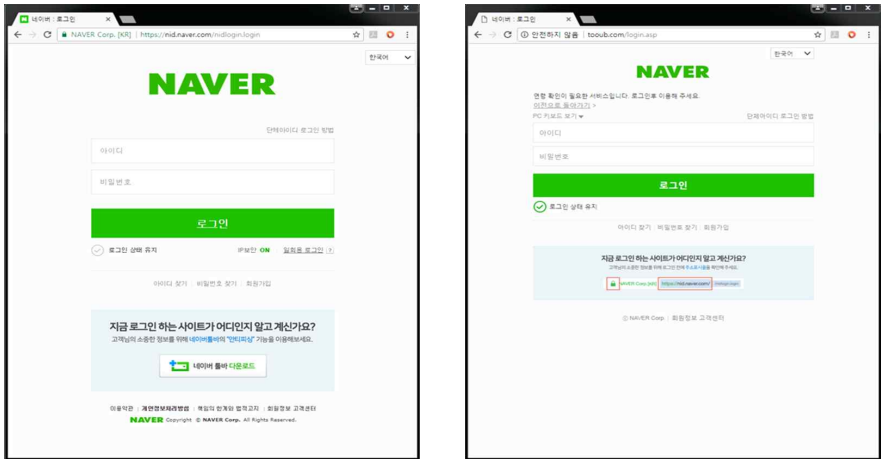
1. 서 론

악성 URL을 이용한 개인정보 강제수집, 악성코드 유포 등의 사이버 위협이 지속적으로 발생하고 있다. 이러한 사이버 위협을 대응하기 위해 악성 URL을 신속하게 탐지하고 피해를 예방하는 보안기술이 요구되고 있다[1]. 악성 URL을 통한 개인정보 강제수집 수법으로 피싱(phishing)이 많이 악용되고 있다. 피싱은 위장된 웹페이지, 이메일을 통하여 PC 및 모바일 기기 사용자가 보유하고 있는 온라인 서비스

※ Corresponding Author : Soon Tai Park, Address: (58324) 9, Jinheung-gil, Naju-si, Jeollanam-do, Korea, TEL : +82-61-820-1030, FAX : +82-61-820-2607, E-mail : stpark12@kisa.or.kr
Receipt date : Oct. 8, 2020, Approval date : Nov. 3, 2020
[†] Security Threat Response R&D Team, Korea Internet & Security Agency (E-mail : redball@kisa.or.kr)
[††] Security Threat Response R&D Team, Korea Internet & Security Agency (E-mail : sss@kisa.or.kr)
[†††] Security Threat Response R&D Team, Korea Internet & Security Agency (E-mail : yeob@kisa.or.kr)
[††††] Security Threat Response R&D Team, Korea Internet & Security Agency
※ This research was financially supported by the Institute of Civil Military Technology Cooperation funded by the Defense Acquisition Program Administration and Ministry of Trade, Industry and Energy of Korean government under grant No. M19204RD2

계정, 주민등록번호, 주민등록번호, 계좌번호, 카드번호 등의 주요 개인정보를 수집하는 공격 기법이다. 피싱 공격자는 사용자의 개인정보 입력을 유도하기 위하여 유명 온라인 서비스의 웹페이지와 동일한 화면 구성을 주로 이용한다. Fig. 1은 국내 유명 포털 사이트의 정상 로그인 페이지와 동일한 화면 구성을 이용한 피싱 페이지 사례를 보여준다. 피싱 페이지는 정상 페이지의 화면과 동일한 구성을 보이지만 실제 URL 주소와 프로토콜은 서로 다름을 알 수 있다. 공격자는 피싱 페이지를 통해 사용자의 계정 정보를 탈취함으로써 사용자의 이메일, 주소록, 사진 등을 도용하는 사생활 침해뿐만 아니라 스팸메일 발송, 스피어 피싱(spear phishing), 악성코드 유포, 디도스(DDos) 공격 등 추가적인 사이버 공격을 수행할 수 있다[2].

악성 URL 접속을 통한 악성코드 유포 공격도 지속적으로 발생하고 있다. 악성 URL을 통해 악성코드가 감염되는 경로는 크게 두 가지로 분류할 수 있다. 첫 번째는 사용자 PC에 직접 악성코드를 감염시키는 유포지(distribution site)와 사용자들로 하여금 유포지로 접속을 유도하는 경유지(hopping site)이다. 한국인터넷진흥원(KISA)에 따르면 2020년 상반기 악성코드 경유지는 2,358개, 유포지 326개, 악성코드는 196개가 탐지되었고, 악성코드 유형별 비율은 정보유출(기기정보, 계정정보) 66.3%, 디도스 9.7%, 원격제어 7.1%, 랜섬웨어 6.1%, 다운로더 5.1%로 나타났



(a) (b)

Fig. 1. Real web page (a) and phishing web page (b) of a portal site.

