Hindawi
Security and Communication Networks
Volume 2022, Article ID 3286623, 12 pages
https://doi.org/10.1155/2022/3286623

Research Article

Detecting Illegal Online Gambling (IOG) Services in the Mobile Environment

Moohong Min,[1] **Jemin J. Lee**,[2] **and Kyungho Lee**[3]

[1]*University College, Sungkyunkwan University, Seoul 03063, Republic of Korea*
[2]*Center for Information Security Technology, Korea University, Seoul 02841, Republic of Korea*
[3]*Department of Information Security, Korea University, Seoul 02841, Republic of Korea*

Correspondence should be addressed to Kyungho Lee; kevinlee@korea.ac.kr

Received 22 November 2021; Accepted 15 January 2022; Published 23 February 2022

Academic Editor: Ilsun You

Despite the extensive ramifications of illegal online gambling (IOG) services, actions taken by government authorities have had little effect in halting these operations. In order to reduce the prevalence of IOG, the ability to detect malicious uniform resource locators (URLs) is crucial. Text mining and binary classification have been widely adopted to detect and prevent spam short message services (SMSs), but government authorities and various task forces that monitor and regulate gambling also rely on the analysis of malicious URLs. This study proposes a novel system to analyse the characteristics of spam URLs, offering a method that can assist government agencies combatting mobile IOG sites.

1. Introduction

Despite the gambling market being one of the most regulated industries around the world, recent advancements in telecommunication technology have allowed illegal gambling to flourish online [1–3]. According to UNODC [4], 80% of sports and racing betting worldwide is illegally operated, with an estimated value of between 340 billion and 1.7 trillion USD. Most racing bets have wager limits, and past studies have focused on the effect of wagering limits on payouts and losses [5]. Moreover, harm-reduction strategies such as customer messaging have been considered by examining four Australian online sports and racing wagering sites [6]. Unlike authorized platforms, IOG sites do not impose limits on betting. Moreover, regulating these sites has become difficult as they must first be detected and then accurately identified.

Recent studies have found that gaming disorders have shown aetiological pathways into problematic gambling [7, 8], while gambling has been associated with the misuse of substances such as alcohol and nicotine in adolescents [9]. Internet gambling disorder is included in the diagnostic and statistical manual (DSM-5) for mental disorders, with detrimental ramifications for adolescents [10]. Common anxiety disorders such as social anxiety, depression, and loneliness have also been positively associated with gaming in adolescents [11]. The number of games introducing randomly-generated in-game rewards has increased throughout the past decade alongside the number of platforms such as mobile game markets, consoles, and PCs [12, 13]. Consequently, loot boxes, a virtual item that produces various rewards through a game of chance, have been banned in various nations such as the Netherlands and Belgium.

IOG sites rely on marketing to attract users, often using a "recommendation" system in which new members are invited by original members. However, as this method cannot bring in a large number of customers and illegal services cannot be advertised publicly, IOG sites also use smartphone applications to send out text messages. IOG organizers gather or purchase contact information to invite random users to their platforms. The Korea Internet and Security Agency (KISA) works with smartphone manufacturers and mobile communication companies to provide Android users with a reporting system through which people can report illegal spam messages sent over short message service (SMS) or multimedia messaging service (MMS). In South Korea,

approximately ten million spam SMSs are reported by KISA each year, and approximately 50% of these were confirmed to be related to illegal gambling. As some people are not aware of these reporting systems or fail to report spam SMSs, the actual number of messages is likely much larger. These messages severely affect the safety of the online environment and, therefore, must be researched so that they can be effectively blocked by relevant authorities. Although it may not be possible to obstruct all spam messages, authorities must still investigate their patterns, content, and features to develop technologies capable of, for example, extracting URLs. While authorities have already taken actions against many illegal gambling houses, illegal operators are willing to risk continuing due to record profits [14].

This study proposes a system based on artificial intelligence to sort illegal gambling messages from reported suspicious messages with a detection accuracy rate of 97%. Moreover, this study finds that illegal messages exhibit several patterns, including features that revise URLs to stop them from being filtered automatically. By reversing such patterns, the URL information can be reconstructed, and it will be easier for IOG websites to be automatically reported and taken down. As a result of our investigation, we suggest technologies to identify illegal gambling SMSs from reported spam and extract URL information from illegal gambling websites. We believe that this method represents a considerable contribution toward automating the process of classifying and blocking illegal sites, thus helping to keep our online environment safer. We further believe that our proposed methods can form the basis of new safeguards for government agencies, citizens, and the gambling industry against various illegal operations.

2. Background

The Council of Europe Convention on the Manipulation of Sports Competitions, better known as the "Macolin Convention," defines illegal gambling as "Any sports betting activity whose type or operator is not allowed under the applicable law of the jurisdiction where the consumer is located" [15]. This definition interprets illegal gambling widely, meaning that the same situation might be judged differently in different countries.

IOG websites mainly target people in countries where online gambling is illegal [16]. Broadly speaking, there are two types of IOG: (i) games and (ii) sports gambling. Online Live Casinos, Web Board Games, Internet reel games, and Power Ball are all illegal in South Korea, with some other illegal games such as ladder rides, snail games, and Mario probability games specifically targeting young people. In online sports gambling, users wage on the outcomes of sporting events, such as horse or cycling races. Examples of IOG are presented in Figure 1.

2.1. Issues with Illegal Gambling. Several key issues have arisen as more and more jurisdictions are allowing and controlling online gambling worldwide. These countries take steps to keep online gambling responsible, such as a dedicated budget for addiction centers and limits on betting amounts [17]. Illegal operators, however, encourage users to bet large amounts frequently and avoid paying taxes.

As illegal gambling is not subject to laws, users might not receive their winnings. In addition to financial fraud, illegal gambling causes several social problems [15]:

(i) Illegal gambling enables money laundering and organized transnational crime

(ii) Match fixing poses a challenge to the dignity of sports

(iii) Illegal gambling causes gambling disorders and related social problems

The disorders mentioned above can be observed in legal gambling but are more severe in illegal gambling (Table 1) [15]. Table 1 is reproduced from Asia Racing Federation 2018. In addition, there is concrete evidence worldwide that illegal gambling contributes to a higher incidence of problems than legal betting.

Illegal gamblers are more likely to be at-risk, moderate-risk, or problem gamblers and less likely to be nonproblem gamblers than those who gamble legally. As a result, problem gambling is more common among people who gamble illegally online, resulting in issues such as depression, alcohol and drug abuse, family breakup, debt, and suicide [18–21].

