IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 13, No. 4, December 2024, pp. 3750~3760
ISSN: 2252-8938, DOI: 10.11591/ijai.v13.i4.pp3750-3760

Application of classification algorithms for smishing detection on mobile devices: literature review

Dylan Faredh Calero Sinche, María Acuña Meléndez, Christian Ovalle
Departamento de Ingeniería, Facultad de Ingeniería, Universidad Tecnológica del Perú, Lima, Perú

Article Info

Article history:

Received Jan 9, 2024
Revised Mar 1, 2024
Accepted Mar 21, 2024

Keywords:

Artificial intelligence
Machine learning
Mobile phishing
Mobile security
Smishing

ABSTRACT

Smishing is a form of phishing carried out via mobile devices to steal confidential information from victims. The number of smishing attacks has increased in recent years due to the large number of users acquiring these easy-to-use and functional devices. This literature review objective is to examine the techniques and methods used in smishing attacks using classification algorithms. To do so, we conducted a manual search process and selected 155 articles from Scopus and 29 articles from access to research for development and innovation (ARDI). Of these, 36 articles met the inclusion criteria. In addition, the algorithms most commonly used by the studies were random forest classification techniques, decision trees, and neural networks. These studies analyzed various machine learning models for detecting phishing and smishing messages. The attack simulation scenarios included generating web pages, sending fake links (URLs), and installing malicious applications. The analysis evaluated web pages and SMS messages using a database containing legitimate as well as smishing messages. Based on the results, it is suggested to combine these methods to improve detection performance, making it more robust and promising.

Corresponding Author:

Christian Ovalle
Departamento de Ingeniería, Facultad de Ingeniería, Universidad Tecnológica del Perú
Av. Petit Thouars 116, Lima 15046, Peru
Email: dovalle@utp.edu.pe

1. INTRODUCTION

Currently, the increase in mobile connectivity has increased exponentially, which has led to the emergence of new users who, through the ease offered by cell phones, perform various processes with them [1]–[3], the main ones are researching, bank payments, shopping, sales, entertainment, and studying. In turn, the increased use of cell phones has exposed users to growing risks such as phishing, malware, and smishin [4], [5], the latter being a growing problem since it is a variant of phishing specifically targeted at smartphone users. Therefore, this type of attack represents a significant threat due to the increase in the number of people who perform transactions [6] and operations through their mobile devices. Additionally, 90% of users open SMS messages immediately upon receipt, regardless of the sender [7], which increases the likelihood of information theft.

Hence, this literature review aims to explore the current state of knowledge in developing security models based on classification algorithms for detecting smishing on mobile devices. Consequently, it seeks to provide a critical foundation for the continuous improvement of mobile security and protection against smishing threats. In addressing this security issue efficiently, it is crucial to consider the potential of emerging technologies, as they assist in closing present gaps [8]. Blockchain technology, as one such advancement, renders data immutable [9] and has demonstrated promise and adaptability across various technological and cybersecurity fields [10]–[14]. Nevertheless, it is important to note that, despite its potential advantages, the practical implementation of blockchain technology faces challenges requiring careful attention in parallel [15]. Studies in cybersecurity have identified an increase in phishing attacks targeting end users who utilize smartphones [16]. Furthermore, an analysis of the decentralization of services on the Internet, specifically regarding domain name system (DNS), was conducted. This analysis highlights blockchain technology as an essential tool and delves into the threats and risks associated with DNS decentralization [17]. The blockchain is used to enhance security in detecting phishing attacks in the cloud, emphasizing the importance of protecting user data in that environment [18]. Considering both emerging and established technologies and addressing the lack of comprehensive classifications of methodologies to counter smishing [19], this review covers broad and updated approaches to strengthen security on mobile devices against smishing threats.

In this context, the research aims to identify the main mechanisms and approaches to detect phishing and smishing attacks. Due to the increase in these types of attacks, the objective is to analyze techniques and methods based on classification algorithms to enhance our understanding of the potential dangers posed by such attacks. Therefore, the study is structured as follows: the methodology section describes the systematic literature review method employed, including the research questions and the selection process of the analyzed material. Furthermore, the results section presents and organizes the techniques and methods applied, utilizing existing classification algorithms. Similarly, the discussion delves into the controversy surrounding the sources and classification algorithms selected, providing interpretative criteria on the state of the art, current perspectives, and limitations. Finally, the conclusions section summarizes the main results and limitations of this systematic literature review study and suggests directions for future research on the subject.

2. METHODOLOGY

The review methodology employed adheres to the population, intervention, control, and outcomes (PICO) criteria for the formulation of research questions. Accordingly, a series of steps were followed that covered the formulation of questions, the selection of keywords, the scope of the review, the definition of inclusion and exclusion criteria, and the execution of the search sequence. Thus, the selection of information articles was performed according to the preferred reporting items for systematic reviews and meta-analyses (PRISMA) guidelines, which help in writing and better recognizing the key aspects to be considered [20], [21]. Data extraction was performed using a form adapted to compare the information extracted from the articles studied. A total of 36 articles were analyzed to strengthen the basis of the review. Subsequently, a comprehensive analysis of the results obtained was carried out, followed by the presentation of the discussion of the results and the formulation of conclusive conclusions of the study. Using PRISMA, the most relevant articles closely aligned with our research topic were systematically selected. A stepwise selection process was developed, guided by the principles described in the PRISMA statement [20], to achieve detailed criteria and filters applied in the literature on the topic of our review, specifically, the application of classification algorithms for the detection of impersonation on mobile devices.

A total of four research questions (RQ) were formulated following the PICO framework to conduct a comprehensive review of the topic [22]. In this study, the population (P) is composed of smishing and its derivatives, the intervention (I) considered involves the application of classification algorithms, and the outcomes (O) refer to the first results obtained. Consequently, we formulated four RQs that guide the purpose of the study, as detailed in Table 1. Context (C) focuses on mobile devices. Ultimately, the PICO question is formulated as follows, what is the optimal approach to developing a security model that uses classification algorithms for smishing detection?

Table 1. Research questions answering the PICO question

Research questions	Result
RQ1. What are the specific variants of mobile phishing that have been used as the object of study?	– Description of the problem. – Objective of the research.
RQ2. What were the solutions implemented through the classification algorithms for smishing detection?	– What models were used in the development of the study. – Description of the algorithm implemented.
RQ3. What were the results obtained by applying the proposed solutions?	– Evaluation metrics applied. – Achievements attained. – Limitations of the case study.
RQ4. What practices are recommended for smishing detection and mitigation?	– Recommendations presented by the authors.