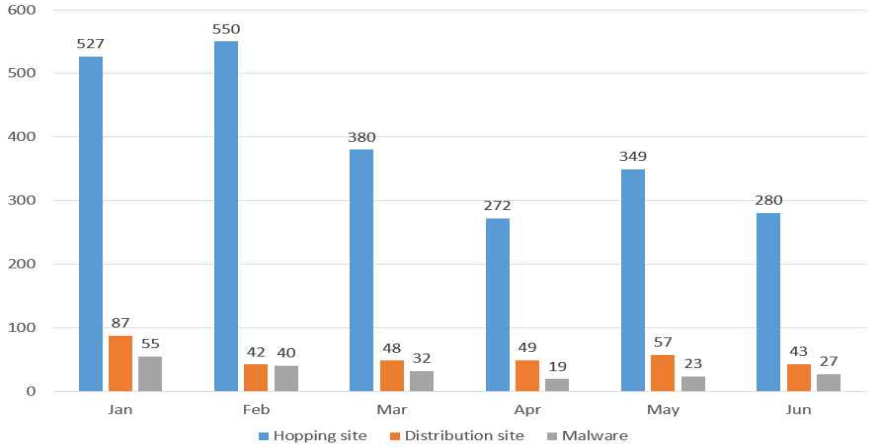


Fig. 2. Status of malicious code hidden sites detection in the first half of 2020.

다[3].

이처럼 웹 환경에서 개인정보 유출, 악성코드 감염 등 사이버 위협을 효율적으로 대응하고 피해를 최소화하기 위해서는 악성 URL을 신속하게 식별하고 차단하는 기술이 필요하다. 그러나 악성 URL의 형태가 다양하고 수시로 생성 및 삭제되기 때문에 블랙리스트(blacklist) 방식이나 시그니처 매칭(signature matching) 방식으로 탐지하거나 필터링하는 방법으로는 대응에 한계가 있다[4].

이러한 한계를 극복하기 위해 최근 머신러닝 기법을 이용하여 악성 URL을 탐지하고 예측하는 연구가 활발하게 진행되고 있다[5-15]. 기존 연구에서는 악성 URL 탐지를 위해 다양한 특징과 머신러닝 알고리즘이 제안되고 있으나 대부분 특징과 전처리 과정을 보완하여 특화된 알고리즘을 제안하고 있어 다양한 머신러닝 알고리즘의 장점을 충분히 반영하기 어렵다. 본 논문에서는 다중 머신러닝 알고리즘을 이용하여 악성 URL을 예측하는 시스템에 대해 제안하고, 예측 정확도를 향상시키기 위해 머신러닝 모델 조합의 예측 결과를 측정하는 실험을 수행하였다. 실험을 통해 단일 모델과 비교하여 다수 모델 조합이 예측 성능 향상에 유용함을 증명하였다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문에서 이용하는 머신러닝 알고리즘과 이를 이용한 악성 URL 탐지 및 예측 관련 연구에 대하여 설명하고 3장에서는 본 논문에서 제안하는 다중 머신러닝 알고리즘을 이용한 악성 URL 예측 시스템에 대해 설명한다. 여기에서는 제안한 시스템의 구성도와 악성 URL 예측을 위한 처리과정, 학습에 사용되는 특징 그리고 구현된 시스템 GUI와 동작 결과의 순서로 서술한다. 그리고 4장에서는 제안한 시스템으로 실험한 결과를 단일 모델과 다중 모델의 예측 정확도를 비교하여 성능을 평가하고 5장에서 결론을 맺는다.

2. 관련연구

Decision tree(DT)는 라벨링(labeling)된 데이터 분류에 주로 사용되는 알고리즘으로 의사결정 규칙을 이용하여 대량의 데이터로부터 데이터 내에 존재하는 관계, 패턴, 규칙 등을 분석하고 모형화하여 분류 및 예측을 수행한다. [5]는 DT를 이용해 하이브리드 방식으로 새로운 특징을 포함하여 100여개 특징을 사용하였으며, 6개의 DT 모델로 학습한 결과를 도출하였다. 결과적으로 제안한 특징을 추가했을 때의 결과가 그렇지 않은 결과보다 정확도가 높음을 제시하였다. [6]은 악성 URL의 구성 패턴 분석을 기반으로 악성 URL을 탐지하는 연구를 수행하였으며 DT를 이용한 실험에서 94%의 탐지 성능을 보였다.