In general, illegal gamblers are able to bet larger amounts of wagers than legal gamblers. At the minimum, the lack of any limitations on gambling activity in illegal environments can spur and worsen the issues of excessive gamblers. Hence, it is necessary to identify IOG websites and block them for social good.

2.2. Comparison of Illegal Gambling across Different Nations. As shown in Table 2, illegal gambling is prevalent, especially in Asia [15]. Table 2 is reproduced from Asia Racing Federation 2018. South Korea constitutes more than 60% of illegal gambling in the world.

2.3. Negative Effects of Illegal Gambling on the Adolescents. Owing to behavioral and emotional immaturities, children are vulnerable to gambling issues through social pressure and advertisements [22]. In several high-income nations, the increased availability of legal gambling has led to an increase in underage gambling and gambling disorders in young people [23].

The increase in the number of online video games with probability-based items has reduced the resistance of many adolescents to gambling since 2000. New levels of exposure to illicit gambling sites have created an environment where teenagers, who spend a considerable amount of time on the Internet, are easily influenced. Although teenage gambling is illegal in most countries, the incidence of problem gambling in adolescents is higher than that seen in adults [24].

2.4. Process for Blocking Illegal Online Gambling Sites. The Korea Racing Authority (KRA), the sole racing authority in Korea, investigates IOG operations alongside other

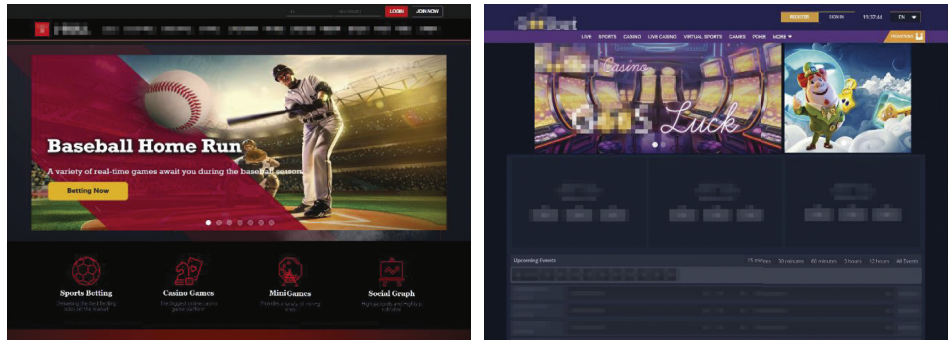

Figure 1: Websites of illegal online gambling.

Table 1: Legal gamblers versus illegal gamblers.

Jurisdiction	Nonproblem gamblers (%)		At-risk, moderate-risk, or problem gamblers (%)	
	Legal gambler	Illegal gambler	Legal gambler	Illegal gambler
Australia [18]	40.3	21.5	59.7	78.5
New Zealand [19]	76.8	68.8	23.2	31.2
Hongkong [20]	62	28	39	73

Table 2: Illegal betting industry margins across six jurisdictions in 2015–2017.

Country	Year	Illegal betting margin (USD million)	Illegal betting margin of the total market (%)
Australia	2015	780	6
New Zealand	2017	32	21
Singapore	2015	336	37
South Africa	2016	14	48
South Korea	2016	1,448	62
Hong Kong	2016	1,610	36
Total		4,220	

government agencies such as the National Gambling Control Committee (NGCC), a national organization that oversees gambling-related public institutions, and the Korea Communication Standard Commission (KCSC), a public institution that screens various illegal websites such as gambling, pornography, and financial fraud. Reporting an IOG site requires evidence such as an URL address or screenshots of the IOG sites. These pieces of evidence are collected from the KRA and NGCC, which are then transferred to the KCSC, who reviews the sites and then notifies Internet Service Providers. The KCSC requires a three-week window to verify these flagged sites. Illegal sites are the most common evidence that the government can use against perpetrators in subsequent legal action.

The process of blocking IOG sites is as follows:

Step #1: crawling URLs associated with IOG

Step #2: collecting suspicious URLs and any supporting evidence

Step #3: submitting URLs and evidence to KCSC

Step #4: KCSC review to verify designation

Step #5: URLs verified to be illegal forwarded to the ISP

Step #6: URLs blocked by ISP

The essential part of the first step is collecting a list of suspicious URLs by sorting through reported sites. The list serves as evidence for cybercrime and allows the KCSC to address criminal activities. These organizations have been collecting IOG data for a considerable period, but there is still difficulty finding the sites automatically through Google and SNS platforms. Hence, the data must be collected manually which is extremely time consuming and allows IOG operators to effectively circumvent enforcement by continuously closing and reopening sites with new URLs. As a result, enabling timely prosecution is now a vital focus for researchers. In this study, we attempt to offer a faster solution.

2.5. Defining the Spam SMS. Spam is defined as any unwanted message sent to a user for commercial gain or simply to cause detriment or discomfort [25]. Another definition of "spam" is promotional information that has been provided without the agreement of recipients from an official KISA website. Spam SMSs include messages that are sent to mobile phones for advertisement purposes, which can range from legal but nonessential information to severely illegal content

[26]. These regulatory definitions fall under the purview of criminal law in South Korea, and offenders thus face fines and imprisonment.

Based on these definitions, the SMS activities below are considered illegal in South Korea:

(i) Advertisement without agreement from the recipient

(ii) Advertisement between 21:00 and 08:00

(iii) Advertisement that does not clearly identify itself as an "advertisement"

(iv) Advertisement for illegal goods or services

2.6. Spam SMS about Illegal Online Gambling. Spam messages containing the term "gamble" are illegal in South Korea, where all accredited legal gambling is operated by the government, but they remain a common tool for IOG platforms. In these messages, the URL is modified to avoid filters, as shown in Table 3.

IOG spam exhibits the following features:

(i) URLs are presented in an abnormal form to avoid smartphone and application filters

(ii) URLs are easily legible to people but not to detection systems

(iii) Messages employ terminology that obscures the illegality of the advertised service

To extract URLs, it is necessary to understand several conversion conditions used with the messages.

2.7. Related Work. Data mining approaches such as supervised classification have been employed to detect spam or illegal content in the past [27]. Cascading Style Sheets (CSS) are often used to detect specific page layouts, and prior studies have used SVM techniques and map-reduce algorithms to detect spam emails [28]. Akbari and Sajedi [29] introduced GentleBoost, an algorithm for SMS spam detection, that achieves high accuracy with minimum storage consumption.

Recent studies that detect spam include CNN-based filtering with deep learning [30–32]. Spam filtering based on sentimental analysis using SentiWordNet has also been proposed [33]. Various other spam filtering methods are discussed in academic literature, such as similarity-based corpus and Wikipedia link-based spam filtering [34].

