Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 8, No. 1, February, 2024

Exploring Individuals’ Experiences with Security Attacks: A Text Mining and Qualitative Study

Rabab Ali Abumalloh [1], Mahmud Alrahhal [2], Nahla El-Haggar [3], Albandari Alsumayt [3], Zeyad M. Alfawaer [3], Sumayh S. Aljameel [4]*

[1] Department of Computer Science and Engineering, Qatar University, Doha 2713, Qatar.

[2] Department of Computer Engineering, Institute of Science, Atatürk University, Erzurum, Turkey.

[3] Department of Computer Science, Applied College, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia.

[4] SAUDI ARAMCO Cybersecurity Chair, Computer Science Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia.

Abstract

Cyber-attacks have become increasingly prevalent with the widespread integration of technology into various aspects of our lives. The surge in social media platform usage has prompted users to share their firsthand experiences with cyber-attacks. Despite this, previous literature has not extensively investigated individuals' experiences with these attacks. This study aims to comprehensively explore and analyze the content shared by cyber-attack victims in Saudi Arabia, encompassing text, video, and audio formats. The primary objective is to investigate the factors influencing victims' perceptions of the security risks associated with these attacks. Following data collection, preparation, and cleaning, Latent Dirichlet Allocation (LDA) is employed for topic modeling, shedding light on potential factors impacting victims. Sentiment analysis is then utilized to examine the nuanced negative and positive perceptions of individuals. NVivo is deployed for data inspection, facilitating the presentation of insightful inferences. Hierarchical clustering is implemented to explore distinct clusters within the textual dataset. The study's results underscore the critical importance of spreading awareness among individuals regarding the various tactics employed by cyber attackers.

Keywords:

COVID-19 Outbreak;

Security Attacks;

Qualitative Study;

Text Mining.

Article History:

Received:	08	September	2023
Revised:	16	December	2023
Accepted:	04	January	2024
Published:	01	February	2024

1- Introduction

The extensive integration of World Wide Web technologies into various aspects of human life has facilitated the transition of many application domains to electronic modes of operation [1]. This integration has not been free of risk and entails an increasing rate of security threats [2], with some advanced attacks that are difficult to recognize by normal users. Different types of malicious attacks have been recognized, including crack attempts, Denial of Service (DoS) attacks, or port scans. Users’ perceptions of the level of security presented by a particular service provider refer to “perceived security”. During the COVID-19 crisis, IT has been utilized in conventional and unconventional ways to face unprecedented obstacles. The shift of many services and operations to online modes to allow distance work, shopping, and learning has become unavoidable, in which emerging technologies such as robots, AI applications, cloud computing, drones, chatbots, virtual dashboards, wearable devices, and autonomous systems enable this digital shift. This shift has

[*] **CONTACT**: saljameel@iau.edu.sa

DOI: http://dx.doi.org/10.28991/ESJ-2024-08-01-010

touched several areas of our lives, including the judiciary, healthcare, governance, business, community service, education, and more. For example, in the education field, the sudden shift towards online education during the COVID-19 crisis has influenced millions of learners [3]. In the post-crisis era, individuals continue to embrace these emerging technologies in their lives.

Along with this quick noticeable shift, there is a need for a cyber-safe distance-based environment. Several studies have indicated a significant increase in malware and scam attacks during COVID-19 [4]. As indicated by Shi [5], by March 2020, there was a 600% rise in COVID-19-related phishing attacks. Common gateway interfaces indicated a 30,000% rise in the number of cyber risks, which were linked to the COVID-19 crisis [6]. Between January to April 2020, around 907,000 spam messages, 48,000 malicious URLs, and 737 malware-related incidents, which were linked to the current crisis, were located by Interpol [4]. Saudi Arabia prioritizes cybersecurity and is ranked second among nations in terms of dedication to this topic. However, the country has tremendous difficulty, with 22.5 million cyberattacks per year [7]. As a result, Saudi Arabia has launched a number of cybersecurity efforts, education initiatives, and instructional resources to tackle this problem. Furthermore, the country's cybersecurity abilities are constantly being improved and expanded. There is a call for improving the awareness, education, and knowledge of the end-users [8]. Building upon the survey of 1001 respondents conducted within the UK Department of Trade and Industry, which specifically focused on Information Security Breaches and explored the actions most beneficial for UK businesses in addressing future risks, awareness among end users is of great importance. The majority of respondents (62%) underlined the importance of 'increased public knowledge and awareness regarding information security concerns' [9]. Unfortunately, despite widespread media coverage of security hazards, there is concern over whether end users have the requisite knowledge to protect themselves.