Random forest(RF)는 분류, 회귀 분석 등에 사용되는 앙상블 학습방법의 일종으로, 훈련 과정에서 구성한 다수의 DT로부터 분류 또는 평균 예측치를 출력한다. [7]은 RF를 이용하여 악성 URL 분류 연구를 수행하였고 다양한 URL 특징을 사용하여 랜덤하게 훈련된 DT들의 앙상블로 분류하는 예측 방법을 제안하였다. [8]은 악성 URL을 배포하는 악성 도메인을 탐지하는 연구를 수행하였으며 RF를 이용한 실험에서 91.5%의 탐지 성능을 보였고, [9]는 앙상블 기법을 이용한 다수의 학습방법들로 피싱 웹사이트의 분류 성능을 비교하였으며 RF가 가장 좋은 성능을 보였다.

Gradient boosting machine(GBM)는 RF와 마찬가지로 분류, 회귀 분석 등에 사용되는 앙상블 학습방법의 일종으로 앙상블 방법론에서 RF가 배깅(bagging) 계열에 속하는 반면 GBM은 부스팅(boosting) 계열에 속하는 알고리즘이다. [10]은 GBM를 이용하여 피싱 URL 탐지 성능을 측정하였다. 해당 연구에서는 피싱 URL 15,000개, 정상 URL 15,000만개를 대상으로 어휘적(lexical) 특징 26개를 이용하여 90.7%의 탐지 정확도를 보였다. [11]은 URL의 어휘적 특징을 중심으로 212개 특징을 이용하여 피싱 URL을 탐지하는 연구를 수행하였다.

XGBoost(XGB)는 gradient boosting 알고리즘을 분산 환경에서 실행할 수 있도록 구현한 라이브러리로 분류, 회귀 문제를 모두 지원하고 성능과 자원 효율이 우수하여 악성코드를 식별하고 분류하는 분야에서도 많이 사용되고 있다. [12]는 XGB를 이용하여 악성 URL 탐지 성능을 측정하였다. 해당 연구에서는 악성 URL 약 18만개, 정상 URL 약 35만개를 이용하여 17개 특징을 추출하였고, XGB를 이용한 탐지 정확도는 72%를 도출하였다. [13]은 30개 특징을 추출하여 XGB를 통해 피싱 URL 탐지 기법을 제시하였다.

Support vector machine(SVM)은 하나의 클래스에 속하는 포인트들이 모여 있는 지역에 경계를 설정

하는 방식의 알고리즘으로 최적의 경계가 결정되면 입력 데이터가 경계의 어느 부분에 있는지에 따라 분류를 수행한다. [14]는 URL 문자열의 복잡도를 계산하여 악성 URL과 정상 URL를 구분하는 기법을 제안하였다. 분류 알고리즘으로 SVM을 사용하였고, 평균 12.2%의 미탐율을 보였다. [15]는 SVM을 이용하여 트위터(twitter)의 악성 short URL을 탐지하는 기법을 제시하였다.

이처럼 기존 연구에서는 악성 URL를 탐지하고 예측하기 위해 다양한 특징 및 머신러닝 알고리즘을 제안하고 있으나 대부분 특징과 전처리 과정을 보완하여 특화된 알고리즘을 제안하고 있어 다양한 머신러닝 알고리즘의 장점을 충분히 반영하지 못하고 있다. 본 논문에서는 신속한 악성 URL 예측을 위해 URL로부터 특징 추출 과정이 용이한 어휘적 특징을 이용하고 단일 모델의 예측 성능을 개선할 수 있는 다수의 모델 조합을 적용한 다중 머신러닝 기반 악성 URL 예측 시스템을 제안한다.

3. 다중 머신러닝 기반 악성 URL 예측 시스템

본 논문에서 제안하는 다중 머신러닝 기반 악성 URL 예측 시스템은 URL의 어휘적 특징을 이용하여 여러 머신러닝 알고리즘별로 모델을 생성하고, 모델들의 조합을 통해 URL의 악성여부를 예측하는 시스템이다. Fig. 3은 다중 머신러닝 기반 악성 URL 예측 시스템의 구성도를 보여준다. 본 논문에서 제안하는 시스템은 특징 추출 모듈, 벡터 생성 모듈, 모델 생성 모듈, 악성 URL 예측 모듈로 구성된다.

특징 추출 모듈은 학습을 위해 수집한 대량의 정상/악성 URL을 입력받아 어휘적 특징을 추출한다.

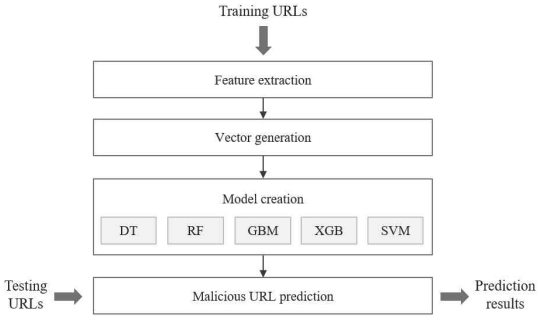


Fig. 3. Configuration diagram of malicious URL prediction system.