2.1. Keyword selection

Keywords were selected according to the study approach for the extraction of information sources. These terms, composed of one or more words, serve as descriptors for the case study queries, guiding the search engine queries to obtain relevant answers and solve the research problems posed. Table 2 presents the specific keywords used. In addition, the Scopus and access to research for development and innovation (ARDI) databases were used to perform a semantic search of the questions posed in the PICO methodology.

Table 2. Keywords - search syntax

Item	Keywords	Search equation syntax
P	Mobile phishing, smishing	Phishing OR supplantation OR “Phishing crime” OR smishing
I	Machine learning, artificial intelligence, deep learning, support vector machine (SVM), random forest trees (RFT).	“Artificial intelligence” OR “Machine learning” OR “Deep learning” OR “Artificial neural networks” OR “Support vector machines” OR “Decision trees” OR “Random Forest technique”
O	Detection, mitigation, vulnerabilities, information leakage, mobile security	Detection OR mitigation OR authentication OR "Phishing detection" OR Vulnerabilities OR “Mobile security” OR “Information Leak” OR Phishing attacks OR Losses OR Threats
C	Mobile Phones / Smartphone	"Mobile devices" OR Smartphone OR Mobile OR “Smart devices” OR Android

2.2. Search sequence

The search for information sources was carried out in the Scopus and ARDÍ databases. The scientific studies to be considered cover the period from 2018 to 2023. The algorithm obtained from this sequence was applied to the title, abstract, and keywords to answer the PICO review question.

2.3. Search algorithm

A search algorithm was executed on the Scopus and ARDÍ databases, yielding 184 information sources. Automatic filters were applied to select documents relevant to the proposed review topic, as outlined in Table 3. The proposed algorithm was designed meticulously to align with the PICO review question to enhance mobile phishing detection capabilities. By employing systematic filters and criteria, the proposed algorithm identified pertinent studies and datasets essential for rigorous analysis in this specialized field.

Table 3. Search algorithms

Database	Search algorithms
SCOPUS	TITLE-ABS-KEY (phishing OR "Phishing Mobile" OR supplantation OR "Phishing crime" OR smishing) AND TITLE-ABS-KEY ("machine learning" OR "Decision Tree" OR "Deep learning" OR "neural network" OR "Support vector machines" OR convolutional OR "Bayesian network" OR "Random Forest technique") AND TITLE-ABS-KEY (detection OR mitigation OR authentication OR vulnerabilities OR "Mobile security" OR "Information Leak" OR losses OR threats) AND TITLE-ABS-KEY (“Mobile devices" OR smartphone OR mobile OR "Smart devices" OR android).
ARDI	Phishing AND mobile AND “machine learning” AND security

2.4. Definition of inclusion and exclusion criteria

The following review study determines the points to be developed based on the quality and updating of the information. In defining the proposed criteria for the articles, we considered studies that present clear information on the methodology applied to the case study, the year of publication, the language, and the type of document. The following inclusion and exclusion criteria were used, as shown in Tables 4 and 5.

Table 4. Inclusion criteria

Criteria	Justification
Research focus	Studies should address the manifestation of Phishing on mobile devices.
Importance factor	Contain methods or techniques linked to classification and applied to Artificial Intelligence.
Experimental	Analyses applied in real environments, simulation or testing of phishing cases.
Quantitative information	Research should report statistical results of the application of such methods. of the application of such methods.

Table 5. Exclusion criteria

Criteria	Justification
Type of publication	Thesis, Books, university book chapters (not updated), conference paper.
Importance factor	Research that does not clearly present a development methodology.
Unit of analysis	Jobs that do not consider Mobile Phishing, smishing as their focus of interest.
Type of language	Languages other than English and Spanish.

Figure 1 shows the PRISMA flowchart, which shows the article selection process for developing the systematic literature review on the application of classification algorithms for detecting smishing on mobile devices. 36 scientific studies were obtained following the PRISMA methodology to address the research questions posed. Thus, the studies were classified according to the problem addressed by each author through a full-text review of the abstracts, introduction, objectives, and methodology for collecting and comparing the methods applied according to the classification algorithms used for smishing detection.

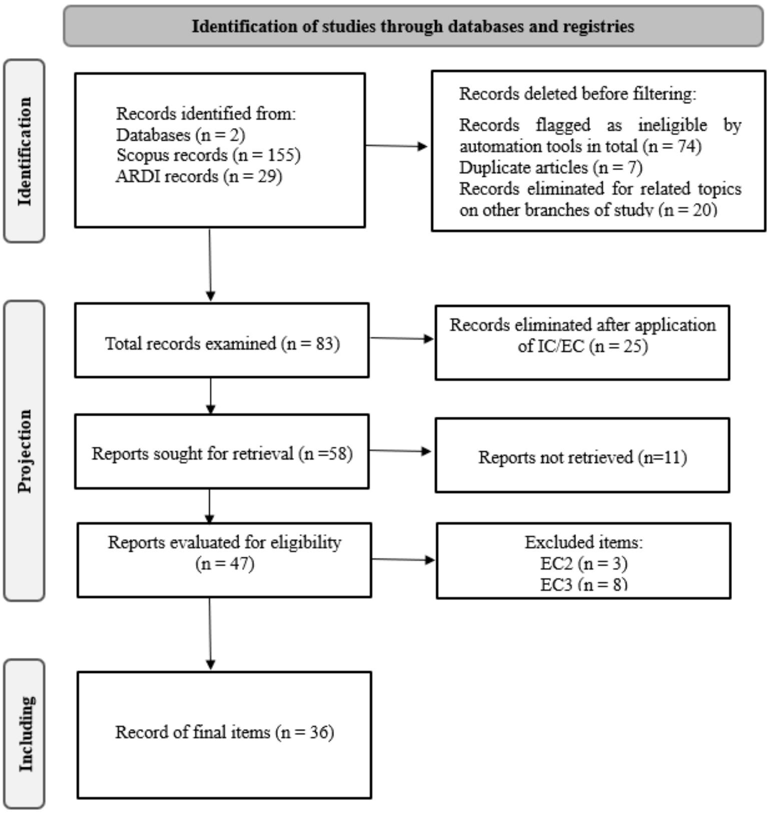
Identification of studies through databases and registries
Identification
Records identified from:
Databases (n = 2)
Scopus records (n = 155)
ARDI records (n = 29)
Records deleted before filtering:
Records flagged as ineligible by automation tools in total (n = 74)
Duplicate articles (n = 7)
Records eliminated for related topics on other branches of study (n = 20)
Projection
Total records examined (n = 83)
Records eliminated after application of IC/EC (n = 25)
Reports sought for retrieval (n =58)
Reports not retrieved (n=11)
Reports evaluated for eligibility (n = 47)
Excluded items:
EC2 (n = 3)
EC3 (n = 8)
Including
Record of final items (n = 36)

