Mobile Applications for Cybercrime Prevention: A Comprehensive Systematic Review

Irma Huamanñahui Chipa[1], Javier Gamboa-Cruzado[2], Jimmy Ramirez Villacorta[3]
Facultad de Ingeniería de Sistemas, Universidad Nacional Mayor de San Marcos, Lima, Perú[1, 2]
Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional de la Amazonía Peruana, Iquitos, Perú[3]

Abstract—**Now-a-days, cybercrime, cyberattacks, cyber security, phishing and malware are taking a more notorious role in people's daily lives, not only at the international level. The great technological leaps brought with them new modalities of cybercrime, the number of victims of cybercriminals has increased considerably. The objective of this study is to determine the state of the art about Mobile Applications and their impact on Computer Crime Prevention. Therefore, it has become necessary to know what preventive measures are being taken, such as techniques for detecting computer crimes, their modalities and their classification. To close this knowledge gap, a systematic literature review (SLR), a methodology proposed by Kitchenham & Charters, was proposed to obtain the detection techniques and classification of computer crimes based on the review of 68 papers published between the years 2017 and 2022. Likewise, different tables and graphs of the selected studies are provided, which offer additional information such as the most used keywords per paper, biometric networks, among others.**

Keywords—Computer crimes; cyberattacks; cyber security; mobile apps; phishing; machine learning; malware; systematic literature review

I. Introduction

Due to the Covid-19 pandemic, the use of Information and Communication Technologies (ICT) has taken an enormous leap forward, especially in the less developed countries of Latin America. In the labor field, many continue to opt for teleworking, online sales have increased notoriously, in the same way computer crimes in all its forms have also been increasing. A computer crime is a crime committed through the use of electronic tools and methods, against people or organizations [1, 6]. It should also be noted that computer crimes have a tendency to become a long-term factor in the political and economic process, due to the lack of great success in counteracting them [4]. There are several types of cybercrime, for which various criteria must be used to classify them [2]. There are two categories of computer crimes: those that are computer or cell phone assisted, such as child pornography, fraud, money laundering and cyberstalking, while computer crimes that are computer-centric include hacking, phishing and website defacement [6]. As well as there are computer crimes there are also techniques to counter various computer crimes; such as Machine Learning, Data mining, Neural network, Firewall, etc. [2, 6, 8, 27,68].

Being clear about the types of cybercrime and possible techniques to counteract them, would be of great help if these in turn are disseminated to users, so that they can avoid becoming victims of cybercriminals. In 2017 cybercrime costs amounted to approximately $600 billion in the United States, by 2019 they increased by 118% in the first half of the year leading to huge losses and financial implications, and by 2020 the statistics increased from 71% in mobile malware and 689% in PowerShell malware [1].

Therefore, it is important to determine the types of computer crimes and techniques that help to counteract them and above all to have a dissemination plan to all users of mobile applications, who day by day perform different operations online, or simply use their cell phones to enter their social networks. There are different studies in which they apply other technologies and tools such as Machine Learning to prevent computer crimes [2, 6, 8, 27,68], as well as they also use artificial intelligence to be able to counteract computer crimes [70, 71].

Given this worrying reality, i.e., the lack of knowledge of the advances and achievements of experimental research worldwide and its impact on the prevention of computer crimes in the countless articles published, and the limited dissemination of systematic review articles on the subject will allow the international research community to close these technological and scientific gaps.

In the present study, the aim is to conduct a comprehensive systematic review of research regarding mobile applications that help prevent computer crimes. Few studies involving both variables were found, but studies found on other tools and technologies that help to counteract computer crimes are also shown.

The structure of the document is organized as follows. Section II presents the Background of the study. The research methodology is presented in Section III. Section IV presents the research results and discussions. Section V presents the conclusions and future studies. Finally, Section VI presents the acknowledgements.

II. Background and Related Works

In this study, no SLR has been found that is focused on presenting how mobile applications can improve the prevention of computer crimes, however, some papers have been found that partially provide answers to the problem of computer crimes, not necessarily using mobile applications, but other technologies and some potential methods and techniques to detect computer crime threats.

The authors Al-Khater, Al-Ma'adeed, Ahmed, Sadiq & Khan [6] conducted a comprehensive literature review on computer crime detection techniques, for this purpose they first made a classification of the types of computer crimes, then they presented the computer crime detection techniques using Statistical methods, Machine Learning, Neural Networks, Deep Learning, Fuzzy Logic Neural Network, Data Mining and other techniques. They managed to make a broad classification of computer crimes, they also analyzed numerous studies regarding the detection rates achieved and some limitations, advantages and disadvantages of each technique.

Wiafe, Nti, Nyarko, Assyne & Gulliver [70], conducted an SLR with 131 papers, which were analyzed using quantitative and qualitative methods, to minimize the knowledge gap regarding artificial intelligence methods to combat computer crimes. The study was focused on intrusion prevention and detection systems, where it was determined that the most used technique was support vector machines.

Author Jeong [71] also conducted a literature review on security threats and crimes related to Artificial Intelligence. His paper defines the term Artificial Intelligence crime and classifies it into 2 categories: Artificial Intelligence as a crime tool and Artificial Intelligence as a target crime, inspired by a taxonomy of cybercrime: Computer as a crime tool and Computer as a crime tool. Through the proposed taxonomy, foreseeable Artificial Intelligence crimes are systematically studied and related, forensic techniques are also addressed.

Weichbroth & Łysik [72], performed a RSL on a set of keywords, aiming to identify and analyze existing threats and best practices in mobile security. To obtain the results, 167 users were evaluated; the results show a high awareness of threats and their countermeasures in the mobile application domain. While recognizing the risks associated with physical and social factors, the majority of respondents stated the use of integrated methods to mitigate the negative impact of malware and social engineering scams.

Liu, Xu, Zhang, & Sun [73] conducted a systematic literature review, where they suggest that machine learning is an effective and promising way to detect Android malware. This paper presents a comprehensive survey of Machine Learning-based Android malware detection approaches, they also present the background of Android applications including Android system architecture, security mechanisms, and Android malware classification with the aim to help scholars get a complete picture of Machine Learning-based Android malware detection.

The RSL provides a comprehensive review of new threats and techniques to be able to counter cybercrime, given the new juncture of the Covid-19 pandemic, there have been huge leaps in the use of ICT and thus new cybercrime threats have also been generated. To process the information extracted from the papers, the artificial intelligence tool (RAj) developed by the author Dr. Javier Gamboa Cruzado has been used.

III. Methodology

The review method used is based on the fundamentals and guidelines of Kitchenham & Charters [69]. The method allows the formulation of research questions, objectives, search sources and their respective strategies, also allows the selection of studies by exclusion criteria, achieving the identification of studies, also applying quality criteria, data extraction and finally the synthesis of findings. It can be seen in Fig. 1.

A. Research Problems and Objectives

In the SLR conducted, the formulation of the research questions made it possible to formulate the search strategies necessary to achieve a good extraction and analysis of the data. It also made it possible to identify the research objectives, as shown in Table I.

B. Search Sources and Search Strategies

The libraries used to perform the research searches are: Web of Science, Scopus, ProQuest, ScienceDirect, ACM Digital Library, Wiley Online Library and Taylor & Francis Online.

The search strategy included keywords relevant to the research. As shown in Table II.

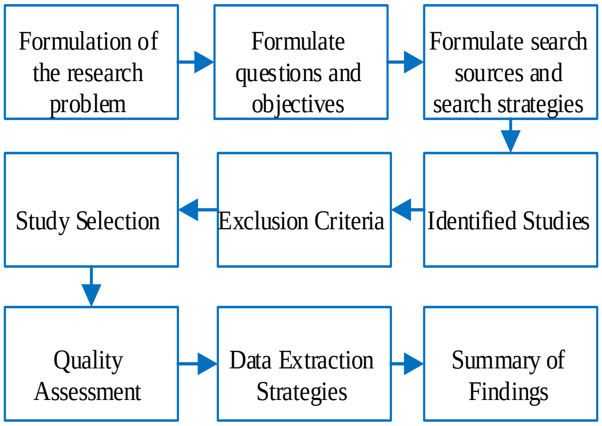

Formulation of the research problem
Formulate questions and objectives
Formulate search sources and search strategies
Study Selection
Exclusion Criteria
Identified Studies
Quality Assessment
Data Extraction Strategies
Summary of Findings

Fig. 1. Stages of Systematic Literature Review.