벡터 생성 모듈은 특징을 수치화, 정규화를 통해 벡터 형태의 학습데이터로 변환한다. 모델 생성 모듈은 5개 머신러닝 알고리즘별 학습을 수행하여 모델을 생성한다. 마지막으로 악성 URL 예측 모듈은 테스트 URL을 입력받아 모델별 예측 결과를 도출한다. Fig. 4는 다중 머신러닝 기반 악성 URL 예측 시스템의 처리 과정을 보여준다.

신속하게 악성 URL을 예측하기 위해서는 URL로부터 특징 추출과 처리 과정이 용이해야 되므로 본 논문에서는 URL만으로 추출이 가능한 어휘적 특징을 이용하였다. Table 1은 URL로부터 추출하는 24개의 어휘적 특징을 보여준다. 본 논문에서는 특징별로 측정하는 단위에 따라 길이(length), 개수(count), 존재여부(existence) 유형으로 구분하였다.

이러한 설계를 기반으로 제안하는 시스템을 운영할 수 있는 웹 기반의 GUI을 구현하였다. GUI의 주요 기능은 신규 URL을 입력하는 기능과 머신러닝 모델별 예측 결과를 출력하는 기능이다. Fig. 5는 사용자가 신규 URL을 입력할 수 있는 GUI를 보여준다. 사용자가 입력한 URL에 대해 머신러닝 모델별 예측 결과는 정상과 악성으로 구분하여 보여준다. 정상 URL과 악성 URL 샘플을 이용하여 예측 결과를 보여주는 GUI는 각각 Fig. 6과 Fig. 7과 같다. 정상 URL 샘플은 온라인 쇼핑 사이트로 모델별 예측 결과는 모두 정상이었고, 악성 URL 샘플은 전자상거래를 기반으로 하는 IT 업체의 로그인 사이트를 사칭한 피싱 사이트로 모델별 예측 결과는 모두 악성이었다.

4. 실험 결과 및 고찰

다중 머신러닝 기반 악성 URL 예측 시스템의 성능을 측정하기 위해 정상 URL 436,722개, 악성 URL 158,081개 등 총 594,803개의 URL을 이용하였다. 정상 URL은 글로벌 웹 사이트 순위 정보를 제공하는 서비스인 Alexa[16]를 통해 수집하였고, 악성 URL은 피싱 정보를 제공하는 서비스인 Openphish[17]와 Phishtank[18], 그리고 KISA에서 운영하고 있는 악성코드 은닉 사이트 탐지 시스템(MCF)[19]에서 수집하였다. 모델을 생성하기 위한 학습데이터와 성능 측정을 위한 테스트데이터는 정상 URL과 악성 URL에서 각각 80%, 20% 비율로 구분하여 사용하였다.

24개 어휘적 특징을 이용하여 5개 머신러닝 알고리즘(DT, RF, GBM, XGB, SVM)별로 학습을 수행

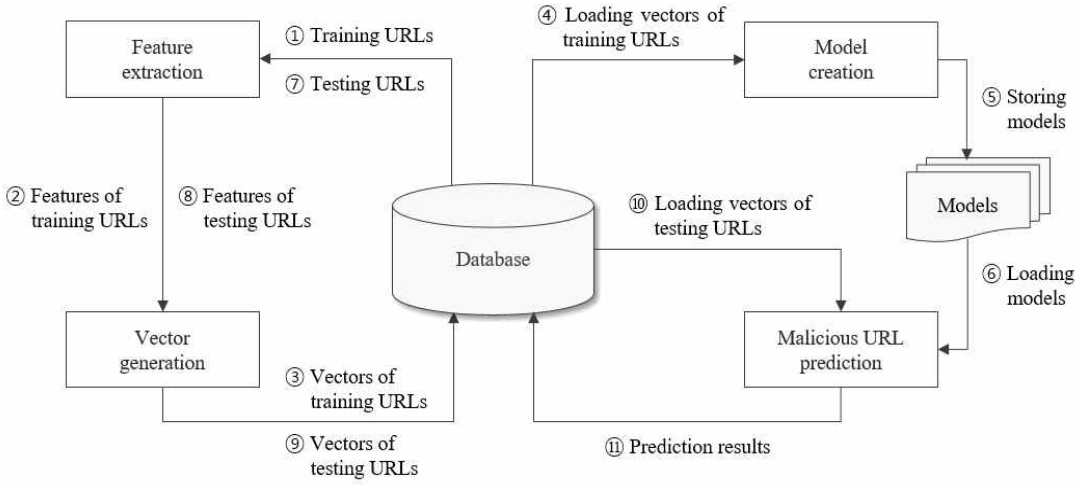


Fig. 4. Process of malicious URL prediction system.