Figure 1. PRISMA flow diagram

3. RESULTS AND DISCUSSION

According to the results obtained through the PRISMA methodology [20], information extraction from the selected articles was carried out. The majority of the studies focused on training classification algorithms applied in various cases [23]. An exhaustive analysis of the studies was conducted to identify the different methods of smishing and phishing attacks targeting mobile devices. The classification algorithms most frequently used in the articles were random forest classification, decision trees, logistic regression, naive Bayes, k-nearest neighbors, and neural networks. These algorithms were the most implemented in the selected studies. The studies demonstrate that smishing is continuously updated as new threats are detected, and positive results were obtained using the classification algorithms mentioned in this review. It is worth noting that some of the analyzed sources did not present experimentation of their proposed methods. Instances of attack simulation involved accessing websites, sending false links (URLs), installing malicious applications, and impersonating through SMS messages. The evaluation of web pages and SMS messages was conducted using a database of legitimate and smishing messages. The following section presents the process and development to address the review question.

3.1. Bibliometric data analysis

In this section, considerations related to the study's nature and the publication year of the selected documents were taken into account to gather comprehensive insights into each record. Currently, systematic review studies focusing on the addressed topic are scarce. Consequently, the information collection process relied on articles and conference papers to synthesize the results applied in each study. Based on the review results, the analysis revealed that 24 papers fall under the category of articles, while 12 studies are classified as conference papers. Figure 2 illustrates the reviewed articles published from 2018 to the present. A majority, comprising 70%, were disseminated through articles, with the remaining 30% presented in conference papers. The articles selected to answer the review question show an increase from the year 2022 in the conference papers and do not have a noticeable variation according to the publications made in the course of the year selected as inclusion criteria for the studies.

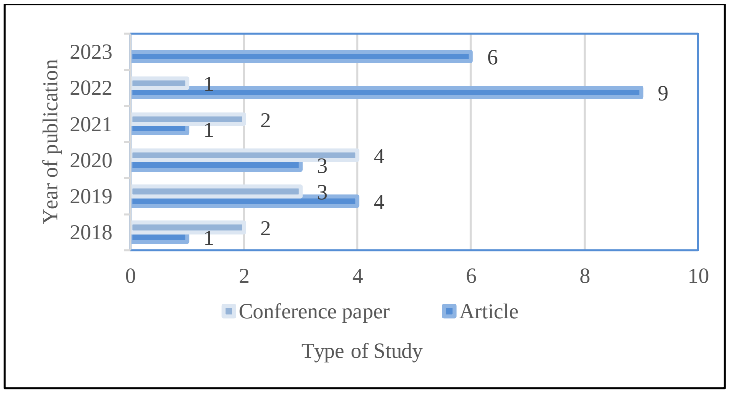

Figure 2. Publications by year and type of study

3.2. Content analysis

This section will systematically organize the collected information to address each review question outlined in the methodology. It will also delineate the critical factors influencing the selection of techniques and algorithms employed across the studies. The subsequent presentation will unveil the outcomes derived from the systematic analysis, providing explicit responses to the review inquiries.

– What is the optimal approach for crafting a security model utilizing classification algorithms to detect smishing?

Based on the examination of the scrutinized studies [24]–[28], this paper delineates an optimal approach for crafting and implementing a security model that encompasses the filtering and denial of mobile SMS services, employing two sophisticated classification algorithms-random forest and vector machine [25], [29], [30]. The authors' utilization of classification algorithms was thoroughly investigated to unearth vulnerabilities in smishing detection. The studies crafted diverse models and mobile applications tailored to address the identified issues, integrating machine learning to enhance smishing detection processes in fraudulent web pages and SMS messages [24], [30]–[33]. A majority of the articles articulate their methodological approach, applying classification algorithms for the analysis of web pages, email messages, malicious URLs, QR codes, and mobile applications. Figure 3 illustrates three examples of smishing.

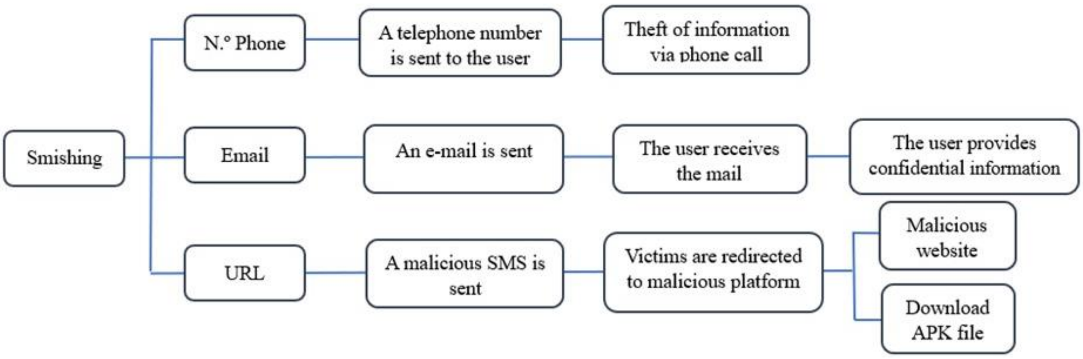
Smishing
N.° Phone
A telephone number is sent to the user
Theft of information via phone call
Email
An e-mail is sent
The user receives the mail
The user provides confidential information
URL
A malicious SMS is sent
Victims are redirected to malicious platform
Malicious website
Download APK file

Figure 3. Smishing attack process [34]

Smishing operations [34] via text messages start with an SMS from the attacker that includes a URL, email, or phone number. Clicking on the link redirects the user to a dangerous website. On this site, a form with a supposed gift is presented, asking the victim for personal information, such as bank details. Alternatively, the malicious message may contain a link that downloads a file to the victim's device [29], [33], [35].