TABLE I. Research Questions and Objectives

Research Question	**Objective**
RQ1: What are the most commonly used techniques in Computer Crime Prevention investigations?	To know the techniques of Computer Crime Prevention.
RQ2: What are the most used Keywords in Mobile Application research and Cybercrime prevention?	Determine the most used keywords in the papers on Mobile Applications and Cybercrime prevention.
RQ3: What are the most cited papers, by country, number of citations and by source in research on mobile applications and cybercrime prevention?	Identify the most cited papers by country, number of citations and sources in research on mobile applications and cybercrime prevention.
RQ4: What are the types of computer crimes in the investigations reviewed?	To know the classification of computer crimes in the investigations reviewed.
RQ5: Which Authors are Co-Occurring in Research on Mobile Applications and Cybercrime Prevention?	Determine the authors who frequently co-occur in research on mobile applications and cybercrime prevention.

TABLE II. SEARCH DESCRIPTORS AND THEIR SYNONYMS

Descriptor	Type of Variable
Mobile Applications/ Applications	Independent Variable
Computer Crime Prevention/ Computer Crimes	Dependent Variable

The search equations were used according to the selected sources, as shown in Table III.

TABLE III. SOURCES AND SEARCH EQUATIONS

Source	**Search Equations**
Web of Science	(ALL=((“mobile apps”) OR apps AND (“prevention from cybercrime”) OR cybercrime))
Scopus	(ALL ("mobile apps") OR ALL (apps) AND ALL ("prevention from cybercrime") OR ALL (cybercrime))
ProQuest	(“mobile apps”) OR apps AND (“prevention from cybercrime”) OR cybercrime
ScienceDirect	(("mobile apps" OR apps) AND ("prevention from cybercrime" OR cybercrime))
ACM Digital Library	[[All: "mobile apps"] OR [All: apps]] AND [[All: "prevention from cybercrime"] OR [All: cybercrime]]]
Wiley Online Library	("mobile apps" OR apps) AND ("prevention from cybercrime" OR cybercrime)
Taylor & Francis Online	[[All: "mobile apps"] OR [All: apps]] AND [[All: "prevention from cybercrime"] OR [All: cybercrime]]

C. Identified Studies

The search yielded 561,055 papers, see Fig. 2.

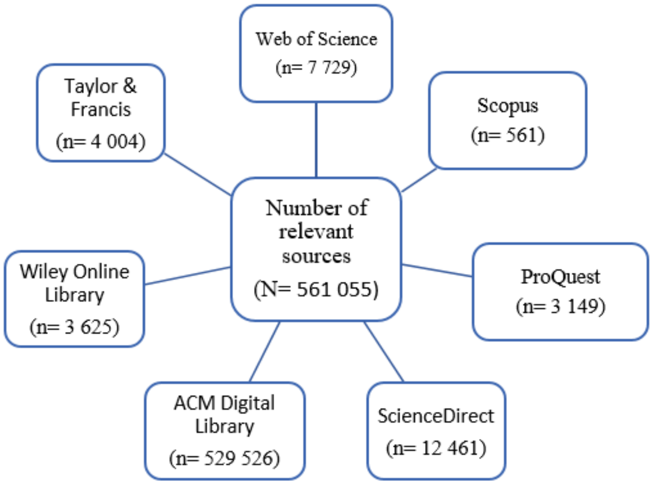


Fig. 2. Number of Studies Identified.

D. Exclusion Criteria

Six exclusion criteria (EC) were applied in order to obtain papers with more relevance to the present investigation. The EC were as follows:

CE1: The papers are older than five years.

CE2: The papers are not written in English.

SG3: The full text of the paper is not available.

SG4: The papers were not published in Conferences or peer-reviewed Journals.

SD5: The titles and keywords of the papers are not very appropriate

SD6: The proposed solution does not apply to the prevention of cybercrime.

E. Study Selection

To select the most relevant studies, exclusion criteria were applied to ensure that the papers selected were relevant to the research. Quality criteria were then applied to ensure that the papers selected provided solutions and answers to the research questions. See Fig. 3.

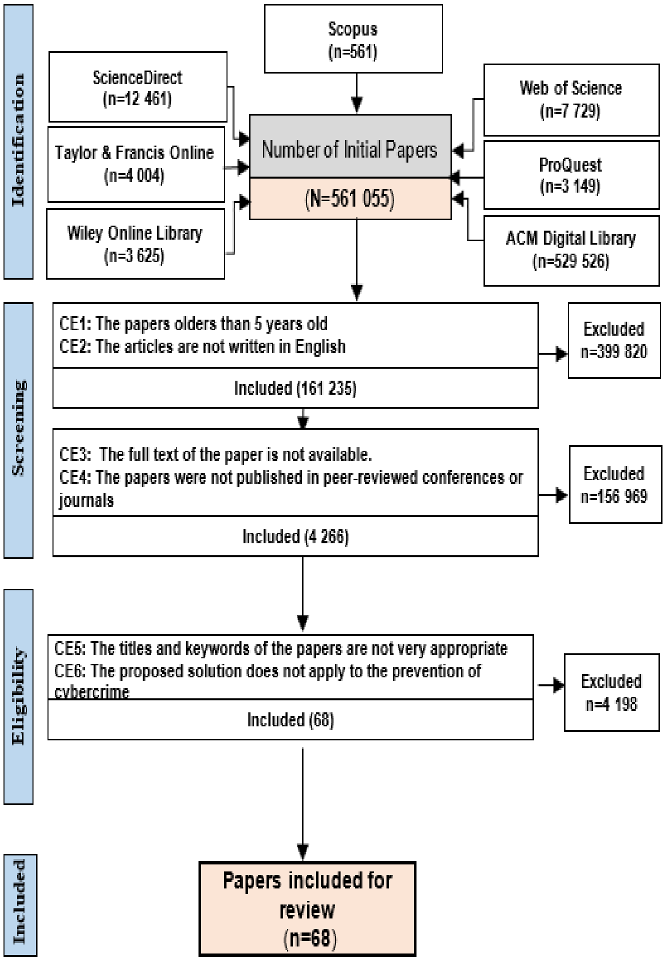

Identification
Screening
Eligibility
Included
Scopus
(n=561)
ScienceDirect
(n=12 461)
Web of Science
(n=7 729)
Number of Initial Papers
(N=561 055)
Taylor & Francis Online
(n=4 004)
ProQuest
(n=3 149)
Wiley Online Library
(n=3 625)
ACM Digital Library
(n=529 526)
CE1: The papers olders than 5 years old
CE2: The articles are not written in English
Included (161 235)
Excluded
n=399 820
CE3: The full text of the paper is not available.
CE4: The papers were not published in peer-reviewed conferences or journals
Included (4 266)
Excluded
n=156 969
CE5: The titles and keywords of the papers are not very appropriate
CE6: The proposed solution does not apply to the prevention of cybercrime
Included (68)
Excluded
n=4 198
Papers included for review
(n=68)

Fig. 3. PRISMA Flowchart.

F. Quality Assessment

As a final step for the selection of the papers, four quality criteria (QA) were applied, with the aim of selecting papers that are of quality for the literature review. Quality criteria used:

QA1. Is the purpose of the research clearly explained?

QA2. Is the research methodology clearly explained?

QA3. Is the specific subject area used clearly defined?

QA4. Are the results of the experiments performed clearly identified and reported?

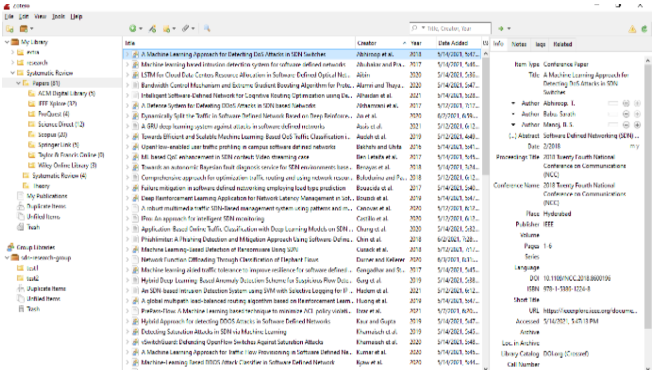
These rules were applied to identify the final list of research papers reviewed. After the evaluation of the 4 QAs to the 68 papers, it was determined that all of them had met the quality criteria.