Table 1. Lexical features extracted from URLs

Category	Lexical features	Number
Length-based features	Length of URL, Length of hostname, Length of TLD, Length of path, Depth of URL, Length of first directory	6
Count-based features	Counts of 'http', Counts of 'https', Counts of 'www', Counts of '@', Counts of '?', Counts of '&', Counts of '#', Counts of '%', Counts of '.', Counts of '=', Counts of '_', Counts of '-', Counts of '-' in hostname, Counts of subdomain, Counts of digits, Counts of letters	16
Existence-based features	Existence of IP as hostname, Existence of short URL	2

하였다. 학습에 이용된 URL은 475,842개로 정상 URL 349,476개, 악성 URL 126,366개를 이용하였다. 학습을 통해 생성된 5개 머신러닝 모델을 생성하였고, 테스트에 이용된 URL은 118,961개로 정상 URL 87,246개, 악성 URL 31,715개를 이용하였다.

실험에서 사용된 데이터 셋을 대상으로 특징 간의 상관관계를 분석하였다. 특징 중 URL 내 'www'의 개수, 'https'의 개수, 숫자 개수가 각각 -0.35, -0.34, 0.3로 다른 특징에 비해 높은 상관관계를 보였다. 상관관계 수치만을 보면 개별적인 특징만으로는 정상 URL과 악성 URL을 예측하는데 큰 영향을 주지 않

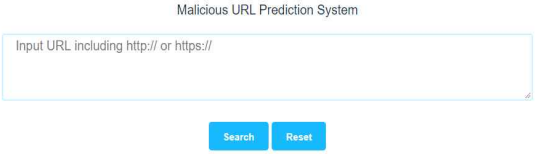
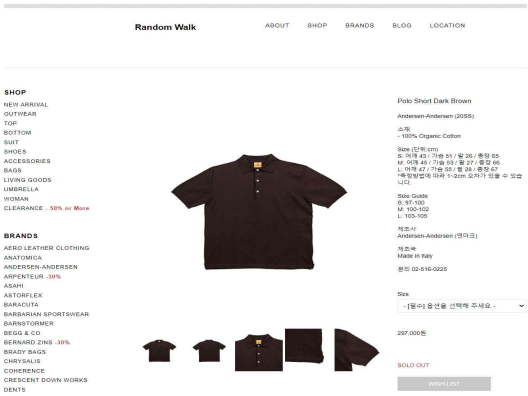


Fig. 5. GUI for URL input.

는다는 것을 알 수 있다. 그러나 24개의 특징을 모두 이용하는 경우에는 Table 3에서 보듯이 정상 URL과 악성 URL 예측에 유용한 것을 알 수 있다.

5개 머신러닝 모델을 이용한 실험결과에서 예측 정확도(accuracy)는 평균 91.35%를 보였으며, RF가 93.51%로 가장 좋은 성능을 보였다. 그러나 정상 URL에 대한 recall을 측정한 결과에서 SVM과 XGB가 각각 97.43%과 96.91%로 RF의 96.82% 보다 높았고, 악성 URL에 대한 precision을 측정한 결과에서는 XGB와 RF가 90.61%로 동일한 성능을 보였고, 정상 URL에 대한 recall을 측정한 결과도 GBM과 RF가 96.82%로 동일한 성능을 보였다.

이와 같이 서로 동일한 특징을 이용했음에도 불구하고 모델별로 성능이 서로 다르게 나타났으며, 이러한 점을 착안하여 가장 좋은 성능을 보인 RF를 기준으로 다른 모델들을 조합한 경우의 정확도를 비교하였다. 다중 모델을 이용하여 정상 URL과 악성 URL



(a)

Look up again

[Analysis URL]: http://www.randomwalk.co.kr/product/detail.html?product_no=1797&cate_no=109&display_group=1

Algorithm	Prediction	Benign rate	Malicious rate
DT	Benign	1.00	0.00
RF	Benign	0.90	0.10
GBM	Benign	1.00	0.00
XGB	Benign	0.88	0.12
SVM	Benign	1.00	0.00

(b)

Fig. 6. A benign URL (a) and the prediction result (b) of (a).

(a)

Look up again

[Analysis URL]: http://update.amazoon-co-jp.monster/pc/

Algorithm	Prediction	Benign rate	Malicious rate
DT	Malicious	0.00	1.00
RF	Malicious	0.02	0.98
GBM	Malicious	0.00	1.00
XGB	Malicious	0.05	0.95
SVM	Malicious	0.00	1.00

(b)

Fig. 7. A malicious URL (a) and the prediction result (b) of (a).

을 구분하기 위해서 RF를 포함한 3개 모델과 5개 모델을 조합하였고 모델 조합에서 다수 모델이 동일하게 탐지한 결과로 예측 정확도를 측정하였다. RF를 단일 적용한 것과 비교하여 모델 조합의 평균 오탐수는 정상 URL에서 777개, 악성 URL에서 211개가 줄어서 오탐수가 평균 16.13% 감소하였다. 또한, 예측 정확도(accuracy)는 RF와 비교하여 모델 조합이 평균 0.83%가 증가하였고, RF와 SVM, GBM을 조합한 경우에 가장 높은 성능 향상을 보였다.