Various models [36]–[40] were employed on a feature matrix generated from a dataset using count vectorizers and term frequency-inverse document frequency (TFIDF). The benchmark model, naive-Bayes multinomial, demonstrated suboptimal performance, whereas random forest excelled with 94.86% accuracy in count vectorization and an even more impressive 99.86% accuracy with TFIDF. Table 6 illustrates the performance of the same model using the TFIDF vectorization technique. Unlike the other models, random forest excelled, achieving an accuracy rate of 99.86%.

Table 6. Model performances with TFIDF vectorization

Model	Training time	Accuracy	AUC	F1-score	Log-loss
Multinomial naive Bayes	4.75 ms	0.8982	0.8986	0.9066	3.51
Logistic regression	74.3 ms	0.9857	0.9857	0.9856	0.49
SVM	671 ms	0.9966	0.9965	0.9965	0.11
K-nearest neighbors	2.39 ms	0.9864	0.9864	0.9865	0.46
Random forest	1.7 s	0.9986	0.9986	0.9986	0.04
AdaBoost	2.07 s	0.9975	0.9972	0.9972	0.09
Extra tree classifier	1.99 s	0.9984	0.9984	0.9984	0.05

3.2.1. RQ1. What are the specific variants of mobile phishing that have been used as the object of study?

Thirty-six articles underwent thorough examination, encompassing studies that explored the detection of phishing across diverse domains [24]–[27]. These domains included smishing attacks via emails and SMS [28]–[33], [35], [41]–[44], phishing detection of spam messages housing malicious URLs [45]–[52], phishing via QR codes [52], and phishing detection within mobile applications [53], [54]. Remarkably, the articles primarily elaborated on the use of machine learning techniques to detect and prevent phishing attacks and their variations on mobile devices. They leveraged existing classification algorithms while also proposing innovative applications.

Following these initial investigations, subsequent studies focused specifically on analyzing smishing [30], [31], [33], [35], [41]–[46], [49], [55]. Moreover, Table 6 provides a detailed breakdown of the classification algorithms most commonly employed in these studies. Subsequently, assessments were carried out to assess the reliability and legitimacy of web pages, online services, and spam messages housing malicious URLs [24], [26], [28], [29], [32], [47], [48], [50], [56]. Noteworthy is the observation that the crux of the study object, addressed in the proposed solutions, pertains to smishing, with 44% of the total articles referencing this specific type of phishing. This challenge stems from the inherent difficulty in identifying smishing, given their constrained content and the diverse array of characters employed by attackers, along with URLs that closely mimic legitimate pages.

3.2.2. RQ2. What were the solutions implemented through the classification algorithms for smishing detection?

In each phishing scenario, we conducted comprehensive comparisons among the proposed solutions. Our analysis unveiled that more than half of the articles leverage machine-learning techniques to update databases for the detection of phishing or smishing. The studies consistently employ widely recognized classification algorithms, such as random forest, decision tree, support vector machine, logistic regression, naive Bayes, and artificial neural network [27]–[35], [41]–[46], [49]–[51], [53], [56]. The authors meticulously elucidated their training methodologies, providing valuable insights into their approaches and the implementation of their proposed solutions. Furthermore, researchers introduced mobile applications designed explicitly for smishing identification [53], [54]. They offered an in-depth overview of the most frequently utilized techniques for implementing and categorizing phishing, introducing an innovative approach known as the graphical user interface (GUI)-squatting attack to assess mobile application interfaces [54]. Consequently, the proposed solutions across various studies exhibit variations based on the specific objectives aimed at addressing the problem. A substantial segment of the scrutinized solutions underwent testing in controlled experimental settings, yielding consistently positive outcomes. Table 7 succinctly presents the proposed solutions and their respective training processes, showing that researchers present new models designed to address various phishing attack scenarios. However, it is highlighted that the classification algorithms implemented are mostly the most used among the studies analyzed.

3.2.3. RQ3. What were the results obtained by applying these proposed solutions?

Several studies similarly employed classification algorithms while addressing various mobile attack scenarios. They applied machine learning techniques to evaluate their efficacy or enhance their respective solutions, aiming to achieve elevated accuracy levels in smishing detection [50], resulting in an impressive 99.57% accuracy rate. Table 8 comprehensively summarizes the accuracy levels observed in all the studies analyzed. This table presents the results obtained in each study, along with its corresponding smishing detection accuracy. Importantly, studies integrating classification algorithms with artificial intelligence predominantly achieved rates exceeding the 90% threshold. This highlights the effectiveness of the techniques used to detect and recognize smishing attacks. The overall average, provided at the end, is 95.39%, signifying a remarkable level of reliability and firm performance in identifying phishing and its mobile-oriented variants, including smishing.

Table 7. Proposed solutions and training process

Reference	Proposed Solutions	Training process
[24]–[27]	Deep learning techniques and expert systems for phishing and malware detection	Artificial neural networks
[28]–[33], [35], [41], [44]	Hybrid framework for feature extraction from phishing email and SMS texts	Convolutional neural networks
[45]–[51]	URL smishing classifier in SPAM messages	SPAM log bank with malicious URLs
[53], [54]	GUI-Squatting attack mobile application	Convolutional neural networks
[55]	Two-dimensional code (QR) method	SVM, pyramidal function network (FPN)