Various machine learning models have also been utilized to detect and classify malicious URLs [35]. Yan et al. [36] proposed an unsupervised learning algorithm that trains URL embedding models, an approach that far exceeded the performance of other algorithms such as SVM, DT, LR, NB, and CNN. The accuracy of deep learning methods was far higher than conventional machine learning methods when utilizing binary classification to filter spam messages [37].

Liu et al. studied "spear phishing" (targeted phishing efforts) and promotional SMS from a security point of view [38]. And our own previous study on illegal gambling utilized a readable transformation technique (RTT) [39].

Table 3: Examples of modified URLs found in spam SMSs.

No.	URL representation
1	p m a 33. c σ m
2	tⓚtⓚ889.com
3	⑥8㎸g ~ com
4	uda47.c▣m
5	WAR23.N/E/T
6	bv876.cI▷m
7	②⑥㎸⑨.me
8	dsa-1004.c-Ω_M
9	⑤④kmg"COm^2
10	pⓡoⓒt-⑦469.com

3. Research Design and Methods

We propose a system for classifying messages based on the characteristics identified earlier and then extracting and converting IOG URLs. In order to identify the ideal NLP approach, this study uses real data from spam messages to test binary classification algorithms.

Several studies have classified spam SMSs using machine learning. Nagwani and Sharaff proposed the use of ML algorithms such as Naïve Bayes (NB), support vector machine (SVM), non-negative matrix factorization, and latent Dirichlet allocation to identify spam [40], while Almeida et al. suggested text normalization [41]. Fattahi and Mejri applied natural language processing (NLP) techniques, namely, Bag of Words (BoW) and Term Frequency-Inverse Document Frequency (TF-IDF) to identify spam SMSs [42]. Choudhary and Jain applied random forest (RF) classification algorithms [43]. Sethi et al. compared NM, RF, and logistic regression (LR) algorithms [44].

NLP aids in the detection, extraction, and interpretation of particular information from text, which is often used in web search engines, for example, Apple's Siri and Google Translate. For NLP in English text, our study employs the natural language toolkit documentation. In this study, we referred to KoNLPy, an open-source library designed for Korean language text mining. There are five NLPs in KoNLPy: okt, mecab, komoran, kkma, and hannanum.

Examples of the okt options are presented as follows:

(i) okt.morphs() splits text based on the morpheme

(ii) okt.nouns() extracts nouns from the text

(iii) okt.phrases() extracts word segments

Other NLPs have similar options.

The next step is a feature vectorizer. Typical examples of vectorizers include the following:

(i) CountVectorizer: a vectorizer that counts the number of words in each text

(ii) TfidfVectorizer: a vectorizer that uses the "TF-IDF" tune scale of frequencies by counting words in each text to focus on meaningful spam messages

(iii) HashingVectorizer: a vectorizer that uses a hash function to increase the processing speed of the CountVectorizer

As these have been designed for the Korean language, different NLP and feature extractors would be needed to classify spam messages in other languages.

This study obtained data from KISA, including suspected spam SMSs reported by smartphone users from 2020 and legal SMSs, such as nonbeneficial public advertisements. SMSs contain 160 or fewer characters. After removing duplicates, 30,527 unique messages were tested. Messages with slight differences, such as one letter or number, were included. This study labeled gambling-related messages (14,334 messages) as "Class 1" and nongambling-related messages (16,193 messages) as "Class 2."

This study began with preprocessing, which deleted words and phrases that commonly appear at the beginning of Korean messages, such as "sent from web" or "advertisement." The experiments were then designed to have three parts.

3.1. Deciding Parameter of Vectorizers. This study used three vectorizers (TfidfVectorizer, CountVectorizer, and HashingVectorizer). A criterion algorithm was set, and the parameters for each vectorizer were determined. Then, the performances of the vectorizers were compared.

3.2. Deciding KoNLPy and Matching Options. To determine KoNLPy and its options for the experiment, representative KoNLPs such as okt, mecab, hannanum, and kkma, as well as the RF algorithm with each option, were chosen for this study. From the next experiment, okt and mecab were used to consider their performance and speed.

3.3. ML Algorithm, KoNLPy, and Matching Options. All ML algorithms were selected using a hyperparameter tuning process. This study used the GridSearchCV function. The range of this function used the numbers found in this study's pilot test. "Training set" and "Test set" were randomly chosen based on a 3:1 ratio, and classes were set at this rate. Cross validation was performed four times.

4. Proposed Detection System

We propose two automatic detection systems to identify IOG websites using spam SMS, as shown in Figure 2.

Vectorizers for NLP and feature extraction are selected and configured depending on the language. The algorithm then produces optimized modeling with hyperparameter tuning. After applying samples of spam to the model, SMSs can be classified and extracted. The proposed system applies the option of morphs to mecab KoNLPy and the SVM algorithm, which was chosen for this study.

As described in Section 2.6, classified illegal gambling messages exhibit repeated patterns in the ways that they obscure URLs. The extraction and conversion process can be seen as a recovery operation that creates an accessible form of each URL. This study used more than 250 conversion rules to interpret the characters; detailed examples have been provided in the Appendix. As conversion rules can differ based on the language and legal requirements of the country, further collection and analysis are required.

The resulting URL is tested through an alive check process to confirm if it is active. If the alive check is positive, the URL is an IOG website, and screen capture functions can be used to report it.

5. Experiments

5.1. Parameters of the Vectorizer. To filter spam SMSs, this study used the RF algorithm [16] as a criterion, which was also used in previous studies. Each parameter was determined through experiments. Random forest, an ensemble learning method for classification and regression, works by training a large number of decision trees. For classification tasks, the random forest's output is the class chosen by the majority of trees. The mean or average prediction of the individual trees is returned for regression tasks [45, 46].

Each parameter was manually increased (ngram_range and min_df were adjusted in units of 1, and max_df was adjusted in units of 0.1), and a parameter representing the best performance was selected.

The parameters that exhibit the best performance are as follows:

(i) TfidfVectorizer: ngram_range = (1, 4), min_df = 3, max_df = 0.9

(ii) CountVectorizer: ngram_range = (1, 2), min_df = 3, max_df = 0.9

(iii) HashingVectorizer: ngram_range = (1, 2)

Each parameter was determined through experiments, and the process for manual determination has not been mentioned here. The outcomes of vectorizers based on the RF algorithm are listed in Table 4.

The F1-score is made up of two components: precision and recall. The F1-score's purpose is to combine the precision and recall measurements into a single number, and it was created to work well with the unbalanced data. Looking at the results of F1-score and accuracy, it is clear that count vectorizer performs best among the vectorizers based on the current best performance parameter.