특히, 5개 모델 조합의 예측 정확도가 94.60%로 3개 모델 조합의 평균 예측 정확도인 94.30% 보다는 높았으나, (RF+XGB+GBM)과 (RF+SVM+GBM) 모델 조합보다는 높지 않았다. 이는 모델 간의 예측 결과에 차이가 있음에도 모델 조합은 URL의 정상과 악성을 판별하는데 다수 모델이 동일하게 탐지한 결과를 이용했기 때문에 모델 개수가 증가하더라도 개별 모델의 성능에 따라 항상 성능이 높아지지 않는다는 것을 알 수 있다.

그리고, 모델별 테스트 URL을 대상으로 예측 결과를 도출하는데 소요된 시간을 측정하였다. 5개 모델의 평균 소요 시간은 1250.52초로 나타났으며 DT가 4.52초로 가장 짧았고 SVM이 6,052.08초로 가장 길었다. SVM을 제외한 모델들의 평균 소요 시간은

Table 2. URLs dataset

Type	Number of URLs			
	Training (≒80%)	Testing (≒20%)	Total	
Benign	349,476	87,246	436,722	594,803
Malicious	126,366	31,715	158,081	

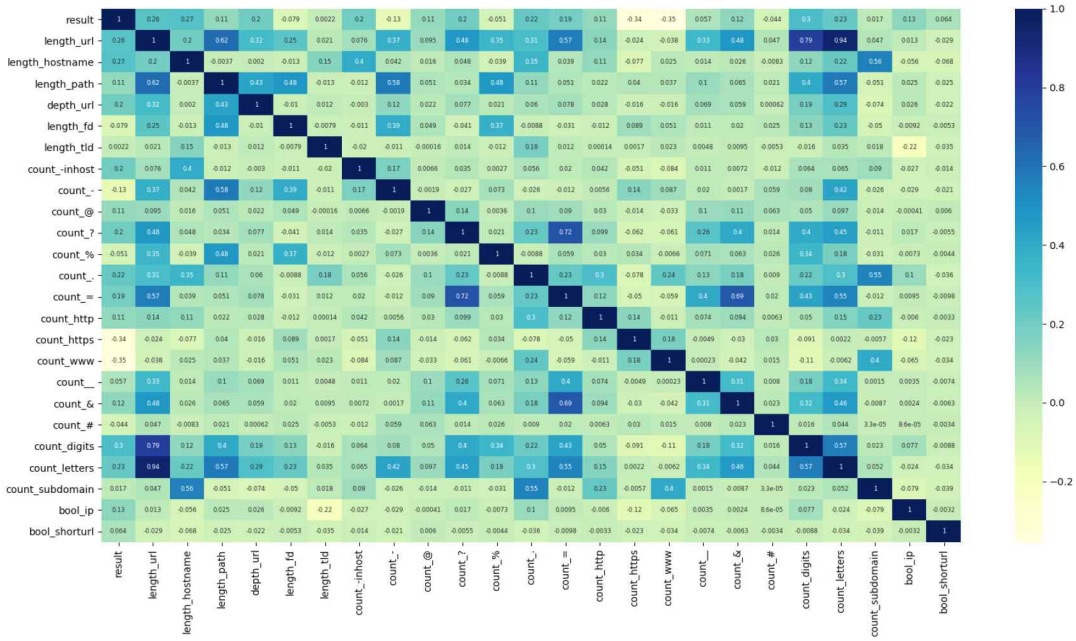


Fig. 8. Heatmap of correlation between features.

Table 3. Performance comparison of machine learning algorithms

Algorithm	Type	Performance			
		Precision [%]	Recall [%]	F1-score [%]	Accuracy [%]
DT	Benign	93.67	95.00	94.33	91.63
	Malicious	85.69	82.34	83.98	
RF	Benign	94.47	96.82	95.63	93.51
	Malicious	90.61	84.41	87.40	
GBM	Benign	90.73	96.82	93.67	90.41
	Malicious	89.26	72.79	80.19	
XGB	Benign	93.66	96.91	95.26	92.92
	Malicious	90.61	81.95	86.06	
SVM	Benign	87.89	97.43	92.42	88.27
	Malicious	89.93	63.08	74.15	

50.13초로 SVM이 다른 모델과 비교하여 상대적으로 소요 시간이 비효율적으로 나타났다. 특히, 다수 모델의 조합으로 예측하는 소요 시간은 모델 중 가장 긴 시간이 걸리는 모델에 종속되므로 가장 긴 소요 시간을 갖는 SVM이 포함된 모델 조합의 소요 시간은 모두 SVM의 소요 시간과 동일하게 된다. 따라서 예측 정확도와 소요 시간을 종합적으로 고려해보면 (RF+XGB+GBM) 모델 조합이 예측에 가장 효율적임을 알 수 있다.