Table 8. Evidence of phishing mitigation effectiveness and results

Reference	Precision (%)	Methodologies used
Gupta *et al.* [50]	99.57	Four machine learning algorithms were evaluated: random forest, k-nearest neighbors, logistic regression and support vector machine.
Jain *et al.* [46]	99.03	Gradient boosted decision tree algorithm was used.
Jain and Gupta [51]	98.74	Evaluation of message data set, the "random forest" classification algorithm was used.
Ulfath *et al.* [31]	98.57	Convolutional neural networks were implemented.
Shaaban *et al.* [49]	98.50	Artificial neural network (ANN) classification algorithm.
Akande *et al.* [41]	98.42	Classification algorithms: RIPPER and C4.5.
Ghourabi *et al.* [29]	98.37	Combination of two deep learning methods short and long memory neural networks Convolutional neural networks and long short-term memory (LSTM).
Yerima and Bashar [45]	98.00	Random forest and decision tree classification algorithm.
Mishra and Soni [30]	97.93	Neural networks with back propagation algorithm.
Mahdavifar and Ghorbani [26]	97.50	It uses an algorithm called deep inference justification (DIJ) to extract refined rules from a trained deep neural network.
Haynes *et al.* [24]	96.00	Artificial neural networks were used.
Zouina and Outtaj [27]	95.80	The smishing detection based on correlation algorithm (SmiDCA) model incorporates dimensionality reduction, based on the random forest classification algorithm.
Yao *et al.* [55]	94.70	Faster region-based convolutional neural network (R-CNN).
Jain *et al.* [25]	93.85	Classification algorithms logistic regression, decision tree and random forest.
Mao *et al.* [47]	93.70	The classifiers evaluated are AdaBoost (AB), random forest, super vector machine and decision tree).
Zaw and Vasupongayya [28]	93.66	Variability of phishing attacks, false positives and false negatives.
Sonowal and Kuppusamy [44]	93.37	SmiDCA model incorporates dimensionality reduction, use of random forest classification algorithm.
Ozker and Sahingoz [48]	92.86	Random forest, support vector machines, logistic regression and decision tree.
Catal *et al.* [56]	92.70	Two classification algorithms were implemented: Super vector machine and random forest.
Korkmaz *et al.* [32]	92.11	Logistic regression, random forest and decision tree.
Jain and Gupta [43]	92.00	The classification algorithms used evaluated decision trees with RIPPER.
Balim and Gunal [54]	83.30	"GUI-Squatting attack", which uses image processing and deep learning based on convolutional neural networks.
Goel and Jain [42]	-	Proposed smishing -classifier model does not present accuracy results.
Chen *et al.* [53]	-	The reviewed study did not implement a classification algorithm.

In the following study [34], the following metrics were implemented to measure the performance and effectiveness of the security model. Table 9 shows the evaluation metrics, which show the evaluation of the performed models, covering the following performance metrics [34], [57], [58]. A, true positives (TP) mean accurately predicted malware instances, while false negatives (FN) denote misclassified malware instances. True positive rate (TPR) stands for recovery and sensitivity. B, false positives (FP) represent the count of incorrectly predicted benign classifications. C, F-measure is used for comparative performance analysis.

Table 9. Model evaluation metrics

N.º	Evaluation metrics	Formulation of metrics
A	Accuracy	$\frac{TP + TN}{TP + TF + TN + FN}$
B	Precision	$\frac{TP}{TP + FP}$
C	F-measure	$\frac{2. \text{Precision}}{\text{Precision} + \text{Recall}}$

3.2.4. RQ4. What practices are recommended for smishing detection and mitigation?

This section presents the main insights from the studies conducted, which can serve as valuable considerations for future research. These insights possess the capacity to aid in formulating essential guidelines to improve smishing detection, either by introducing innovative methodologies or refining existing ones. Table 10 lists the studies that deserve further exploration, as recommended by the authors, to provide a more complete understanding of the problem addressed. This table highlights many recommendations that emphasize the effectiveness of using machine learning techniques to improve phishing detection results. Furthermore, it suggests delving deeper into this domain to guide future research efforts.

Table 10. Recommendations for smishing detection

Reference	Recommendations
[25]	They recommend investigating the use of ensemble learning techniques, such as Bagging and Boosting.
[30]	Use efficient machine learning algorithms to detect and prevent smishing.
[45]	Investigate other types of novelty detection models based on semi-supervised machine learning.
[28]	Address more adaptive techniques and models for any domain where smishing occurs.
[55]	Use improved logo recognition techniques.
[46]	Using content analysis to better recognize patterns to indicate smishing.
[29]	Perform analysis of URLs or files that are attached to SMS messages.
[24]	Regularly update databases of known smishing sites.
[31]	Introduce significant new rules that can improve the true positive rate and overall targeting accuracy.
[26]	Use a combination of deep neural networks and expert systems to improve the accuracy and robustness of the systems.
[44]	Add more features and use new feature selection algorithms to improve accuracy.
[27]	Evaluate the size of the URL, the number of dashes, dots, numeric IP characters in the URL.

3.3. Discussion

The scope of articles related to the application of machine learning-based classification algorithms for smishing detection on mobile devices has significantly contributed to the development of this work. This discussion encompasses the obtained results about information selection and review questions, conducted within the Scopus and ARDI databases. Although we found commonalities among articles using keywords, it became evident that they lacked a specific emphasis on mobile devices. Nevertheless, the outcomes yielded positive results that were consistent with the predefined objectives of the review. It's worth noting that most studies centered on smishing cases, yet a few omitted explicit mentions of the context in which they deployed and evaluated the implemented algorithm. An analysis of machine learning techniques revealed a prevalent utilization of similar classification algorithms across studies, leading to comparable results. Some articles specifically addressed smishing, whereas others delved into exploring novel methods for phishing detection. As a result, the enduring influence and applicability of mobile augmented reality may stimulate additional evidence-based practical research into phishing and smishing attacks.

The authors employed techniques and methodologies to address prevalent smishing attacks and proposed viable solutions. The implemented classification algorithms necessitate a continuous data stream for the identification of smishing instances on mobile devices. This impact is evident across all classification algorithms, albeit having undergone various testing methodologies, yielding similar results. The assessment of these findings displayed variability due to the diverse approaches employed. The simulation encompassed the integration of a character database for the recognition of both textual content and images through the utilization of artificial intelligence. Consequently, the proposed solutions require periodic updates to effectively discern evolving patterns of attacks. The predominant strategies for mitigating smishing primarily revolve around end-user awareness, given their pivotal role as the primary target for phishing attackers. The examined studies advocate for the exploration of deep learning techniques, particularly the utilization of convolutional neural networks and recurrent neural networks (RNN). It is advisable to regularly update the database of detection systems to enhance accuracy over time. Leveraging the advantages offered by deep neural networks can significantly contribute to the identification of SMS spam. Additionally, there is a notable gap in the existing literature concerning the prevention of cybercrime in mobile applications, emphasizing the need for further research in this area due to the limited number of studies addressing this crucial aspect.