G. Data Extraction Strategy

Once the final list of papers was obtained, the necessary information was extracted to support and answer the research questions.

The information extracted from the papers were the following: Article ID, title of the paper, URL, source, Country, Number of pages, language, type of publication, authors, affiliation, number of citations, abstract, keywords, sample size.

The Mendeley tool was used to manage the papers, as shown in Fig. 4.



Title	Creator	Year	Date Added
A Machine Learning Approach for Detecting DoS Attacks in SDN Switches	Abhiroop et al.	2018	5/14/2021, 5:47...
Machine learning based intrusion detection system for software defined networks	Abubakar and Pra...	2017	5/14/2021, 5:46...
LSTM for Cloud Data Centers Resource Allocation in Software-Defined Optical Net...	Aibin	2020	5/14/2021, 5:36...
Bandwidth Control Mechanism and Extreme Gradient Boosting Algorithm for Prote...	Alamri and Thaya...	2020	5/14/2021, 5:47...
Intelligent Software-Defined Network for Cognitive Routing Optimization using De...	Alhaidan et al.	2021	5/14/2021, 5:28...
A Defense System for Defeating DDoS Attacks in SDN based Networks	Alshamrani et al.	2017	5/12/2021, 7:17...
Dynamically Split the Traffic in Software Defined Network Based on Deep Reinforce...	An et al.	2020	6/2/2021, 6:59...
A GRU deep learning system against attacks in software defined networks	Assis et al.	2021	5/12/2021, 6:12...
Towards Efficient and Scalable Machine Learning-Based QoS Traffic Classification i...	Audah et al.	2019	5/12/2021, 4:40...
OpenFlow-enabled user traffic profiling in campus software defined networks	Bakhshi and Ghita	2016	5/14/2021, 5:41...
ML based QoE enhancement in SDN context: Video streaming case	Ben Letaifa et al.	2017	5/14/2021, 5:45...
Towards an autonomic Bayesian fault diagnosis service for SDN environments base...	Benayas et al.	2018	5/14/2021, 3:24...
Comprehensive approach for optimization traffic routing and using network resour...	Boldurina and Pa...	2018	5/12/2021, 6:12...
Failure mitigation in software defined networking employing load type prediction	Bouacida et al.	2017	5/14/2021, 5:40...
Deep Reinforcement Learning Application for Network Latency Management in Sof...	Bouzidi et al.	2019	5/14/2021, 5:47...
A robust multimedia traffic SDN-Based management system using patterns and m...	Cancuas et al.	2020	5/12/2021, 6:12...
IPro: An approach for intelligent SDN monitoring	Castillo et al.	2020	5/12/2021, 6:12...
Application-Based Online Traffic Classification with Deep Learning Models on SDN...	Chang et al.	2020	5/14/2021, 5:32...
PhishLimiter: A Phishing Detection and Mitigation Approach Using Software-Define...	Chin et al.	2018	6/2/2021, 7:28...
Machine Learning-Based Detection of Ransomware Using SDN	Cusack et al.	2018	5/12/2021, 6:17...
Network Function Offloading Through Classification of Elephant Flows	Durner and Kellerer	2020	6/3/2021, 6:11...
Machine learning aided traffic tolerance to improve resilience for software defined...	Gangadhar and St...	2017	5/14/2021, 5:45...
Hybrid Deep Learning-Based Anomaly Detection Scheme for Suspicious Flow Dete...	Garg et al.	2019	5/14/2021, 5:38...
An SDN-based Intrusion Detection System using SVM with Selective Logging for IP ...	Hadem et al.	2021	5/12/2021, 6:12...
A global multipath load-balanced routing algorithm based on Reinforcement Learn...	Huang et al.	2019	5/14/2021, 5:47...
PrePass-Flow: A Machine Learning based technique to minimize ACL policy violati...	Ibrar et al.	2021	5/7/2021, 6:20...
Hybrid Approach for detecting DDOS Attacks in Software Defined Networks	Kaur and Gupta	2019	5/14/2021, 5:47...
Detecting Saturation Attacks in SDN via Machine Learning	Khamaiseh et al.	2019	5/14/2021, 5:45...
vSwitchGuard: Defending OpenFlow Switches Against Saturation Attacks	Khamaiseh et al.	2020	5/14/2021, 5:48...
A Machine Learning Approach for Traffic Flow Provisioning in Software Defined Ne...	Kumar et al.	2020	5/14/2021, 5:45...
Machine-Learning Based DDOS Attack Classifier in Software Defined Network	Kyaw et al.	2020	5/14/2021, 5:44...

Item Type: Conference Paper
Title: A Machine Learning Approach for Detecting DoS Attacks in SDN Switches
Author: Abhiroop, T.
Author: Babu, Sarath
Author: Manoj, B. S.
(...) Abstract: Software Defined Networking (SDN) ...
Date: 2/2018 m y
Proceedings Title: 2018 Twenty Fourth National Conference on Communications (NCC)
Conference Name: 2018 Twenty Fourth National Conference on Communications (NCC)
Place: Hyderabad
Publisher: IEEE
Volume:
Pages: 1-6
Series:
Language:
DOI: 10.1109/NCC.2018.8600196
ISBN: 978-1-5386-1224-8
Short Title:
URL: https://ieeexplore.ieee.org/docume...
Accessed: 5/14/2021, 5:47:13 PM
Archive:
Loc. in Archive:
Library Catalog: DOI.org (Crossref)
Call Number:

Fig. 4. Document Management with Mendeley.

H. Summary of Findings

The data extracted to answer the research questions were tabulated as quantitative data where an in-depth analysis of the data was performed in order to answer each research question, also allowing statistical comparisons between all findings per research question.

IV. Results and Discussion

A. General Description of the Studies

The 68 papers selected were processed and the necessary information was extracted. Table IV shows the two types of publications used in the reviewed research: 66 were published in Journals and 2 in Conferences.

The authors Meneses, Silva & Colaço [74], also considered two types of publications for their research: Journal with 29% and Conference with 71%.

Other authors considered more types of publications, for example: Hijji & Alam [75], considered seven types of publications for their research of 52 documents such as: (Journals: 23.1%, Conferences / Workshops: 1.9%, White papers: 17.3%, Report articles: 19.2%, websites: 21.2%, blogs: 13.5% and News report: 3.8%).

Likewise, Cascavilla, Tamburri & Van [76], for their research considered three types of sources: Workshop, Conference and Journal.

TABLE IV. Sources and Search Equations

Type of Publication	N° Papers
Journal	66
Conference	2
Total	**68**

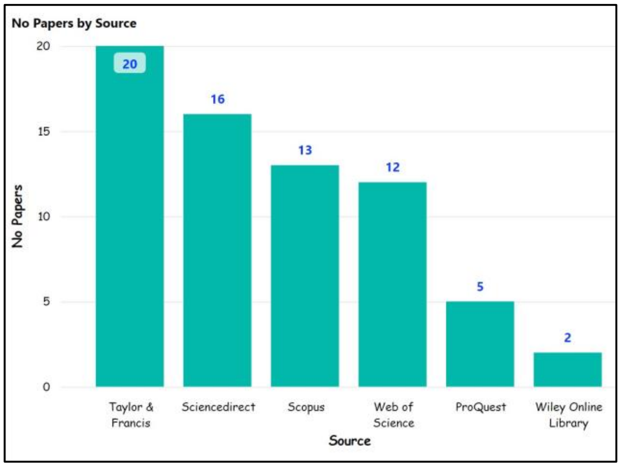


Fig. 5. Papers by Source.

Fig. 5 shows the number of articles selected by type of source, where it can be seen that Taylor & Francis contributed 20 papers, while ScienceDirect contributed 16 papers, followed by Scopus with 13 papers, Web of Science with 12 papers, ProQuest with 5 papers and Wiley Online Library with 2 papers.

For the present study, seven types of important sources were initially considered, but after applying the exclusion criteria, six types of sources were left.