Based on the above discussion, the main aim of this study is to explore individuals' perceptions of security risk through their posted experiences on social media portals. To meet the goal of the study, we retrieved the data from the social media portals, and the LDA was utilized to discover the dimensions of individuals' experiences. Sentiment analysis was utilized to examine the negative and positive perceptions of the individuals. NVivo was deployed to inspect the data and present insightful inferences from it. Heiriricial clustering was implemented to examine the different clusters in the textual data set. The novelty of this study is emphasized through the deployment of a user-based methodology that investigates users' experiences, referring to the content reported by the users themselves. While the literature has traditionally explored perceived security using a quantitative approach [10, 11], this study brings a unique perspective by focusing on qualitative aspects. On the other hand, previous studies examining social media content have often concentrated on specific contexts or areas within the domain of perceived security. In the study by Okey et al. [12], the authors investigated the content posted on social media using LDA and sentiment analysis, but focusing on users' perceptions of the security of the ChatGPT.

To simplify the reading of this study, we present a list of abbreviations used in this study in Table 1. The rest of the study is structured as follows; research background is presented in Section 2, the material and method are displayed in Section 3, the discussion of the results is presented in Section 4, and the conclusion along with practical contributions is presented in Section 5.

Table 1. List of abbreviations

Abbreviation	Full Term
ML	Machine Learning
NLP	Natural language Processing
LDA	Latent Dirichlet Allocation
DoS	Denial of Service
WEF	World Economic Forum
PPE	Personal Protection Equipment
WHO	World Health Organization
KSA	Kingdom of Saudi Arabia
IT	Information Technology

2- Background

2-1- Security Risks and Social Media

The advent of social media portals has enabled easy access to large volumes of data and allowed instant sharing of social data [13]. Social media portals allow users to share their statuses, personal information, interests, locations, ideas, and behaviors. It also enabled the users to reflect on their experiences through the online reviews and ratings that are formed as user-generated content. Day by day, several social media portals are introduced to people, with advanced technologies and high-quality services that are provided, including WhatsApp, Instagram, Facebook, Twitter, and Snapchat. The sharing of such data has many advantages; however, it has imposed several threats in terms of security and privacy aspects [14]. Facebook, Google+, Twitter, LinkedIn, Instagram, WhatsApp, and many other online social networks allow users to create profiles, exchange personal data, and share posts with people all over the globe. All social networks require user data to build their profiles; these profiles entail private data such as names, country of origin, birthdate, email, mobile phone, and other sensitive information. Such a diverse atmosphere attracts attackers for penetrating users' information [15, 16]. With the rapid progress of deep learning and machine learning techniques, attackers have discovered various attribute inference attack approaches, leading to information leakage and posing a threat to social media confidentiality [17, 18]. For example, tweets from users can be used in machine-learning models to identify users' information, such as location, age, and gender [19].

While the sharing of personal data has become more widespread and convenient, it has also given rise to the disclosure of information that can be exploited for criminal purposes [13]. An integral dimension of social information sharing involves the intersection of social data and location data, where both types of information are divulged concurrently, posing inherent security risks to individuals. The evolution of social media has become intricately connected with various forms of security threats, including fraud attacks, injection flaws, the theft of sensitive data, information leakage, SQL injection attacks, phishing attacks, malware attacks, and more [14]. Within the realm of social media, security risks encompass a spectrum of challenges, ranging from cross-site scripting and injection flaws to information leakage.

Key cyber-attacks can be categorized into Social Engineering, Spear Phishing, and Web Application-related attacks. Social Engineering relies on establishing trust with users to access specific information at both individual and organizational levels. Social media platforms such as Facebook, Twitter, and Instagram facilitate users sharing critical content with their social connections. By gaining the trust of users, malware can be embedded into shared content, deceiving users through malicious links [20]. Spear Phishing attacks target specific types of social media users, attempting to scam them by prompting actions like clicking on links containing malware or opening specific documents [21]. Web Application attacks might entail the access of malicious web applications on users' accounts, which might be granted by the user unintentionally [22].