However, similar to any other review, this article does pose some limitations. These include factors such as the selection of keywords and the establishment of inclusion and exclusion criteria, which might impact the quantity of results derived from the selected research. Furthermore, a scrutiny of the studies we analyzed allows us to distill the primary issues and constraints they confront. These encompass a limited database, structural aspects of research, scalability issues for real-time analysis with extensive web page volumes, precision in detecting abbreviations, and the textual length of messages per experiment. Notably, there is a dearth of updated systematic reviews regarding the research topic surrounding the use of classification algorithms for smishing detection. Given that this technology has emerged in recent years, and experiments in this domain are ongoing, the effectiveness of the methods proposed in this study in a real-world environment remains a subject for further investigation.

4. CONCLUSION

This study establishes a precise and clear working methodology for reviewing the application of classification algorithms in smishing detection on mobile devices. Integrating various methods proposed by different authors forms a comprehensive framework that effectively addresses emerging cases of smishing, reflecting a heightened research interest in this area. With smishing, particularly the transmission of malicious text messages with URLs, dominating 44% of the reviewed articles, the study highlights the urgent need to tackle challenges associated with this prevalent phishing attack. Despite content limitations, the results demonstrate commendable outcomes, with consistently high accuracy levels surpassing 90%, averaging an impressive 95.48%. This underscores the robust performance of algorithms employed in detecting smishing, making classification algorithms pivotal in assessing effectiveness on mobile devices. Accordingly, most studies employed standard classification algorithms, such as logistic regression, KNN, Bayes Net, naive Bayes, radial basis function, decision tree, SVM, random forest, and also used deep neural networks, to analyze the specific characteristics of malicious SMS and URLs. These techniques proved effective, yielding promising results with high rates of true positives and negatives. However, it is crucial to highlight areas for improvement and propose avenues for future research, including integrating ensemble learning techniques, investigating alternative novelty detection models, performing in-depth analysis of URLs and SMS message attachments, and constantly updating databases hosting recognized phishing sites to increase accuracy rates and strengthen the resilience of phishing and smishing detection systems. In conclusion, the analysis of phishing detection on mobile devices shows us and provides a promising approach based on machine learning and deep learning techniques. However, continued research is required due to the increase of processes and activities that users can perform with their cell phones and the implementation of the recommendations proposed by the authors to further improve the detection and mitigation of these threats in the future and that the proposed methodologies do not become outdated.

ACKNOWLEDGMENTS

We express the sincerely gratitude to Technological University of Peru for its constant support in providing me with all the tools and infrastructure necessary to carry out this research, such as the availability of literature, access to laboratories, and management support, which have been fundamental for the success of this project.

REFERENCES

[1] A. Althunibat, M. A. Almaiah, and F. Altarawneh, “Examining the factors influencing the mobile learning applications usage in higher education during the covid-19 pandemic,” *Electronics*, vol. 10, no. 21, 2021, doi: 10.3390/electronics10212676.

[2] G. R. D. Lazaro and J. M. Duart, “Moving learning: a systematic review of mobile learning applications for online higher education,” *Journal of New Approaches in Educational Research*, vol. 12, no. 2, pp. 198–224, 2023, doi: 10.7821/naer.2023.7.1287.

[3] M. W. -Fernando, “The use of mobile technologies in online shopping during the covid-19 pandemic - an empirical study,” *Procedia Computer Science*, vol. 192, pp. 3413–3422, 2021, doi: 10.1016/j.procs.2021.09.114.

[4] M. Hijji and G. Alam, “A multivocal literature review on growing social engineering based cyber-attacks/threats during the covid-19 pandemic: challenges and prospective solutions,” *IEEE Access*, vol. 9, pp. 7152–7169, 2021, doi: 10.1109/ACCESS.2020.3048839.

[5] A. Alzahrani, “Coronavirus social engineering attacks: Issues and recommendations,” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 5, pp. 154–161, 2020, doi: 10.14569/IJACSA.2020.0110523.

[6] J. Zhu and M. Wang, “Analyzing the effect of people utilizing mobile technology to make banking services more accessible,” *Frontiers in Public Health*, vol. 10, 2022, doi: 10.3389/fpubh.2022.879342.

[7] H. A. M. Wahsheh and M. S. Al-Zahrani, “Lightweight cryptographic and artificial intelligence models for anti-Smishing,” *Lecture Notes in Networks and Systems*, vol. 322, pp. 483–496, 2022, doi: 10.1007/978-3-030-85990-9_39.

[8] S. Abdi, I. Kitsara, M. S. Hawley, and L. P. de Witte, “Emerging technologies and their potential for generating new assistive technologies,” *Assistive Technology*, vol. 33, pp. 17–26, 2021, doi: 10.1080/10400435.2021.1945704.

[9] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, “Differential privacy-based blockchain for industrial internet-of-things,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4156–4165, 2020, doi: 10.1109/TII.2019.2948094.

[10] P. D. Ameyaw and W. T. D. Vries, “Blockchain technology adaptation for land administration services: The importance of socio-cultural elements,” *Land Use Policy*, vol. 125, 2023, doi: 10.1016/j.landusepol.2022.106485.

[11] M. Iranmanesh, P. Maroufkhani, S. Asadi, M. Ghobakhloo, Y. K. Dwivedi, and M. L. Tseng, “Effects of supply chain

transparency, alignment, adaptability, and agility on blockchain adoption in supply chain among SMEs," *Computers and Industrial Engineering*, vol. 176, 2023, doi: 10.1016/j.cie.2022.108931.

[12] M. O. Momoh, P. U. Chinedu, W. Nwankwo, D. Aliu, and M.S. Shaba, "Blockchain adoption: applications and challenges," *International Journal of Software Engineering and Computer Systems*, vol. 7, no. 2, pp. 19–25, 2021, doi: 10.15282/ijsecs.7.2.2021.3.0086.

[13] P. Jiang *et al.*, "Blockchain technology applications in waste management: Overview, challenges and opportunities," *Journal of Cleaner Production*, vol. 421, 2023, doi: 10.1016/j.jclepro.2023.138466.

[14] N. Shohruhxon, "Leveraging blockchain technology in small businesses: exploring the pros and cons," *Universal Journal of Academic and Multidisciplinary Research*, vol. 1, no. 2, pp. 63–67.

[15] M. Alimohammadlou and S. Alinejad, "Challenges of blockchain implementation in SMEs' supply chains: an integrated IT2F-BWM and IT2F-DEMATEL method," *Electronic Commerce Research*, 2016, pp. 1–6, 2023, doi: 10.1007/s10660-023-09696-3.