5.2. Deciding KoNLPy and the Matching Options. Ten combinations of representative KoNLPy (okt, mecab, hannanum, and kkma) and each option (morphs, nouns, and phrases) were used for tests in this study (Table 5).

The loading and execution time for 100K characters, drawn from the official website of KoNLPy, are shown in Table 6.

The okt, kkma, and mecab KoNLPy exhibited excellent accuracy, but kkma was very slow as indicated in Table 6. As a result, this paper performed experiments using okt and mecab.

5.3. ML Algorithm, KoNLPy, and the Matching Options. The experiments presented in Sections 5.1 and 5.2 were processed using the RF algorithm, whereas the following

```
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.feature_extraction.text import HashingVectorizer
class classifier:
  ...
  def vectorize(self, opt3):
    ...
    self.vectorizers = [TfidfVectorizer(tokenizer = self.tokenize,
        stop_words = self.stop_words, ngram_range = (1,4), min_df = 3, max_df = 0.9), CountVectorizer(tokenizer = self.tokenize,
stop_words = self.stop_words, ngram_range = (1,2), min_df = 3, max_df = 0.9), HashingVectorizer(tokenizer = self.tokenize,
stop_words = self.stop_words, ngram_range = (1,2))]
```

Algorithm 1: Deciding parameter of vectorizers.

```
import konlpy.tag as kn
class classifier:
  ...
  okt = kn.Okt()
  mecab = kn.Mecab(dicpath = "PATH")
  tokenizers = [okt.morphs, okt.nouns, okt.phrases, mecab.morphs, mecab.nouns, None].
```

Algorithm 2: Deciding KoNLPy and matching options.

```
from sklearn.model_selection import GridSearchCV
from sklearn.model_selection import train_test_split
class classifier:
  ...
  def adapt(self, opt1, opt2, opt3, grid = True):
    ...
    self.grid_cv = GridSearchCV(self.clf, self.param_grid, cv = 4, scoring = "accuracy," verbose = 2, n_jobs = −1).
    ...
  def get_data(self):
    ...
    self.train_x, self.test_x, self.train_y, self.test_y = train_test_split(self.original_data.text.tolist(), self.original_data.score.tolist(),
test_size = 0.25, shuffle = True, stratify = self.original_data.score.tolist(), random_state = 0).
```

Algorithm 3: ML algorithm, KoNLPy, and matching options.

experiment was processed with five combinations of the three vectorizers (TfidfVectorizer, CountVectorizer, and HashingVectorizer), KoNLPy, and the options that were decided in advance. Four ML algorithms (linearSVM, rbpSVM, LR, and RF) were then added to the experiment. The main objective of the SVM algorithm is to find a line or side that separates data of different classes with the largest margin. As such, the algorithm finds the optimal linear decision boundary or hyperplane that linearly separates data. The kernel SVM technique is a method of mapping and classifying data that might otherwise be difficult to distinguish linearly into high-dimensional features. rbfSVM is known to perform well as one of the types of kernels.

Linear regression is a traditional statistical model. By fitting a linear equation to observed data, linear regression seeks to model the relationship between two variables. RandomForest is described in section 5.1 as an ensemble learning algorithm. Overall, 60 cases ($3 \times 4 \times 5$) were tested.

The combinations of KoNLPy and matching options are listed in Table 7.

The outcomes of the study with four algorithms, including the RF, are given as follows.

The results from the TfidfVectorizer are depicted in Figure 3. The x-axis consists of the various algorithms and vectorizers, and the y-axis exhibits accuracy.

The top three combinations were as follows:

(i) linearSVM and okt.morphs: 97.99% accuracy

(ii) mecab.morphs and rbpSVM: 97.95% accuracy

(iii) logistic regression and okt.morphs: 97.92% accuracy

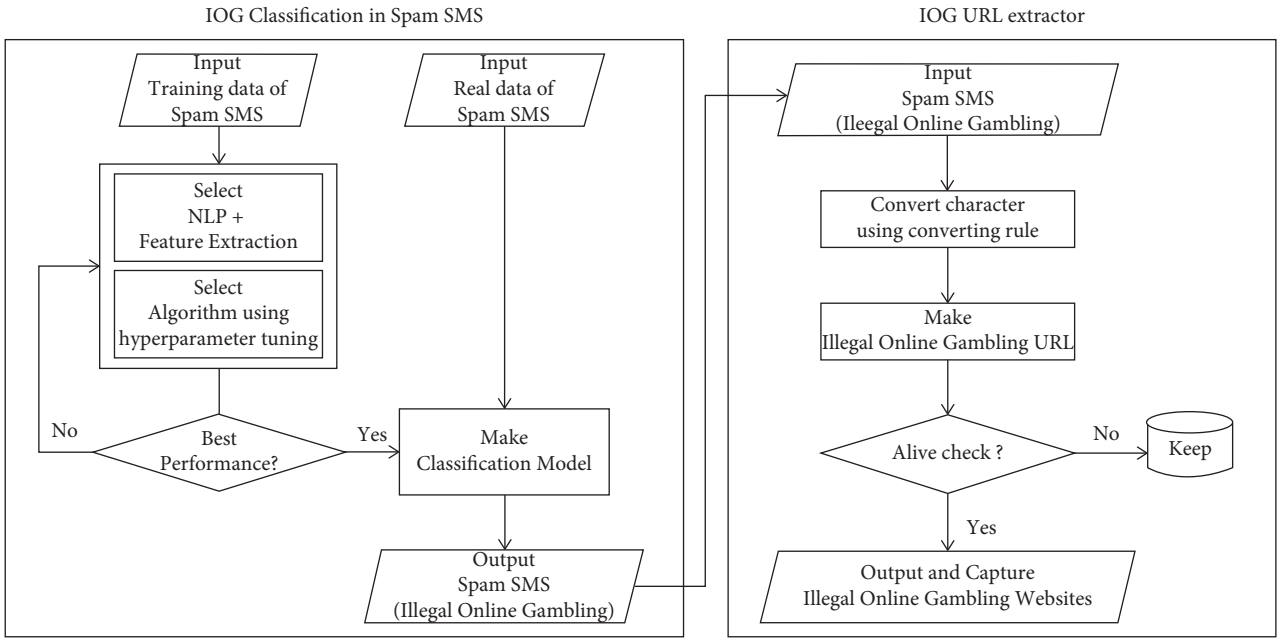

Figure 2: Detection system for IOG websites.

Table 4: Outcomes of the vectorizers.