Other authors such as Meneses, Silva & Colaço [74] considered five types of sources to search for the papers of their research on the detection of new fraudulent intelligences: ACM, Engineering Village, IEEE, Scopus and Web of Science.

Fig. 6 shows the 68 papers selected for SLR grouped by country. It can be seen that United Kingdom is the country that publishes the most papers, with 19 papers representing 20.88%, followed by US with 13 papers representing 14.29%.

For the authors Tandon, Kaur, Mäntymäki & Dhir [77], the country that contributed most to their research was the USA with 135 papers followed by the United Kingdom with 82 papers.

For Sonkor, & García de Soto [78], they classify the reviewed publications by country according to 3 categories: (a) Constrution and Cybersecurity (USA with 42%, United Kingdom with 33%, United Arab Emirates with 17% and South Africa with 8%), (b) Constrution and OT (The levels of operational technology) (USA with 20%, Germany with 16%, Hong Kong with 8%, Russia with 8% and others with 48%)and (c) OT and cybersecurity (USA with 18%, China with 12%, Singapore with 9%, United Kingdom with 9%, Australia with 6%, Germany with 6%, Japan with 6% and others with 33%).

B. Answers to Research Questions

RQ1: What are the most commonly used techniques in Cybercrime Prevention investigations?

The results of the literature review found 14 computer crime detection techniques. Which are not necessarily listed in a specific order, the % obtained should be considered to determine which technique is the most applied. Table V shows the computer crime detection techniques.

The most applied techniques are Machine Learning which is found in 19 papers [6], [8], [12], [19], [26], [27], [32], [34], [46], [47], [48], [49], [50], [56], [59], [60], [63], [64] and [68] with 26. 4% of the total, likewise Data Mining is found in 12 papers [6], [23], [27], [34], [47], [48], [49], [50], [54], [55], [61] and [68] with 16.7%.

The authors Al-Khater, Al-Ma'adeed, Ahmed, Sadiq & Khan [6], considered in their research that the detection techniques for computer crimes are: Statistical, Machine Learning (which is divided into Neural (Deep Learning and Fuzzy Logic Neural)), Data Mining and other techniques such as Computer Vision Techniques, Biometric Techniques, Cryptography and Forensics tools. Although the authors classified the techniques in 4 groups, there is agreement with the types of techniques mentioned.

With the authors Meneses, Silva & Colaço [74] do not agree with part of their classification of the detection techniques found, such as: Data Mining and Machine Learning.

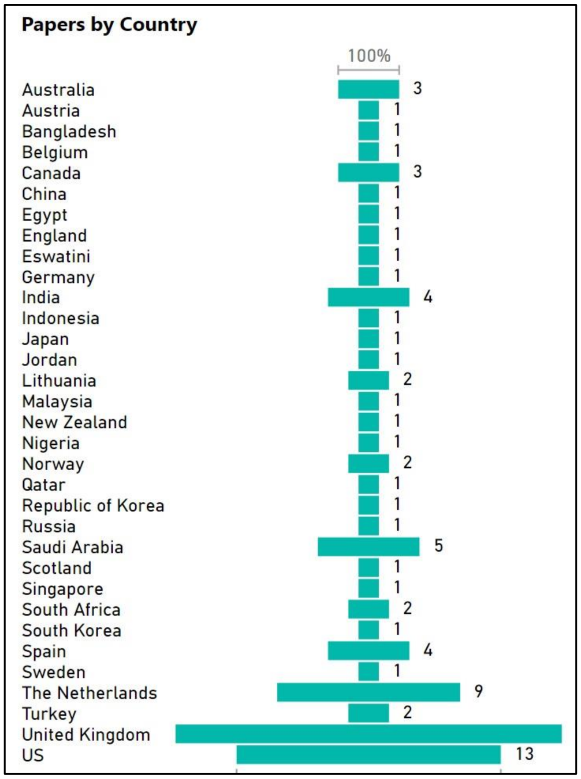


Fig. 6. Papers by Country.

TABLE V. COMPUTER CRIME DETECTION TECHNIQUES

Detection Techniques	**Reference**	**Qty. (%)**
Statistical	[6]	1 (1.4)
Machine Learning	[6] [8] [12] [19] [26] [27] [32] [34] [46] [47] [48] [49] [50] [56] [59] [60] [63] [64][68]	19 (26.4)
Data Mining	[6] [23][27][34][47][48][49][50][54][55] [61][68]	12 (16.7)
Neural network	[6] [26][27][49][50][56][59][68]	8 (11.1)
Deep learning	[6] [27][49][50][59][68]	6 (8.3)
Fuzzy logic neural network	[6]	1 (1.4)
Computer Vision Techniques	[6]	1 (1.4)
Biometric Techniques	[6]	1 (1.4)
Cryptography	[6][11][23][27][38][55][64]	7 (9.7)
Forensics tools	[6][61]	2 (2.8)
Proxies	[34]	1 (1.4)
Firewalls	[2][6][11][23][27][29]38][40][55] [56][62][68]	12 (16.7)
Cyber Liability Insurance	[5]	1 (1.4)

Guo, Cho, Chen, Sengupta, Hong & Mitra [79], considered as data-driven deception detection techniques: data driven, social honeypots, user profile, message content, network structure, early detection, information propagation mitigation and blockchain - based authenticity. Therefore, there is no agreement on any detection technique because the authors more focused on online social deception techniques.

The authors Bangui & Buhnova [80], in their research regarding Machine Learning techniques for intrusion detection, considered the following techniques: Neural networks with 34%, followed by SVM with 20%, Regression techniques with 10%, Learning Automata with 7%, Markov models with 7%, k-means with 7%, Naive Bayes with 7%, Decision Tree with 3%, Random Forest with 3% and K-NN with 3%. There is only agreement on some techniques since the study is more focused on Machine Learning techniques.

Based on the results shown in Table V, it can be inferred that, although the most used techniques are Machine Learning, Data Mining and Neural network, they are applied jointly and with other techniques, such as Deep learning, Fuzzy logic neural network, among others, to obtain better results in Computer Crime Prevention. In this sense, applying these techniques in different organizations and countries, would improve the performance of their computer systems, generating reliability in the organization and reducing maintenance costs.

RQ2: What are the most used Keywords in Mobile Application research and Cybercrime prevention?

According to the results of the literature review, the most used keywords are: cybercrime with 23 repetitions, followed by cybersecurity with 14 repetitions. See Fig. 7 and Fig. 8.

Although the most repeated keywords are Cybercrime and Cybersecurity, it should be emphasized that the word covid-19 conceptually is not related to the research, but as a result of the current situation, it managed to increase computer crimes, and even causing the emergence of new modalities of computer crimes, due to the technological leap worldwide.

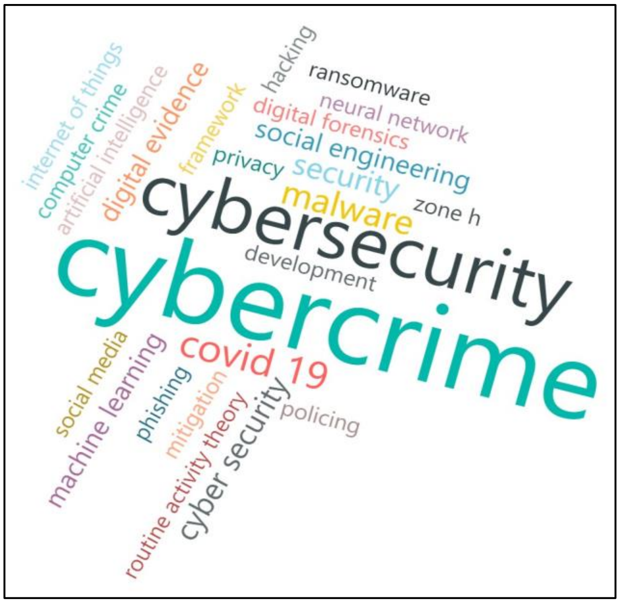


Fig. 7. Keywords Most Frequently Repeated in the Papers.