[16] J. Lee, Y. Lee, D. Lee, H. Kwon, and D. Shin, "Classification of attack types and analysis of attack methods for profiling phishing mail attack groups," *IEEE Access*, vol. 9, pp. 80866–80872, 2021, doi: 10.1109/ACCESS.2021.3084897.

[17] C. Patsakis, F. Casino, N. Lykousas, and V. Katos, "Unravelling Ariadne's thread: exploring the threats of decentralised DNS," *IEEE Access*, vol. 8, pp. 118559–118571, 2020, doi: 10.1109/ACCESS.2020.3004727.

[18] R. N. Karthika, C. Valliyammai, and M. Naveena, "Phish block: a blockchain framework for phish detection in cloud," *Computer Systems Science and Engineering*, vol. 44, no. 1, pp. 777–795, 2022, doi: 10.32604/csse.2023.024086.

[19] S. Chanti and T. Chithralekha, "A literature review on classification of phishing attacks," *International Journal of Advanced Technology and Engineering Exploration*, vol. 9, no. 89, pp. 446–476, 2022, doi: 10.19101/IJATEE.2021.875031.

[20] M. J. Page *et al.*, "PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews," *The BMJ*, vol. 372, 2021, doi: 10.1136/bmj.n160.

[21] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *The BMJ*, vol. 372, 2021, doi: 10.1136/bmj.n71.

[22] G. Robleda, "Structured question to generate search for a systematic review," *Enfermería Intensiva*, vol. 30, no. 3, pp. 144–147, 2019, doi: 10.1016/j.enfie.2019.07.001.

[23] U. I. Akpan and A. Starkey, "Review of classification algorithms with changing inter-class distances," *Machine Learning with Applications*, vol. 4, 2021, doi: 10.1016/j.mlwa.2021.100031.

[24] K. Haynes, H. Shirazi, and I. Ray, "Lightweight URL-based phishing detection using natural language processing transformers for mobile devices," *Procedia Computer Science*, vol. 191, pp. 127–134, 2021, doi: 10.1016/j.procs.2021.07.040.

[25] A. K. Jain, N. Debnath, and A. K. Jain, "APuML: An efficient approach to detect mobile phishing webpages using machine learning," *Wireless Personal Communications*, vol. 125, no. 4, pp. 3227–3248, 2022, doi: 10.1007/s11277-022-09707-w.

[26] S. Mahdavifar and A. A. Ghorbani, "DeNNeS: deep embedded neural network expert system for detecting cyber attacks," *Neural Computing and Applications*, vol. 32, no. 18, pp. 14753–14780, 2020, doi: 10.1007/s00521-020-04830-w.

[27] M. Zouina and B. Outtaj, "A novel lightweight URL phishing detection system using SVM and similarity index," *Human-Centric Computing and Information Sciences*, vol. 7, no. 1, 2017, doi: 10.1186/s13673-017-0098-1.

[28] S. K. Zaw and S. Vasupongayya, "Enhancing case-based reasoning approach using incremental learning model for automatic adaptation of classifiers in mobile phishing detection," *International Journal of Networked and Distributed Computing*, vol. 8, no. 3, pp. 152–161, 2020, doi: 10.2991/ijndc.k.200515.001.

[29] A. Ghourabi, M. A. Mahmood, and Q. M. Alzubi, "A hybrid CNN-LSTM model for SMS spam detection in arabic and english messages," *Future Internet*, vol. 12, no. 9, 2020, doi: 10.3390/FI12090156.

[30] S. Mishra and D. Soni, "DSmishSMS-A system to detect smishing SMS," *Neural Computing and Applications*, vol. 35, no. 7, pp. 4975–4992, 2023, doi: 10.1007/s00521-021-06305-y.

[31] R. E. Ulfath, H. Alqahtani, M. Hammoudeh, and I. H. Sarker, "Hybrid CNN-GRU framework with integrated pre-trained language transformer for SMS phishing detection," *ACM International Conference Proceeding Series*, pp. 244–251, 2021, doi: 10.1145/3508072.3508109.

[32] M. Korkmaz, O. K. Sahingoz, and B. Diri, "Detection of phishing websites by using machine learning-based URL analysis," *2020 11th International Conference on Computing, Communication and Networking Technologies*, pp. 1-7, 2020, doi: 10.1109/ICCCNT49239.2020.9225561.

[33] S. Mishra and D. Soni, "Smishing detector: a security model to detect Smishing through SMS content analysis and URL behavior analysis," *Future Generation Computer Systems*, vol. 108, pp. 803–815, 2020, doi: 10.1016/j.future.2020.03.021.

[34] A. R. Mahmood and S. M. Hameed, "Review of smishing detection via machine learning," *Iraqi Journal of Science*, vol. 64, no. 8, pp. 4244–4259, 2023, doi: 10.24996/ijs.2023.64.8.42.

[35] IISEC, A. Varol, and IEEE, "Innovative technologies for digital transformation," *1st International Informatics and Software Engineering Conference (IISEC-2019)*, 2019.

[36] I. S. Mambina, J. D. Ndibwile, and K. F. Michael, "Classifying swahili Smishing attacks for mobile money users: a machine-learning approach," *IEEE Access*, vol. 10, pp. 83061–83074, 2022, doi: 10.1109/ACCESS.2022.3196464.

[37] G. Giorgi, A. Saracino, and F. Martinelli, "Email spoofing attack detection through an end-to-end authorship attribution system," *International Conference on Information Systems Security and Privacy*, pp. 64–74, 2020, doi: 10.5220/0008954600640074.

[38] B. L. J. Chuan, M. M. Singh, and A. R. M. Shariff, "APTGuard: Advanced persistent threat (APT) detections and predictions using android smartphone," *Lecture Notes in Electrical Engineering*, vol. 481, pp. 545–555, 2019, doi: 10.1007/978-981-13-2622-6_53.

[39] M. Rajab, "Visualization model based on phishing features," *Journal of Information and Knowledge Management*, vol. 18, no. 1, 2019, doi: 10.1142/S0219649219500102.

[40] R. B. M. Shivakumar, B. D. Parameshachari, "GSSS institute of engineering and technology for women, institute of electrical and electronics engineers. bangalore section, and institute of electrical and electronics engineers," *4th International Conference on Electrical, Electronics, Communication, Computer Technologies nd Optimization Techniques: ICEECCOT - 2019*, 2018.