5. 결 론

웹 환경에서 악성 URL을 악용한 개인정보 강제수집, 악성코드 유포 등 사이버 위협이 지속적으로 발생하고 있다. 이러한 사이버 위협을 대응하기 위해 악성 URL을 신속하게 탐지하고 예측하는 보안기술이 시급히 요구되고 있으며 최근 머신러닝 기법을 이용하여 악성 URL을 탐지하고 예측하는 연구가 활발히 진행되고 있다. 본 논문에서는 신속한 악성

Table 4. Performance of machine learning algorithm combination

Algorithm	Type	Performance			
		Precision [%]	Recall [%]	F1-score [%]	Accuracy [%]
RF+DT+GBM	Benign	94.64	97.18	95.89	93.89
	Malicious	91.61	84.86	88.10	
RF+DT+XGB	Benign	94.74	97.17	95.94	93.96
	Malicious	91.61	85.15	88.26	
RF+DT+SVM	Benign	94.62	97.31	95.94	93.96
	Malicious	91.96	84.77	88.22	
RF+XGB+SVM	Benign	94.73	97.98	96.33	94.52
	Malicious	93.87	85.01	89.22	
RF+XGB+GBM	Benign	94.92	97.93	96.40	94.64
	Malicious	93.76	85.58	89.48	
RF+SVM+GBM	Benign	94.75	98.39	96.54	94.82
	Malicious	95.04	85.01	89.75	
RF+DT+XGB +SVM+GBM	Benign	94.78	98.03	96.38	94.60
	Malicious	94.01	85.16	89.36	

Table 5. Improvement rate of false positive and accuracy

Algorithm	Type	Improvement rate(IR)		
		False Positive(FP) [qty]	IR of FP [%]	IR of Accuracy [%]
RF	Benign	2,775	-	-
	Malicious	4,944	-	
RF+DT+GBM	Benign	2,464	11.21	0.38
	Malicious	4,803	2.85	
RF+DT+XGB	Benign	2,472	10.92	0.45
	Malicious	4,710	4.73	
RF+DT+SVM	Benign	2,351	15.28	0.45
	Malicious	4,829	2.33	
RF+XGB+SVM	Benign	1,760	36.58	1.01
	Malicious	4,755	3.82	
RF+XGB+GBM	Benign	1,807	34.88	1.13
	Malicious	4,572	7.52	
RF+SVM+GBM	Benign	1,408	49.26	1.31
	Malicious	4,753	3.86	
RF+DT+XGB +SVM+GBM	Benign	1,721	37.98	1.08
	Malicious	4,708	4.77	

Table 6. Test time of machine learning algorithms

Algorithm	DT	RF	GBM	XGB	SVM
Time [sec]	4.52	87.63	82.26	26.10	6,052.08

URL 예측을 위해 특징 추출이 용이한 어휘적 특징을 이용하고 다중 머신러닝 모델을 적용한 악성 URL 예측 시스템을 제안하였다. 그리고 실험을 통해 단일 모델 보다 다양한 모델 조합이 악성 URL 예측 성능 향상에 유용함을 증명하였다.

향후 연구에서는 악성 URL 예측 정확도와 처리속도 개선을 위해 대량의 악성 URL을 지속적으로 확보하고, 다양한 어휘적 특징을 대상으로 유용성을 검증을 통해 예측 모델을 정교화하고자 한다. 그리고 머신러닝 알고리즘뿐만 아니라 딥러닝 알고리즘을 추가하고 알고리즘별로 적합한 특징을 차별적으로 적용하여 다양한 알고리즘의 장점을 최대한 이용할 계획이다. 또한, 다중 모델의 결과를 조합하는 앙상블 기법을 개발하여 향상된 예측결과가 도출될 수 있도록 시스템을 고도화할 예정이다.

REFERENCE

[1] H.K. Kang, S.S. Shin, D.Y. Kim, and S.T. Park, "A Study on Analysis of Feature Information for Malicious URL Prediction," *Proceeding of the 21th Conference on Electronics and Information Communications*, pp. 1-4, 2019.

[2] H.K. Kang, S.S. Shin, D.Y. Kim, and S.T. Park, "A Study on the Design of Malicious URL Prediction System Based on Machine Learning," *Proceeding of the Korea Multimedia Society Conference*, pp. 13-16, 2020.

[3] Malicious Code Hidden Site Detection Trend Report in the First Half of 2020 (2020), https://www.krcert.or.kr/data/reportView.do?bulletin_writing_sequence=35537 (accessed July 29, 2020).

[4] D. Sahoo, C. Liu, and S.C.H. Hoi, "Malicious URL Detection Using Machine Learning: A Survey," *arXiv Preprint arXiv:1701.07179*, 2017.