No.	Vectorizer	Class	Precision	Recall	F1-score	Accuracy
1	TfidfVectorizer	1	0.9784	0.7998	0.8802	0.9031
		2	0.8600	0.9859	0.9186	
2	CountVectorizer	1	0.8694	0.9533	0.9094	0.9155
		2	0.9594	0.8852	0.9208	
3	HashingVectorizer	1	0.9841	0.6011	0.7464	0.8182
		2	0.7562	0.9922	0.8583	

Table 5: Result of KoNLPy and the matching options.

No.	KoNLPy.Option	Time (s)	Class	Precision	Recall	F1-score	Accuracy
1	okt.morphs	3386.639	1	0.9118	0.9483	0.9297	0.9362
			2	0.9571	0.9265	0.9416	
2	okt.nouns	2486.764	1	0.9673	0.5835	0.7279	0.8059
			2	0.7466	0.9842	0.8491	
3	okt.phrases	3117.513	1	0.9153	0.9471	0.9309	0.9375
			2	0.9564	0.9298	0.9429	
4	mecab.morphs	1482.722	1	0.9245	0.9462	0.9352	0.9417
			2	0.9560	0.9380	0.9469	
5	mecab.nouns	957.6458	1	0.9749	0.5703	0.7196	0.8022
			2	0.7415	0.9882	0.8472	
6	hannanum.morphs	2738.434	1	0.4413	0.4782	0.4590	0.4984
			2	0.5515	0.5145	0.5324	
7	hannanum.nouns	2960.964	1	0.4707	0.2578	0.3331	0.5407
			2	0.5633	0.7676	0.6498	
8	kkma.morphs	8756.802	1	0.9651	0.8948	0.9286	0.9388
			2	0.9203	0.9741	0.9464	
9	kkma.nouns	8280.039	1	0.9840	0.8131	0.8904	0.9109
			2	0.8684	0.9894	0.9250	
10	kkma.sentences	9004.297	1	0.9717	0.8877	0.9278	0.9385
			2	0.9158	0.9793	0.9465	

Table 6: Time result of KoNLPy and the matching options.

KoNLPy	Loading time (s)	Execution time (s)
kkma	5.6988	35.7163
komoran	5.4866	25.6008
hannanum	0.6591	8.8251
okt	1.4870	2.4714
mecab	0.0007	0.2838

Table 7: Time result of KoNLPy and the matching options.

No.	KoNLPy	Options
1	okt	Morphs Nouns Phrases
2	mecab	Morphs Nouns

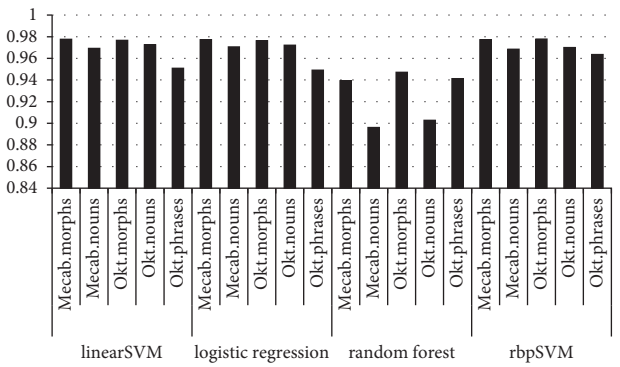

Figure 3: Accuracy results for the TfidfVectorizer.

With TfidfVectorizer, it is apparent that the overall performance of the random forest algorithm is lower than that of the other three algorithms.

The accuracy results of the CountVectorizer are illustrated in Figure 4. The top three results are as follows:

(i) okt.morphs and rbpSVM: 97.78% accuracy

(ii) mecab.morphs and linearSVM: 97.75% accuracy

(iii) mecab.morphs and rbpSVM: 97.72% accuracy

Even with CountVectorizer, it is apparent that the random forest algorithm has a lower overall performance than the other three algorithms.

The accuracy results of the HashingVectorizer are shown in Figure 5. The top three algorithms with the top accuracy are listed as follows:

(i) mecab.morphs and rbpSVM: 97.96% accuracy

(ii) mecab.morphs and linearSVM: 97.91% accuracy

(iii) logistic regression and mecab.morphs: 97.89% accuracy

Among the 60 experimental outcomes, the case where the okt.morphs KoNLPy of linearSVM was applied to TfidfVectorizer yielded the best performance. Several algorithms tested in this study classified more illegal gambling SMSs than the RF algorithm.

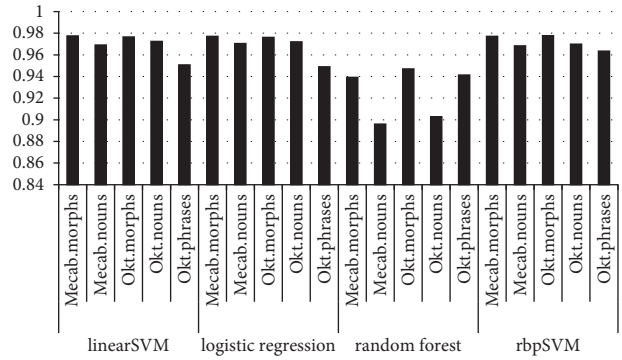

Figure 4: Accuracy results for CountVectorizer.

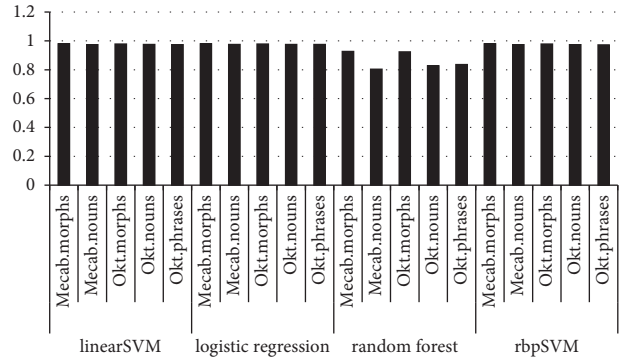

Figure 5: Accuracy results for HashingVectorizer.

The proposed detection system selects an optimized model by continuously comparing performances to discover the best vectorizer that works with NLP and matching options. The process of finding optimized parameters for vectorizers and algorithms requires considerable time, as shown in Table 8.

Therefore, the speed of the process, the purpose of the vectorizers, and the matching options selected should be considered when choosing between models.

5.4. Performance Comparison of the Algorithms. The purpose of the experiment in this section is to comprehensively examine each algorithm and the KoNLPy and option (tokenizer) matching them. This experiment can be seen as an extension of the experiment in Section 5.3 and was conducted based on Tfidf's vector, which showed the highest performance on an accuracy basis.