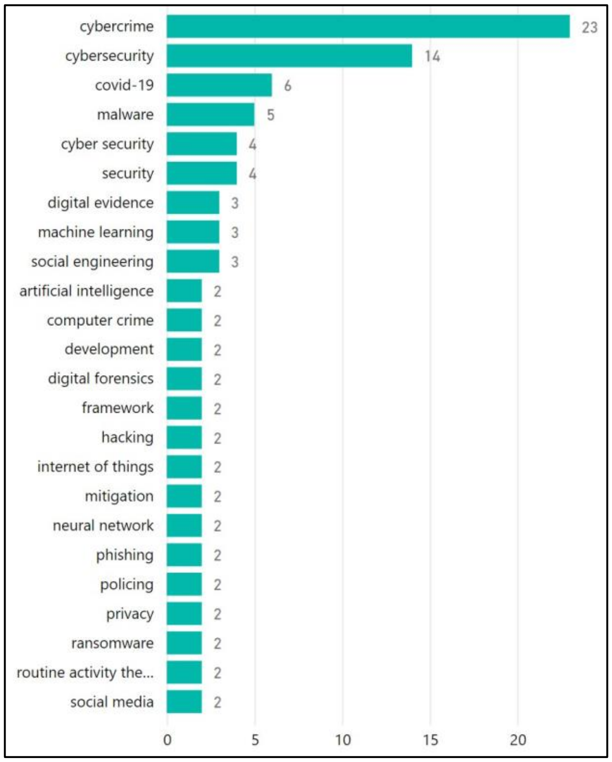


Fig. 8. Number of Keywords in the Papers.

For Tandon, Kaur, Mäntymäki & Dhir [77], in their research regarding the management of computer crimes, considers that the keyword Blockchain is the most used keyword with 311 times in the keywords per author and 138 times per paper. While the research is not closely related to cybercrime it touches on cybercrime issues in parts of the paper.

It can be emphasized that the keywords of this research should be considered in the bibliographic searches regarding Mobile Applications for the prevention of Computer Crimes. They should also be included as keywords in papers produced as a result of experimental research and systematic literature reviews.

RQ3: What are the most cited papers, by country, number of citations and by source in research on mobile applications and cybercrime prevention?

Table VI shows the list of the most cited papers by country, number of citations and source in this study. Of the 68 papers selected for the literature review, the 2 most cited papers are: paper [37] with 67 citations, which was published in ScienceDirect and its author is from United Kingdom, followed by paper [61] with 40 citations which belongs to Web of Science and its author is from Lithuania.

The papers [37, 61], are the most cited, therefore, they are the most relevant of the research. The paper [37] investigated human factors in cyber security, while the paper [61] proposed a tool based on digital evidence object models and habit attribution for computer crime investigation. No other studies with the same research question were found for comparison.

TABLE VI. MOST CITED PAPERS BY COUNTRY AND SOURCE

Ref.	No. Quotations	Country	Source
[37]	67	United Kingdom	ScienceDirect
[61]	40	Lithuania	Web of Science
[57]	39	South Africa	Taylor & Francis
[27]	37	Australia	Scopus
[16]	37	United Kingdom	Taylor & Francis
[25]	34	United Kingdom	Scopus
[44]	29	The Netherlands	Taylor & Francis
[60]	27	Canada	Scopus
[50]	24	Eswatini	ScienceDirect
[45]	24	Japan	Wiley Online L.
[32]	24	United Kingdom	ScienceDirect
[56]	18	United Kingdom	Taylor & Francis
[51]	17	Norway	Taylor & Francis
[42]	17	United Kingdom	Taylor & Francis
[11]	15	The Netherlands	Taylor & Francis
[29]	15	USA	Web of Science
[36]	13	Germany	ProQuest
[64]	11	United Kingdom	Scopus
….	….		
Total	**600**		

Based on what has been reported, it can be concluded that it is necessary to review in detail the papers published in the United Kingdom, Lithuania and South Africa in the experimental studies on Mobile Applications for Cybercrime prevention that will be developed in other countries and in the future.

RQ4: What are the types of computer crimes in the investigations reviewed?

The results of the literature review found 23 types of computer crimes. Which are not necessarily listed in a specific order, the % obtained should be considered to determine which computer crime is most committed by computer criminals. Table VII shows a list of the types of computer crimes.

The types of computer crimes most commonly used by criminal offenders are: Malware present in 39 papers: [1] [2] [3] [4] [5] [6] [7] [9] [12] [15] [16] [21] [22] [23] [24] [25] [26] [29] [32] [33] [34] [35] [40] [42] [43][44] [46] [47] [48] [49] [51] [55] [57] [59] [62] [63] [64] [65] and [68] and represents 14. 2% of the total papers, followed by Phishing found in 31 papers [1] [2] [6] [7] [9] [14] [15] [16] [21] [22] [23] [24] [25] [26] [27] [34] [37] [39] [41] [42] [43] [44] [48] [50] [55] [56] [57] [60] [62] [64] [64] and [68] with 11.3% of the total.

The authors Hijji & Alam [75] in their classification of techniques used for cyber-attacks during the Covid-19 pandemic indicate that the type of computer crime Phishing is the most used with 35.3%, followed by Spam with 16.3%, and among the most important are Scams with 13.7%, Smishing with 12.4%, Extortion with 2.6%, cyberbulling with 2.0% and cyberstalking with 1.3%. It is agreed that Phishing is one of the most used computer crimes.

An & Kim [34], classified computer crimes differently, separating into 2 groups crime articles for services (Phishing, Brute Force attack, DDoS attack, Spamming) and crime articles for products (Drive-by download, Botnet, Exploit, Ransoware, Rootkit and Trojan) do not agree with some of the mentioned types.

For the authors Iakovakis & Xarhoulacos [81], the types of computer crimes produced during Covid-19, are: Phishing with 59%, Malware - Ransomware with 36%, Malicious Domains with 22% and new falsehoods with 14%. According to the results the study agrees that both Phishing and Malware are the most used computer crimes.

Other authors such as Wiafe, Nti, Nyarko, Assyne & Gulliver [70], considered according to publications per year the following computer crimes: Intrusion, encryption and certification, imaging and capcha, phishing, malware, traficc, DoS and others.

Karie, Kebande & Venter [82], consider that the major motivations for attacks are computer crimes with 81.7%, followed by Cyber Espionage with 12.2%, Cyber Warfare with 4.3% and Hacktivism with 1.7%.

TABLE VII. MOST CITED PAPERS BY COUNTRY AND SOURCE

Type of Cybercrime	**Reference**	**Qty. (%)**
Cyber Terrorism	[6] [11] [17] [39] [41] [42]	6 (2.2)
Cyber Warfare	[3] [6] [11] [39]	4 (1.5)
Cyber Espionage	[3] [6] [11] [39]	4 (1.5)
Child Pornography	[2] [6] [9] [19] [30] [41] [50]	7 (2.5)
Cyber Bullying	[6] [10] [43]	3 (1.1)
Cyber Extortion	[23] [42]	2 (0.7)
Cyberstalking	[2] [6] [9] [28] [50] [57] [68]	7 (2.5)
Cyber Fraud / Online Fraud	[2] [6] [9] [10] [16] [22] [28] [30] [33] [43] [53] [57] [65]	13 (4.7)
Phishing	[1] [2] [6] [7] [9] [13] [14] [16] [21] [22] [23] [24] [25] [26] [27] [34] [37] [39] [41] [42] [43] [44] [48][50] [55] [56] [57] [60] [62] [64] [68]	31 (11.3)
Denial of service Attack / DOS	[5] [6] [9] [14] [16] [25] [27] [35] [42] [43] [44] [52] [62]	13 (4.7)
SQL Injection Attack / SQL injection	[5] [6] [7] [27] [66]	5 (1.8)
Malware	[1] [2] [3] [4] [5] [6] [7] [9] [12] [15] [16] [21] [22] [23] [24] [25] [26] [29] [32] [33] [34] [35] [40] [42] [43] [44] [46] [47] [48] [49] [51] [55] [58] [59] [62] [63] [64] [65] [68]	39 (14.2)
Trojans	[6] [9] [15] [24] [34] [57] [59] [64] [68]	9 (3.3)
Identity Theft	[1] [2] [6] [8] [9] [11] [24] [28] [29] [36] [40] [41] [42] [43] [45] [46] [48] [57] [68]	19 (6.9)
Key Logger	[15] [56]	2 (0.7)
Screen Logger	[9]	1 (0.4)
Evil Twin	[9]	1 (0.4)
Botnets	[3] [6] [10] [12] [20] [23] [27] [34] [35] [43] [63][64] [65]	13 (4.7)
Social Engineering	[1] [2] [5] [6] [9] [14] [21] [23] [24] [25] [26] [27] [34] [38] [41] [42] [48] [55] [57] [62] [64] [65] [66]	23 (8.4)
Worms	[3] [6] [9] [27] [56] [57] [59]	7 (2.5)
Ransomware	[1] [5] [14] [15] [20] [21] [23] [24] [25] [27] [29] [31] [32] [34] [35] [38] [41] [43] [47] [48] [51] [55] [57] [59] [60] [64] [67]	27 (9.8)
Hacking	[2] [6] [11] [14] [15] [16] [17] [18] [19] [22] [25] [28] [30] [31] [34] [35] [39] [41] [44] [46] [47] [50] [55] [56] [57] [60] [61] [62] [63] [64]	30 (10.9)
Data breach	[5] [15] [21] [25] [27] [42] [43] [60] [68]	9 (3.3)