[41] O. N. Akande *et al.*, "SMSPROTECT: An automatic Smishing detection mobile application," *ICT Express*, vol. 9, no. 2, pp. 168–176, 2023, doi: 10.1016/j.icte.2022.05.009.

[42] D. Goel and A. K. Jain, "Smishing-classifier: A novel framework for detection of Smishing attack in mobile environment," *Communications in Computer and Information Science*, vol. 828, pp. 502–512, 2018, doi: 10.1007/978-981-10-8660-1_38.

[43] A. K. Jain and B. B. Gupta, "Rule-based framework for detection of Smishing messages in mobile environment," *Procedia Computer Science*, vol. 125, pp. 617–623, 2018, doi: 10.1016/j.procs.2017.12.079.

[44] G. Sonowal and K. S. Kuppusamy, "SMIDCA: An anti-Smishing model with machine learning approach," *Computer Journal*, vol. 61, no. 8, pp. 1143–1157, 2018, doi: 10.1093/comjnl/bxy039.

[45] S. Y. Yerima and A. Bashar, "Semi-supervised novelty detection with one class SVM for SMS spam detection," *International Conference on Systems, Signals, and Image Processing*, vol. 2022, 2022, doi: 10.1109/IWSSIP55020.2022.9854496.

[46] A. K. Jain, B. B. Gupta, K. Kaur, P. Bhutani, W. Alhalabi, and A. Almomani, "A content and URL analysis-based efficient

approach to detect smishing SMS in intelligent systems," *International Journal of Intelligent Systems*, vol. 37, no. 12, pp. 11117–11141, 2022, doi: 10.1002/int.23035.

[47] J. Mao *et al.*, "Phishing page detection via learning classifiers from page layout feature," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, Dec. 2019, doi: 10.1186/s13638-019-1361-0.

[48] U. Ozker and O. K. Sahingoz, "Content based phishing detection with machine learning," *2020 International Conference on Electrical Engineering, ICEE 2020*, 2020, doi: 10.1109/ICEE49691.2020.9249892.

[49] M. A. Shaaban, Y. F. Hassan, and S. K. Guirguis, "Deep convolutional forest: a dynamic deep ensemble approach for spam detection in text," *Complex and Intelligent Systems*, vol. 8, no. 6, pp. 4897–4909, 2022, doi: 10.1007/s40747-022-00741-6.

[50] B. B. Gupta, K. Yadav, I. Razzak, K. Psannis, A. Castiglione, and X. Chang, "A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment," *Computer Communications*, vol. 175, pp. 47–57, 2021, doi: 10.1016/j.comcom.2021.04.023.

[51] A. K. Jain and B. B. Gupta, "Feature based approach for detection of Smishing messages in the mobile environment," *Journal of Information Technology Research*, vol. 12, no. 2, pp. 17–35, 2019, doi: 10.4018/JITR.2019040102.

[52] I. H. Chipa, J. G. -Cruzado, and J. R. Villacorta, "Mobile applications for cybercrime prevention: a comprehensive systematic review," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 10, pp. 73–82, 2022, doi: 10.14569/IJACSA.2022.0131010.

[53] S. Chen, L. Fan, C. Chen, M. Xue, Y. Liu, and L. Xu, "GUI-squatting attack: automated generation of android phishing apps," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2551–2568, 2021, doi: 10.1109/TDSC.2019.2956035.

[54] C. Balim and E. S. Gunal, "Automatic detection of Smishing attacks by machine learning methods," *1st International Informatics and Software Engineering Conference: Innovative Technologies for Digital Transformation*, 2019, doi: 10.1109/UBMYK48245.2019.8965429.

[55] W. Yao, Y. Ding, and X. Li, "Deep learning for phishing detection," *16th IEEE International Symposium on Parallel and Distributed Processing with Applications, 17th IEEE International Conference on Ubiquitous Computing and Communications, 8th IEEE International Conference on Big Data and Cloud Computing, 11t*, pp. 645–650, 2018, doi: 10.1109/BDCloud.2018.00099.

[56] C. Catal, G. Giray, B. Tekinerdogan, S. Kumar, and S. Shukla, "Applications of deep learning for phishing detection: a systematic literature review," *Knowledge and Information Systems*, vol. 64, no. 6, pp. 1457–1500, 2022, doi: 10.1007/s10115-022-01672-x.

[57] S. Mishra and D. Soni, "Implementation of 'Smishing detector': an efficient model for Smishing detection using neural network," *SN Computer Science*, vol. 3, no. 3, 2022, doi: 10.1007/s42979-022-01078-0.

[58] O. El Kouari, H. Benaboud, and S. Lazaar, "Using machine learning to deal with phishing and spam detection: an overview," *ACM International Conference Proceeding Series*, 2020, doi: 10.1145/3386723.3387891.

BIOGRAPHIES OF AUTHORS

Dylan Faredh Calero Sinche is student of systems and computer engineering of the Technological University of Peru, Lima, Peru. His current research interests include machine learning, Smishing detection, mobile security, and information security models. He can be contacted at email: u18201660@utp.edu.pe.

María Acuña Meléndez is professor at the Faculty of Engineering of Engineering of the Technological University of Peru, Lima, Peru. She holds a Ph.D. in Systems Engineering. Her research areas are information systems and communications, as well as systems auditing and information security. She has participated in several research projects, as well as in thesis advising. She has registered several patents on software copyrights. Her research interests include information systems, data science, information security, data mining, artificial intelligence, and knowledge management among other related lines of research. She can be contacted at email: c21584@utp.edu.pe.

Christian Ovalle is an associate professor at the Faculty of Engineering of the Technological University of Peru, Lima, Peru. He has a Ph.D. in Systems Engineering with a specialization in artificial intelligence. His research areas are process mining, business data analysis, and pattern recognition. He is the CEO of the 7D consultancy dedicated to the Investigation of intelligent solutions. He has participated in different research projects, receiving awards from the Peruvian Ministry of Defense and the Armed Forces Army for the best general researcher, which is a technology-based company and his innovative products received national and international recognition. He has filed a number of patents and industrial designs on his innovative ideas. His research interests include data mining, artificial intelligence, image/signal processing, bibliometrics, and pattern recognition. He can be contacted at email: dovalle@utp.edu.pe.