The experiment in this section was conducted with a total of seven algorithms. MLP and boosting algorithms

Table 8: Results for the best vectorizers.

Vectorizer	Algorithm	KoNLPy.Option	Accuracy (%)	Time (s)
Tfidf	linearSVM	okt.morphs	97.99	652.27
Tfidf	SVM	mecab.morphs	97.95	5864.59
Tfidf	LR	okt.morphs	97.92	869.072
Count	SVM	okt.morphs	97.78	1766.73
Count	linearSVM	mecab.morphs	97.75	128.868
Count	SVM	mecab.morphs	97.72	380.958
Hashing	SVM	mecab.morphs	97.96	1528.25
Hashing	linearSVM	mecab.morphs	97.91	107.227
Hashing	LR	mecab.morphs	97.89	97.8956

Table 9: Results for comprehensive experiments.

Algorithm	KoNLPy.Option	Accuracy	Precision	Recall	F1-score
linearSVM	Okt.morphs	0.9788	0.9781	0.9791	0.9786
	Okt.nouns	0.9759	0.9753	0.9760	0.9757
	Okt.phrases	0.9784	0.9776	0.9788	0.9782
	Mecab.morphs	0.9795	0.9791	0.9794	0.9792
	Mecab.nouns	0.9757	0.9750	0.9759	0.9754
LR	Okt.morphs	0.9766	0.9756	0.9772	0.9763
	Okt.nouns	0.9742	0.9736	0.9743	0.9739
	Okt.phrases	0.9776	0.9768	0.9780	0.9774
	Mecab.morphs	0.9780	0.9777	0.9778	0.9778
	Mecab.nouns	0.9761	0.9754	0.9762	0.9758
NB	Okt.morphs	0.9750	0.9747	0.9747	0.9747
	Okt.nouns	0.9699	0.9695	0.9695	0.9695
	Okt.phrases	0.9712	0.9714	0.9703	0.9708
	Mecab.morphs	0.9745	0.9746	0.9738	0.9742
	Mecab.nouns	0.9725	0.9720	0.9724	0.9722
RF	Okt.morphs	0.9376	0.9361	0.9407	0.9373
	Okt.nouns	0.9551	0.9535	0.9568	0.9548
	Okt.phrases	0.9278	0.9262	0.9305	0.9274
	Mecab.morphs	0.9520	0.9503	0.9544	0.9517
	Mecab.nouns	0.9617	0.9602	0.9628	0.9613
SVM	Okt.morphs	0.9787	0.9781	0.9788	0.9784
	Okt.nouns	0.9779	0.9773	0.9780	0.9776
	Okt.phrases	0.9775	0.9771	0.9774	0.9772
	Mecab.morphs	0.9785	0.9785	0.9781	0.9783
	Mecab.nouns	0.9767	0.9763	0.9765	0.9764
MLP	Okt.morphs	0.9753	0.9749	0.9751	0.9750
	Okt.nouns	0.9744	0.9737	0.9745	0.9741
	Okt.phrases	0.9738	0.9727	0.9746	0.9736
	Mecab.morphs	0.9753	0.9752	0.9747	0.9750
	Mecab.nouns	0.9720	0.9713	0.9721	0.9717
Boosting (AdaBoost)	Okt.morphs	0.9640	0.9637	0.9635	0.9636
	Okt.nouns	0.9729	0.9723	0.9730	0.9726
	Okt.phrases	0.9687	0.9681	0.9686	0.9684
	Mecab.morphs	0.9686	0.9684	0.9680	0.9682
	Mecab.nouns	0.9716	0.9711	0.9715	0.9713

The F1-score metric was determined by calculating recall and precision as well as accuracy. This is the result of using the metrics.classification_report function of sklearn.

were added. MLP was added for the purpose of applying neural networks, and MLP classifiers were utilized. Boosting algorithms are machine learning ensemble techniques that combine several sequential weak learners to improve prediction or classification performance. The algorithm applied in this experiment is AdaBoost. A total of five KoNLPy and option combinations (Okt.morphs, Okt.nouns, Okt.phrases, Mecab.morphs, and Mecab.nouns) were used.

The GridSearchCV() function was utilized to find the optimal parameters. In sklearn, the GridSearchCV function allows us to identify the best parameters by sequentially inputting hyperparameters used in classification or

regression algorithms to be learned and measured. The option used was cv (cross validation) four times, and scoring was set to accuracy.

As shown in Table 9, there is no KoNLPy/Option (tokenizer) combination with algorithms that clearly demonstrates outstanding performance as a result of the experiment. However, the F1-score indicates that each algorithm has a tokenizer that produces good performance. Generally speaking, the tokenizer of Okt.morphs and Mecab.morphs performs well. However, Mecab.nouns performs best in RF, and Okt.nouns performs best in AdaBoost. Therefore, it is important to select algorithms and KoNLPy.Options that achieve optimal speed as a part of the detection system we propose in the next study.

6. Conclusion

This study developed technologies to extract URL information and automatically classify messages reported as spam. While spam messages have many attributes that make them readily identifiable to human recipients, it has been difficult to rapidly detect gambling-related messages amongst other spam.

First, this study classified 30,527 messages collected by the KISA from 2020 into gambling- and nongambling-related groups for experiments. Then, NLP was used to extract features, and various ML algorithms and hyperparameter tuning (GridSearch) were used to find optimized parameters. To solve the paper's initial problem, this study finally proposed a novel extraction model that yielded 97% accuracy, which implies that the detection technology could provide even higher accuracy when analyzing a mixture of spam and normal messages in real-world conditions.

The proposed technologies can replace current methodologies, which are typically dependent on manual reporting, to quickly and precisely classify approximately 27,000 spam messages that are sent to KISA each day. In particular, the system proposed in this paper can provide a URL pool to quickly block illegal gambling sites based on compiled spam SMS activities. Moreover, our study was able to effectively reduce the time required to detect and block IOG sites, which is the key to stopping operators who evade enforcement by changing their URLs frequently.

This work provides a cornerstone for future researchers interested in detecting illegal gambling and other problematic content that employs spam mass marketing. In the future, we plan to identify optimal parameters (such as the number of hidden layers) centered on DNN and continue research on methods to improve performance. The results of these experiments are limited to text-based data, so further investigation is needed for image-based spam messages.

The proposals presented here may be adopted by ISPs, government agencies, or licensed racing regulators in any country. While this study targeted illegal gambling, the proposed technologies can also be applied to any other field that detects illegal content, such as adult content or illegal loans.