Likewise, Guo, Cho, Chen, Sengupta, Hong & Mitra [79], considered according to their classification five groups of computer crimes: False Information (False Newa, rumors, information manipulation, fake reviews), Luring (Phishing, spamming), Fake Identity (fake profile, compromised account, profile cloning attack), Crowdturfing (Crowdturfing), Human targeted attacks (human trafficking, cyberbullying, cybergrooming and cyberstalking).

On the other hand, Senarak [83] considers as a category of computer crimes to: Hacktivism, Cyber criminality, Cyber espionage, Cyber terrorism and Cyber war.

And the author Jeong [71], in his research regarding security threats, crimes and forensic analysis of artificial intelligence, the most committed computer crime is Advanced Computer as Tool Crime.

The detailed identification of types of cybercrime is expected to further accelerate the development of Mobile Applications that enable the prevention of Cybercrime in all business sectors, leading to the emergence of new businesses based on this technology and a booming economy based on data protection.

RQ5: Which Authors are Co-Occurring in Research on Mobile Applications and Cybercrime Prevention?

According to the literature review, authors E. Rutger Leukfeldt and Steve Van de Weijer present three co-occurrences (weight 3). See Fig. 9.

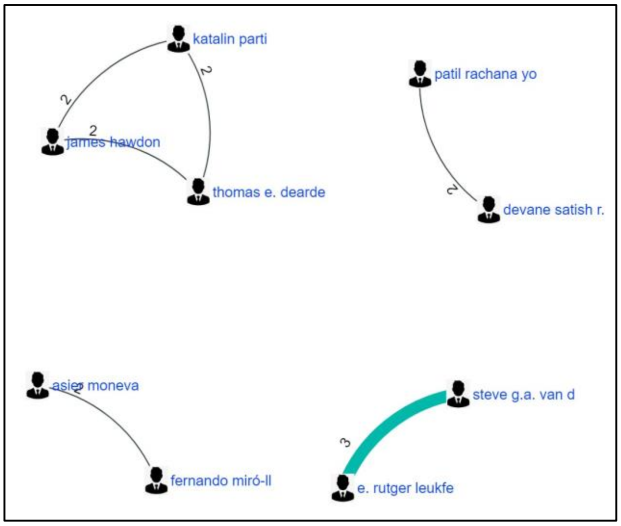


Fig. 9. Co-authorship Bibliometric Network.

While authors E.Rutger Leukfeldt and Steve Van de Weijer are presented together in three papers, it is important to mention that authors James Hawdon, Katalin Parti and Thomas Dearde are presented together in two papers.

For Tandon, Kaur, Mäntymäki & Dhir [77], the author presenting the highest co-occurrence in the selected studies is Wang X. Do not agree with the authors because the research focused more on blockchain.

V. Conclusions and Future Research

This study has managed to identify and analyze which are the most used techniques for the detection of computer crimes, the classification of computer crimes, the most used words in the papers, the most used keywords, the most cited papers and the authors that present cooccurrence in their research based on the research questions posed and analyzed with the systematic literature review between 2017 and 2021 in several databases. The results of the review determine that the most used techniques for the detection of computer crimes are: Statical, Machine Learning, Data Mining, Neural network, Deep learning, Fuzzy logic neural network, Computer Vision Techniques, Biometric Techniques, Cryptography, Forensies tolos, Network Encryption, Proxies, Firewalls and Cyber Liability Insurance. The most used technique is Machine Learning. Likewise, computer crimes were classified as follows: Cyber Terrorism, Cyber Warfare, Cyber Espionage, Child Pornography, Cyber Bullying, Cyber Extortion, Cyber Extortion, Cyberstalking, Cyber Fraud / Online Fraud / Fraud, Cyber Laudering, Phishing, Denial of service Attack, SQL Injection Attack, Malware, Unauthorized System Access, Trojans, Identity Theft, Key Logger, Screen Logger, Evil Twin, Botnets, Social Engineering, Worms, Ransomware, Hacking and Data breach. Few co-authorships were identified among the researchers and very few systematic reviews that made use of bibliometric networks; however, this did not improve the interpretation of the results. Future research should consider a larger number of articles for review and analysis.

References

[1] A. Alzubaidi, “Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia,” Heliyon, vol. 7, no. 1, 2021, doi: 10.1016/j.heliyon.2021.e06016.

[2] N. Akdemir and C. J. Lawless, “Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach,” Internet Res., vol. 30, no. 6, pp. 1665–1687, 2020, doi: 10.1108/INTR-10-2019-0400.

[3] A. Claver, “Governance of cyber warfare in the Netherlands: an exploratory investigation,” Int. J. Intell. Secur. Public Aff., vol. 20, no. 2, pp. 155–180, 2018, doi: 10.1080/23800992.2018.1484235.

[4] R. I. Dremliuga and A. I. Korobeev, “Trends and Methods of Fighting Cybercrime in the Russian Federation in Terms of the Transition to a Digital Economy,” vol. 7, pp. 191–200, 2021.

[5] A. M. Algarni, V. Thayananthan, and Y. K. Malaiya, “Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems,” Appl. Sci., vol. 11, no. 8, 2021, doi: 10.3390/app11083678.

[6] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, “Comprehensive review of cybercrime detection techniques,” IEEE Access, vol. 8, pp. 137293–137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[7] A. Moneva, E. R. Leukfeldt, S. G. A. Van De Weijer, and F. Miró-Llinares, “Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective,” Comput. Human Behav., vol. 126, no. September 2020, 2022, doi: 10.1016/j.chb.2021.106984.

[8] A. Basuchoudhary and N. Searle, “Snatched secrets: Cybercrime and trade secrets modelling a firm’s decision to report a theft of trade secrets,” Comput. Secur., vol. 87, 2019, doi: 10.1016/j.cose.2019.101591.

[9] A. Okutan and Y. Çebi, “A Framework for Cyber Crime Investigation,” Procedia Comput. Sci., vol. 158, pp. 287–294, Jan. 2019, doi: 10.1016/J.PROCS.2019.09.054.

[10] Benoît Dupont, “Enhancing the effectiveness of cybercrime prevention through policy monitoring,” J. Crime Justice, 42 (5), 500-515., vol. 42, pp. 500–515, 2019, doi: 10.1080/0735648X.2019.1691855.Abstract.

[11] B. van den Berg and E. Keymolen, “Regulating security on the Internet: control versus trust,” Int. Rev. Law, Comput. Technol., vol. 31, no. 2, pp. 188–205, 2017, doi: 10.1080/13600869.2017.1298504.

[12] C. Cilleruelo, Enrique-Larriba, L. De-Marcos, and J. J. Martinez-Herraiz, “Malware Detection Inside App Stores Based on Lifespan Measurements,” IEEE Access, vol. 9, pp. 119967–119976, 2021, doi: 10.1109/ACCESS.2021.3107903.

[13] C. Cross, “Dissent as cybercrime: social media, security and development in Tanzania,” J. East. African Stud., vol. 15, no. 3, pp. 442–463, 2021, doi: 10.1080/17531055.2021.1952797.