[5] D. Patil and J. Patil, "Malicious URLs Detection Using Decision Tree Classifiers and Majority Voting Technique," *Journal of Cybernetics and Information Technologies*, Vol. 18, No. 1, pp. 11-29, 2018.

[6] C. Wu, M. Li, L. Ye, X. Zou, and B. Qiang, "Malicious Website Detection Based on URLs Static Features," *Proceeding of International Conference on Modeling, Simulation and Optimization*, pp. 307-313, 2018.

[7] J. Puchyr and M. Holena, "Random-forest-based Analysis of URL Paths," *Proceeding of Conference on Information Technologies-applications and Theory*, pp. 129-135, 2017.

[8] G. Tan, P. Zhang, Q. Liu, X. Liu, C. Zhu, F. Dou, et al., "Adaptive Malicious URL Detection: Learning in the Presence of Concept Drifts," *Proceedings of 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering*, pp. 737-743, 2018.

[9] B.A. Tama and K.H. Rhee, "A Comparative Study of Phishing Websites Classification Based on Classifier Ensembles," *Journal of Korea Multimedia Society*, Vol. 21, No. 5, pp. 617-625, 2018.

[10] Y. Zeng, *Malicious URLs and Attachments Detection on Lexical-based Features using Machine Learning*, Master's Thesis of Victoria University of Engineering, 2018.

[11] S. Marchal, K. Saari, N. Singh, and N. Asokan, "Know Your Phish: Novel Techniques for Detecting Phishing Sites and Their Targets," *Proceeding of the 36th IEEE International Conference on Distributed Computing Systems*, pp. 323-333, 2016.

[12] Predict Malicious Websites: XGBoost (2018), https://www.kaggle.com/craerek/predict-malicious-websites-xgboost. (accessed May 14, 2018)

[13] H. Musa, D.A.Y. Gital, F.U. Zambuk, A. Umar, A.Y. Umar, J.U. Waziri, et al., "A Comparative Analysis of Phishing Website Detection Using XGBoost Algorithm," *Journal of Theoretical and Applied Information Technology*, Vol. 97,

No. 5, pp. 1434-1443, 2019.

[14] H.K. Pao, Y.L. Chou, and Y.J. Lee, "Malicious URL Detection Based on Kolmogorov Complexity Estimation," *Proceedings of the IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technology*, pp. 380-387, 2012.

[15] Y. Alshboul, R.K. Nepali, and Y. Wang, "Detecting Malicious Short URLs on Twitter," *Proceeding of the 21th Americas Conference on Information Systems*, pp. 1-7, 2015.

[16] ALEXA(2020), https://www.alexa.com/ (accessed March 19, 2020)

[17] OpenPhish(2020), https://openphish.com/ (accessed April 19, 2020)

[18] PhishTank(2020), https://phishtank.com/ (accessed April 19, 2020)

[19] H.S. Kim and I.S. Kim, "A Study on Characteristic Analysis and Countermeasure of Malicious Web Site," *Journal of The Korea Institute of Information Security and Cryptology*, Vol. 29, No. 1, pp. 93-103, 2019.

강 홍 구

2002년 건국대학교 컴퓨터공학과 졸업(학사)
2004년 건국대학교 컴퓨터공학과 졸업(석사)
2009년 건국대학교 컴퓨터공학과 졸업(박사)
2009년~2010년 건국대학교 컴퓨터공학과 강의교수
2010년~현재 한국인터넷진흥원 보안위협대응R&D팀 책임연구원
관심분야 : 인공지능, 웹 보안, 악성코드, CTI, 사이버범죄

신 삼 신

2006년 전남대학교 멀티미디어학과 졸업(학사)
2008년 전남대학교 일반대학원 정보보호협동과정 졸업(석사)
2008년~현재 한국인터넷진흥원 보안위협대응R&D팀 책임연구원
관심분야 : 머신러닝, 정보보호, 데이터사이언스

김 대 엽

2014년 인천대학교 컴퓨터공학과 졸업(학사)
2016년 과학기술연합대학원대학교 정보보호공학과 졸업(석사)
2016년~2019년 한컴시큐어 미래인증개발2팀 대리
2019년~현재 한국인터넷진흥원 보안위협대응R&D팀 주임연구원
관심분야 : 인공지능, 웹 보안, 모바일 보안, 인증기술

박 순 태

1992년 단국대학교 전자계산학과 졸업(학사)
1998년 국민대학교 정보과학대학원 정보통신학과 졸업(석사)
2010년 전남대학교 일반대학원 정보보안협동과정 졸업(박사)
1994년~1999년 육군 전산장교
2000년~현재 한국인터넷진흥원 보안위협대응R&D팀 팀장
관심분야 : 정보보호R&D, 정보보안/개인정보보호 실무, 침해사고 대응, 정보통신기반보호, 정보보호 인력양성, IT보안성 평가