Appendix

Example of URL Character Converting Rule

Step #1

```
a = a.replace('\", ")
a = a.replace('\"", ")
 a = a.replace('(', ").replace(')', ")
 a = a.replace("⑴,""1").replace("⑵,"
"2").replace("⑶,""3").replace("⑷," "4").replace("⑸,"
"5")
 a = a.replace("⑹,""6").replace("⑺,"
"7").replace("⑻,""8").replace("⑼," "9").replace("⑽,"
"10")
 a = a.replace("ⓐ,""a").replace("ⓑ,"
"b").replace("ⓒ,""c").replace("ⓓ," "d").replace("ⓔ,"
"e")
 a = a.replace("ⓕ,""f").replace("ⓖ,"
"g").replace("ⓗ," "h").replace("ⓘ," "i").replace("ⓙ,"
"j")
 a = a.replace("ⓚ,""k").replace("ⓛ,"
"i").replace("ⓜ,""m").replace("ⓝ,"
"n").replace("ⓞ," "o")
 a = a.replace("ⓟ,""p").replace("ⓠ,"
"q").replace("ⓡ," "r").replace("ⓢ," "s").replace("ⓣ,"
"t")
 a = a.replace("ⓤ,""u").replace("ⓥ,"
"v").replace("ⓦ,""w").replace("ⓧ,"
"x").replace("ⓨ," "y")
 a = a.replace("ⓩ," "z").replace("—," "-")
 a = a.replace("sv,""sv").replace("㏄,"
"cc").replace("㎚,""nm").replace("㎛,"
"um").replace("㎜," "mm")
```

Step #2

```
if "co_m" in a: a = a.replace("co_m," "com")
if "c_o_m" in a: a = a.replace("c_o_m," "com")
if "c_om" in a: a = a.replace("c_om," "com")
if "com" in a: a = a.replace("com," "com")
if "COm" in a: a = a.replace("COm," "com")
if "c-o`m" in a: a = a.replace("c-o`m,""com")
if "c`om" in a: a = a.replace("c`om,""com")
if "co`m" in a: a = a.replace("co`m,""com")
if "c`o`m" in a: a = a.replace("c`o`m,""com")
if "c`Ω`m" in a: a = a.replace("c`Ω`m,""com")
if "c0㎡" in a: a = a.replace("c0㎡,""com")
if "c`Ωm" in a: a = a.replace("c`Ωm,""com")
```

Data Availability

The spam SMS data used to support the findings of this study have not been made available because of the MOU signed between the agencies.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this study.

Acknowledgments

This research was funded by the Agency for Defense Development (Grant no. UD190016ED).

References

[1] A. McCormack and M. D. Griffiths, "Motivating and inhibiting factors in online gambling behaviour: a grounded theory study," *International Journal of Mental Health and Addiction*, vol. 10, no. 1, pp. 39–53, 2012.

[2] A. Sirola, M. Kaakinen, and A. Oksanen, "Excessive gambling and online gambling communities," *Journal of Gambling Studies*, vol. 34, no. 4, pp. 1313–1325, 2018.

[3] M. Chóliz, "The challenge of online gambling: the effect of legalization on the increase in online gambling addiction," *Journal of Gambling Studies*, vol. 32, no. 2, pp. 749–756, 2016.

[4] "United Nations Office on Drugs and Crime (UNODC)," *Global Report on Corruption in Sport (Illegal betting and sport), SECTION 9*, 2021, https://www.unodc.org/res/safeguardingsport/grcs/section-9_html/SPORTS_CORRUPTION_2021_S9.pdf.

[5] M. Levinson, "A sure bet: why New Jersey would benefit from legalized sports wagering," *The Sports Lawyers Journal*, vol. 13, p. 143, 2006.

[6] R. M. Heirene and S. M. Gainsbury, "Encouraging and evaluating limit-setting among on-line gamblers: a naturalistic randomized controlled trial," *Addiction*, vol. 116, 2021.

[7] D. Columb, M. D. Griffiths, and C. O'Gara, "Online gaming and gaming disorder: more than just a trivial pursuit," *Irish Journal of Psychological Medicine*, pp. 1–7, 2019.

[8] A. Torres-Rodríguez, M. D. Griffiths, X. Carbonell, and U. Oberst, "Internet gaming disorder in adolescence: psychological characteristics of a clinical sample," *Journal of Behavioral Addictions*, vol. 7, no. 3, pp. 707–718, 2018.

[9] A. J. Van Rooij, D. J. Kuss, M. D. Griffiths, G. W. Shorter, T. M. Schoenmakers, and D. Van De Mheen, "The (co-)occurrence of problematic video gaming, substance use, and psychosocial problems in adolescents," *Journal of behavioral addictions*, vol. 3, no. 3, pp. 157–165, 2014.

[10] N. M. Petry, F. Rehbein, D. A. Gentile et al., "An international consensus for assessing internet gaming disorder using the new DSM-5 approach," *Addiction*, vol. 109, no. 9, pp. 1399–1406, 2014.

[11] J.-L. Wang, J.-R. Sheng, and H.-Z. Wang, "The association between mobile game addiction and depression, social anxiety, and loneliness," *Frontiers in Public Health*, vol. 7, p. 247, 2019.

[12] W. Li, D. Mills, and L. Nower, "The relationship of loot box purchases to problem video gaming and problem gambling," *Addictive Behaviors*, vol. 97, pp. 27–34, 2019.

[13] G. A. Brooks and L. Clark, "Associations between loot box use, problematic gaming and gambling, and gambling-related cognitions," *Addictive Behaviors*, vol. 96, pp. 26–34, 2019.

[14] T. Spapens, "Regulating ILL egal gambling markets: the case of illegal Casinos in The Netherlands," in *Crime, Addiction and the Regulation of Gambling*, pp. 93–107, Brill Nijhoff, Leiden, Netherlands, 2008.

[15] A. Racing Federation, *Illegal Betting in an Asian Context*, White Paper, Chennai, India, 2018.

[16] H. Yang, K. Du, Y. Zhang et al., "Casino royale: a deep exploration of illegal online gambling," in *Proceedings of the 35th Annual Computer Security Applications Conference*, pp. 500–513, San Juan, PR, USA, December 2019.

[17] A. Blaszczynski, R. Ladouceur, and H. J. Shaffer, "A science-based framework for responsible gambling: the Reno model," *Journal of Gambling Studies*, vol. 20, no. 3, pp. 301–317, 2004.

[18] E. Langham, A. M. T. Russell, N. Hing, and S. M. Gainsbury, "Sense of coherence and gambling: exploring the relationship between sense of coherence, gambling behaviour and gambling-related harm," *Journal of Gambling Studies*, vol. 33, no. 2, pp. 661–684, 2017.