[14] C. Joyce, F. L. Roman, B. Miller, J. Jeffries, and R. C. Miller, “Emerging Cybersecurity Threats in Radiation Oncology,” Adv. Radiat. Oncol., vol. 6, no. 6, p. 100796, 2021, doi: 10.1016/j.adro.2021.100796.

[15] C. Harfield and J. Schofield, “(Im)material culture: towards an archaeology of cybercrime,” World Archaeol., vol. 52, no. 4, pp. 607–618, 2020, doi: 10.1080/00438243.2021.1882333.

[16] D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, and N. Díaz-Castaño, “Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK,” Eur. Soc., vol. 23, no. S1, pp. S47–S59, 2021, doi: 10.1080/14616696.2020.1804973.

[17] D. Broeders, F. Cristiano, and D. Weggemans, “Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy,” Stud. Confl. Terror., vol. 0, no. 0, pp. 1–28, 2021, doi: 10.1080/1057610X.2021.1928887.

[18] D. S. W. Wong and S. F. Fung, “Development of the cybercrime rapid identification tool for adolescents,” Int. J. Environ. Res. Public Health, vol. 17, no. 13, pp. 1–13, 2020, doi: 10.3390/ijerph17134691.

[19] D. Johnson, E. Faulkner, G. Meredith, and T. J. Wilson, “Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts,” J. Crim. Law, vol. 84, no. 5, pp. 427–450, 2020, doi: 10.1177/0022018320952559.

[20] D. Anagnostakis, “The European Union-United States cybersecurity relationship: a transatlantic functional cooperation,” J. Cyber Policy, vol. 6, no. 2, pp. 243–261, 2021, doi: 10.1080/23738871.2021.1916975.

[21] E. Ventrella, “Privacy in emergency circumstances: data protection and the COVID-19 pandemic,” ERA Forum, vol. 21, no. 3, pp. 379–393, 2020, doi: 10.1007/s12027-020-00629-3.

[22] E. R. Leukfeldt and T. J. Holt, “Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals,” Comput. Human Behav., vol. 126, no. February 2021, p. 106979, 2022, doi: 10.1016/j.chb.2021.106979.

[23] E. Kalaimannan, S. K. John, T. DuBose, and A. Pinto, “Influences on ransomware’s evolution and predictions for the future challenges,” J. Cyber Secur. Technol., vol. 1, no. 1, pp. 23–31, 2017, doi: 10.1080/23742917.2016.1252191.

[24] F. E. Eboibi, “Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures,” Commonw. Law Bull., vol. 47, no. 1, pp. 113–142, 2021, doi: 10.1080/03050718.2020.1834424.

[25] 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, no. January, pp. 7152–7169, 2021, doi: 10.1109/ACCESS.2020.3048839.

[26] H. Ahmad and L. Erdodi, “Overview of phishing landscape and homographs in Arabic domain names,” Secur. Priv., vol. 4, no. 4, pp. 1–14, 2021, doi: 10.1002/spy2.159.

[27] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, “Cybersecurity data science: an overview from machine learning perspective,” J. Big Data, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.

[28] T. E. Dearden, K. Parti, and J. Hawdon, “Institutional Anomie Theory and Cybercrime—Cybercrime and the American Dream, Now Available Online,” J. Contemp. Crim. Justice, vol. 37, no. 3, pp. 311–332, 2021, doi: 10.1177/10439862211001590.

[29] J. Hawdon, K. Parti, and T. E. Dearden, “Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment,” Am. J. Crim. Justice, vol. 45, no. 4, pp. 546–562, 2020, doi: 10.1007/s12103-020-09534-4.

[30] J. A. M. Schiks, S. G. A. van de Weijer, and E. R. Leukfeldt, “High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals,” Comput. Human Behav., vol. 126, no. July 2021, p. 106985, 2022, doi: 10.1016/j.chb.2021.106985.

[31] J. Burton and C. Lain, “Desecuritising cybersecurity: towards a societal approach,” J. Cyber Policy, vol. 5, no. 3, pp. 449–470, 2020, doi: 10.1080/23738871.2020.1856903.

[32] J. S. Atkinson, J. E. Mitchell, M. Rio, and G. Matich, “Your WiFi is leaking: What do your mobile apps gossip about you?,” Futur. Gener. Comput. Syst., vol. 80, pp. 546–557, 2018, doi: 10.1016/j.future.2016.05.030.

[33] J. Herrero, A. Torres, P. Vivas, A. Hidalgo, F. J. Rodríguez, and A. Urueña, “Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user’s dual vulnerability model of cybercrime victimization,” Int. J. Environ. Res. Public Health, vol. 18, no. 7, 2021, doi: 10.3390/ijerph18073763.

[34] J. An and H. W. Kim, “A Data Analytics Approach to the Cybercrime Underground Economy,” IEEE Access, vol. 6, pp. 26636–26652, 2018, doi: 10.1109/ACCESS.2018.2831667.

[35] K. K. e Silva, “Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting?,” Int. Rev. Law, Comput. Technol., vol. 32, no. 1, pp. 21–36, 2018, doi: 10.1080/13600869.2018.1418142.

[36] L. Studen and V. Tiberius, “Social media, quo vadis? Prospective development and implications,” Futur. Internet, vol. 12, no. 9, 2020, doi: 10.3390/FI12090146.

[37] L. Hadlington, “Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours,” Heliyon, vol. 3, no. 7, p. e00346, 2017, doi: 10.1016/j.heliyon.2017.e00346.

[38] L. Y. Connolly and D. S. Wall, “The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures,” Comput. Secur., vol. 87, 2019, doi: 10.1016/j.cose.2019.101568.

[39] L. Maschmeyer, R. J. Deibert, and J. R. Lindsay, “A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society,” J. Inf. Technol. Polit., vol. 18, no. 1, pp. 1–20, 2021, doi: 10.1080/19331681.2020.1776658.

[40] M. Solihat and R. V Wulansari, “Internet of Things Cyber Security in Digital Era,” IOP Conf. Ser. Mater. Sci. Eng., vol. 1158, no. 1, p. 012017, 2021, doi: 10.1088/1757-899x/1158/1/012017.

[41] M. M. Singh and A. A. Bakar, “A systemic cybercrime stakeholders architectural model,” Procedia Comput. Sci., vol. 161, pp. 1147–1155, 2019, doi: 10.1016/j.procs.2019.11.227.

[42] M. Camillo, “Cyber risk and the changing role of insurance,” J. Cyber Policy, vol. 2, no. 1, pp. 53–63, 2017, doi: 10.1080/23738871.2017.1296878.

[43] M. Riek and R. Böhme, “The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates†,” J. Cybersecurity, vol. 4, no. 1, pp. 1–16, 2018, doi: 10.1093/cybsec/tyy004.

[44] M. Weulen Kranenbarg, T. J. Holt, and J. L. van Gelder, “Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap,” Deviant Behav., vol. 40, no. 1, pp. 40–55, 2019, doi: 10.1080/01639625.2017.1411030.

[45] M. G. Umlauf and Y. Mochizuki, “Predatory publishing and cybercrime targeting academics,” Int. J. Nurs. Pract., vol. 24, pp. 1–7, 2018, doi: 10.1111/ijn.12656.

[46] M. L. Williams, M. Levi, P. Burnap, and R. V. Gundur, “Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory,” Deviant Behav., vol. 40, no. 9, pp. 1119–1131, 2019, doi: 10.1080/01639625.2018.1461786.

[47] M. L. Han, B. Il Kwak, and H. K. Kim, "CBR-Based Decision Support Methodology for Cybercrime Investigation: Focused on the Data-Driven Website Defacement Analysis," Secur. Commun. Networks, vol. 2019, 2019, doi: 10.1155/2019/1901548.

[48] M. M. Ahsan Pritom, K. M. Schweitzer, R. M. Bateman, M. Xu, and S. Xu, "Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses," Proc. - 2020 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2020, no. i, 2020, doi: 10.1109/ISI49825.2020.9280539.

[49] M. Alazab, "Automated malware detection in mobile app stores based on robust feature generation," Electron., vol. 9, no. 3, 2020, doi: 10.3390/electronics9030435.