[19] M. Bellringer, M. Garrett, K. Kolandai-Matchett, and M. W. Abbott, *Offshore Gambling by New Zealanders Study*, Gambling & Addictions Research Centre, Final report, 2015.

[20] A. Tessler, K. El Beyrouty, and N. Crapnell, "An exploratory study of illegal gamblers in Hong Kong," *Asian journal of gambling issues and public health*, vol. 7, no. 1, pp. 9–16, 2017.

[21] A. I. B. T. F. A. R. Federation, *Good Practices in Addressing Illegal Betting: A Handbook for Horse Racing and Other Sports to Uphold Integrity*, Handbook, 2021, https://play.google.com/books/reader?id=tYcSEAAAQBAJ&pg=GBS.PP1&hl=ko&printsec=frontcover.

[22] A. M. Emond and M. D. Griffiths, "Gambling in children and adolescents," *British Medical Bulletin*, vol. 136, no. 1, pp. 21–29, 2020.

[23] R. A. Volberg, R. Gupta, M. D. Griffiths, D. T. Ólason, and P. Delfabbro, "An international perspective on youth gambling prevalence studies," *Youth Gambling*, vol. 22, pp. 21–56, 2011.

[24] F. Calado and M. D. Griffiths, "Problem gambling worldwide: an update and systematic review of empirical research (2000-2015)," *Journal of behavioral addictions*, vol. 5, no. 4, pp. 592–613, 2016.

[25] S. A. Saab, N. Mitri, and M. Awad, "Ham or spam? A comparative study for some content-based classification algorithms for email filtering," in *Proceedings of the MELECON 2014-2014 17th IEEE Mediterranean Electrotechnical Conference*, pp. 339–343, IEEE, Beirut, Lebanon, April 2014.

[26] South Korea, "Act on promotion of information and communications network utilization and information protection," 2001, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG.

[27] S. B. Rathod and T. M. Pattewar, "A comparative performance evaluation of content based spam and malicious URL detection in E-mail," in *Proceedings of the 2015 IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS)*, pp. 49–54, IEEE, Bhubaneshwar, India, November 2015.

[28] P. Patil, R. Rane, and M. Bhalekar, "Detecting spam and phishing mails using SVM and obfuscation URL detection algorithm," in *Proceedings of the 2017 International Conference on Inventive Systems and Control (ICISC)*, pp. 1–4, IEEE, Coimbatore, India, January 2017.

[29] F. Akbari and H. Sajedi, "SMS spam detection using selected text features and boosting classifiers," in *Proceedings of the 2015 7th Conference on Information and Knowledge Technology (IKT)*, pp. 1–5, IEEE, Urmia, India, May 2015.

[30] P. K. Roy, J. P. Singh, and S. Banerjee, "Deep learning to filter SMS Spam," *Future Generation Computer Systems*, vol. 102, pp. 524–533, 2020.

[31] S. Dhavale, "C-ASFT: convolutional neural networks-based anti-spam filtering technique," in *Proceedings of the International Conference on Computational Science and Applications*, pp. 49–55, Springer, Singapore, July 2020.

[32] T. Sharmin, F. Di Troia, K. Potika, and M. Stamp, "Convolutional neural networks for image spam detection,"

Information Security Journal: A Global Perspective, vol. 29, no. 3, pp. 103–117, 2020.

[33] E. Ezpeleta, I. Velez de Mendizabal, J. M. G. Hidalgo, and U. Zurutuza, "Novel email spam detection method using sentiment analysis and personality recognition," *Logic Journal of IGPL*, vol. 28, no. 1, pp. 83–94, 2020.

[34] S. Venkatraman, B. Surendiran, and P. Arun Raj Kumar, "Spam e-mail classification for the internet of things environment using semantic similarity approach," *The Journal of Supercomputing*, vol. 76, no. 2, pp. 756–776, 2020.

[35] C. Johnson, B. Khadka, R. B. Basnet, and T. Doleck, "Towards detecting and classifying malicious URLs using deep learning," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*vol. 11, no. 4, pp. 31–48, 2020.

[36] X. Yan, Y. Xu, B. Cui, S. Zhang, T. Guo, and C. Li, "Learning URL embedding for malicious website detection," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6673–6681, 2020.

[37] H. Y. Lee and S. S. Kang, "Word embedding method of sms messages for spam message filtering," in *Proceedings of the 2019 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 1–4, IEEE, Kyoto, Japan, February 2019.

[38] M. Liu, Y. Zhang, B. Liu, Z. Li, H. Duan, and D. Sun, "Detecting and characterizing SMS spearphishing attacks," in *Proceedings of the Annual Computer Security Applications Conference*, pp. 930–943, San Juan, PR, USA, December 2021.

[39] M. Min, J. J. Lee, H. Park, and K. Lee, "Honeypot system for automatic reporting of illegal online gambling sites utilizing SMS spam," in *Proceedings of the 2021 World Automation Congress (WAC)*, pp. 180–185, IEEE, August 2021.

[40] N. K. Nagwani and A. Sharaff, "SMS spam filtering and thread identification using bi-level text classification and clustering techniques," *Journal of Information Science*, vol. 43, no. 1, pp. 75–87, 2017.

[41] T. A. Almeida, T. P. Silva, I. Santos, and J. M. Gómez Hidalgo, "Text normalization and semantic indexing to enhance instant messaging and SMS spam filtering," *Knowledge-Based Systems*, vol. 108, pp. 25–32, 2016.

[42] J. Fattahi and M. Mejri, "SpaML: a bimodal ensemble learning spam detector based on NLP techniques," in *Proceedings of the 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, pp. 107–112, IEEE, Zhuhai, China, January 2021.

[43] N. Choudhary and A. K. Jain, "Towards filtering of SMS spam messages using machine learning based technique," *Communications in Computer and Information Science*, Springer, in *Proceedings of the International Conference on Advanced Informatics for Computing Research*, pp. 18–30, March 2017.

[44] P. Sethi, V. Bhandari, and B. Kohli, "SMS spam detection and comparison of various machine learning algorithms," in *Proceedings of the 2017 international conference on computing and communication technologies for smart nation (IC3TSN)*, pp. 28–31, IEEE, Gurgaon, India, October 2017.

[45] T. K. Ho, "Random decision forests,"vol. 1, pp. 278–282, in *Proceedings of the 3rd international conference on document analysis and recognition*, vol. 1, pp. 278–282, IEEE, Montreal, Canada, August 1995.

[46] T. K. Tin Kam Ho, "The random subspace method for constructing decision forests," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 832–844, 1998.