[50] N. M. Karie, V. R. Kebande, and H. S. Venter, "Diverging deep learning cognitive computing techniques into cyber forensics," Forensic Sci. Int. Synerg., vol. 1, pp. 61–67, 2019, doi: 10.1016/j.fsisyn.2019.03.006.

[51] N. N. Schia, "The cyber frontier and digital pitfalls in the Global South," Third World Q., vol. 39, no. 5, pp. 821–837, 2018, doi: 10.1080/01436597.2017.1408403.

[52] P. R. Yogesh and R. Devane Satish, "Formal Verification of Secure Evidence Collection Protocol using BAN Logic and AVISPA," Procedia Comput. Sci., vol. 167, no. 2019, pp. 1334–1344, 2020, doi: 10.1016/j.procs.2020.03.449.

[53] P. R. Yogesh and R. Devane Satish, "Backtracking Tool Root-Tracker to Identify True Source of Cyber Crime," Procedia Comput. Sci., vol. 171, no. 2019, pp. 1120–1128, 2020, doi: 10.1016/j.procs.2020.04.120.

[54] P. Sharma, D. Arora, and T. Sakthivel, "Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications," Procedia Comput. Sci., vol. 167, no. 2019, pp. 907–917, 2020, doi: 10.1016/j.procs.2020.03.390.

[55] R. A. Ramadan, B. W. Aboshosha, J. S. Alshudukhi, A. J. Alzahrani, A. El-Sayed, and M. M. Dessouky, "Cybersecurity and Countermeasures at the Time of Pandemic," J. Adv. Transp., vol. 2021, no. 2003, 2021, doi: 10.1155/2021/6627264.

[56] K. M. Rajasekharaiah, C. S. Dule, and E. Sudarshan, "Cyber Security Challenges and its Emerging Trends on Latest Technologies," IOP Conf. Ser. Mater. Sci. Eng., vol. 981, no. 2, 2020, doi: 10.1088/1757-899X/981/2/022062.

[57] R. Naidoo, "A multi-level influence model of COVID-19 themed cybercrime," Eur. J. Inf. Syst., vol. 29, no. 3, pp. 306–321, 2020, doi: 10.1080/0960085X.2020.1771222.

[58] R. Collett, "Understanding cybersecurity capacity building and its relationship to norms and confidence building measures," J. Cyber Policy, pp. 1–20, 2021, doi: 10.1080/23738871.2021.1948582.

[59] R. Damaševičius, A. Venčkauskas, J. Toldinas, and Š. Grigaliūnas, "Ensemble‐based classification using neural networks and machine learning models for windows pe malware detection," Electron., vol. 10, no. 4, pp. 1–26, 2021, doi: 10.3390/electronics10040485.

[60] S. Hakak, W. Z. Khan, M. Imran, K. K. R. Choo, and M. Shoaib, "Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies," IEEE Access, vol. 8, pp. 124134–124144, 2020, doi: 10.1109/ACCESS.2020.3006172.

[61] Š. Grigaliunas and J. Toldinas, "Habits attribution and digital evidence object models based tool for cybercrime investigation," Balt. J. Mod. Comput., vol. 8, no. 2, pp. 275–292, 2020, doi: 10.22364/BJMC.2020.8.2.05.

[62] S. Horgan, B. Collier, R. Jones, and L. Shepherd, "Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing," J. Crim. Psychol., vol. 11, no. 3, pp. 222–239, 2020, doi: 10.1108/JCP-08-2020-0034.

[63] S. Piasecki, L. Urquhart, and P. D. McAuley, "Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards," Comput. Law Secur. Rev., vol. 42, p. 105542, 2021, doi: 10.1016/j.clsr.2021.105542.

[64] S. Broadhead, "The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments," Comput. Law Secur. Rev., vol. 34, no. 6, pp. 1180–1196, 2018, doi: 10.1016/j.clsr.2018.08.005.

[65] S. Ambore, C. Richardson, H. Dogan, E. Apeh, and D. Osselton, "A resilient cybersecurity framework for Mobile Financial Services (MFS)," J. Cyber Secur. Technol., vol. 1, no. 3–4, pp. 202–224, 2017, doi: 10.1080/23742917.2017.1386483.

[66] S. G. A. van de Weijer, T. J. Holt, and E. R. Leukfeldt, "Heterogeneity in trajectories of cybercriminals: A longitudinal analyses of web defacements," Comput. Hum. Behav. Reports, vol. 4, no. June, p. 100113, 2021, doi: 10.1016/j.chbr.2021.100113.

[67] T. Stevens and K. O'brien, "Brexit and cyber security," RUSI J., vol. 164, no. 3, pp. 22–30, 2019, doi: 10.1080/03071847.2019.1643256.

[68] Y. E. Suzuki and S. A. S. Monroy, "Prevention and mitigation measures against phishing emails: a sequential schema model," Secur. J., no. 0123456789, 2021, doi: 10.1057/s41284-021-00318-x.

[69] B. A. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report EBSE-2007-01. School of Computer Science and Mathematics, Keele University," no. October 2021, p. 2007, 2007.

[70] I. Wiafe, F. Nti Koranteng, E. Nyarko Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, "Artificial Intelligence for Cybersecurity_ A Systematic Mapping of Literature _ Enhanced Reader." .

[71] D. Jeong, "Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues," IEEE Access, vol. 8, pp. 184560–184574, 2020, doi: 10.1109/ACCESS.2020.3029280.

[72] P. Weichbroth and Ł. Łysik, "Mobile Security: Threats and Best Practices," Mob. Inf. Syst., vol. 2020, 2020, doi: 10.1155/2020/8828078.

[73] K. Liu, S. Xu, G. Xu, M. Zhang, D. Sun, and H. Liu, "A Review of Android Malware Detection Approaches Based on Machine Learning," IEEE Access, vol. 8, pp. 124579–124607, 2020, doi: 10.1109/ACCESS.2020.3006143.

[74] C. V. Meneses Silva, R. Silva Fontes, and M. Colaço Júnior, "Intelligent Fake News Detection: A Systematic Mapping," J. Appl. Secur. Res., vol. 16, no. 2, pp. 168–189, 2021, doi: 10.1080/19361610.2020.1761224.

[75] 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, no. January, pp. 7152–7169, 2021, doi: 10.1109/ACCESS.2020.3048839.

[76] G. Cascavilla, D. A. Tamburri, and W. J. Van Den Heuvel, "Cybercrime threat intelligence: A systematic multi-vocal literature review," Comput. Secur., vol. 105, p. 102258, 2021, doi: 10.1016/j.cose.2021.102258.

[77] A. Tandon, P. Kaur, M. Mäntymäki, and A. Dhir, "Blockchain applications in management: A bibliometric analysis and literature review," Technol. Forecast. Soc. Change, vol. 166, no. October 2020, 2021, doi: 10.1016/j.techfore.2021.120649.

[78] M. S. Sonkor and B. García de Soto, "Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective," J. Constr. Eng. Manag., vol. 147, no. 12, 2021, doi: 10.1061/(asce)co.1943-7862.0002193.

[79] Z. Guo, J. H. Cho, I. R. Chen, S. Sengupta, M. Hong, and T. Mitra, "Online Social Deception and Its Countermeasures: A Survey," IEEE Access, vol. 9, pp. 1770–1806, 2021, doi: 10.1109/ACCESS.2020.3047337.

[80] H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: Survey," Procedia Comput. Sci., vol. 184, no. 2019, pp. 877–886, 2021, doi: 10.1016/j.procs.2021.04.014.

[81] G. Iakovakis, C. G. Xarhoulacos, K. Giovas, and D. Gritzalis, "Analysis and Classification of Mitigation Tools against Cyberattacks in COVID-19 Era," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/3187205.

[82] N. M. Karie, V. R. Kebande, and H. S. Venter, "Diverging deep learning cognitive computing techniques into cyber forensics," Forensic Sci. Int. Synerg., vol. 1, pp. 61–67, 2019, doi: 10.1016/j.fsisyn.2019.03.006.

[83] C. Senarak, "Port cybersecurity and threat: A structural model for prevention and policy development," Asian J. Shipp. Logist., vol. 37, no. 1, pp. 20–36, 2021, doi: 10.1016/j.ajsl.2020.05.001.