2-2- Security Attacks and COVID-19

The COVID-19 crisis has been interlinked with diverse types of cyber-attacks and cyber-crimes that have grown in an unpredictable manner. The crisis has caused several implications on the individual's usual activities and implied several types of disruptions over the globe on both the individual and organizational levels, including shifting to a remote-based manner in work and education, boosting the trail activities towards online commerce, and empowering the feelings of fear among community members [4]. The dramatic change in individuals' lives, among which are feelings of anxiety and stress, has increased the number of cyber-attacks in both local and global areas. The reports indicated a rise in the ratios of malware and scam attacks since the beginning of the crisis [23, 24]. According to Shi [5], a 600% growth in the rate of phishing attacks has been indicated by March 2020. Besides, a 50.1% increase in cyber-attacks, as indicated by the World Economic Forum (WEF), along with 30,000 cyber-attacks that are linked to the crisis, were reported in the time interval between December 2019 and April 2020 [25]. Interpol also reported 48,000 malicious URLs, 737 malware-related incidents, and 907,000 spam messages that are linked to the crisis [4]. Interpol also indicated that the *average payment for ransomware in the second quarter of 2020 reached $178,254, with an increase over the first quarter of 60%* [4]. This indicated that cybercriminals perceive a rise in the probability of payout regarding unusual conditions imposed by the pandemic.

Another piece of evidence is presented by the block of 18 million phishing and malware emails that are linked to the pandemic by Google [26]. These attacks were directly related to the marketing activities of products related to the pandemic, such as drugs, test kits, and PPE. Other attacks were related to the stocks' investments or linked to the impersonations of public organizations such as WHO or local governments [27]. An increasing number of cyber-attacks have been detected, including ransomware and phishing-related attacks. It is not obvious whether these attacks originated from the COVID-19 crisis or not. Literature reported difficulty in measuring the growth of the attacks during the crisis in a quantitative manner or the degree to which the pandemic impacted the type of cyber-attacks. The attackers endeavors to utilize the online platforms were obvious during COVID-19, assuming they will persist for a long time. Therefore, many recommendations and instructions were published by local and global organizations to face the increasing risks of attacks. Still, there is a need to get an in-depth understanding of the types of attacks and the best strategies to face them.

2-3- Types of Cyber Security Attacks

The widespread usage of online social networks has resulted in hundreds of millions of social media users. Platforms such as Facebook, Google+, Twitter, LinkedIn, Instagram, WhatsApp, and various others enable users to create profiles, exchange personal data, and share posts with people globally. The diverse nature of these platforms makes them attractive targets for attackers seeking to breach users' information [15]. Social media platforms strive to address privacy concerns by safeguarding users' sensitive data. However, the rapid advancements in deep learning and learning structures have enabled attackers to exploit automatic data attribute implications, leading to information leakage and compromising social media confidentiality [18]. For instance, tweets from users used in machine-learning models can reveal significant information such as user location, age, and gender [19]. Despite the impressive reasoning capacity of machine learning models, they are susceptible to adversarial attacks [28]. By introducing minor disturbances into the data, attackers can easily manipulate misclassification. Given the vulnerabilities in social media confidentiality defense, the issue can be reduced to a potential adversarial attack problem compared to attribute inference attacks. A recent study by Jia and Gong [19] confirmed that adversarial attacks are emerging as defenders against inference attacks. Researchers [29, 30] have detailed various attacks against user-specific applications, such as the device-centric model to minimize attacks on portable malware, allowing network operators to safeguard clients' mobile devices through their mobile networks. These attacks employ different methods, including Intrusion Detection System tools, various operating systems, collected data, designs, and detection standards Chiang & Tsaur [31] explore permission-based techniques and behavioral-based techniques, demonstrating their effectiveness on Android devices and leveraging mobile ecosystems to safeguard against cybercrime. Khan et al. [32] describe a natural biometric mobile ecosystem, outlining mobile device threats, weaknesses, and challenges.

Malware is employed to pilfer personal data, business information, financial details, and other sensitive information for use as valuable data by malicious actors [33]. Malware has been utilized to target government or corporate data for destruction or theft. Subsequently, it is leveraged to compromise individuals' information, such as bank account and credit card numbers, or other critical information for attackers. The primary motive behind malware development has evolved beyond information theft to profit generation [34]. Once malware infiltrates a victim's system, various cyber-attacks can be employed across hardware, software, and networks. Hardware attacks provide attackers with the means to initiate attacks, making them more challenging to detect compared to software attacks, which are typically protected by antivirus and antispyware programs [35, 36].

All social networks necessitate the completion of user profiles, which contain sensitive information such as names, country, birthdate, email, and mobile phone numbers. This information poses a significant risk if accessed by unauthorized entities [37]. However, contemporary social networks often share and publicize private data and real identities, leading to an expansion of privacy concerns across these platforms [38]. Online social media has become a valuable data source for researchers, data analysts, and others who exploit these resources for phishing, spamming, or advertising purposes [39]. The accessibility of data on social network servers raises concerns about user privacy, as these platforms may not be entirely transparent in safeguarding sensitive information [38].

3- Material and Method

This study comprises four main stages. The qualitative data for this research was gathered from social media platforms. We explored various portals that enabled individuals to articulate their experiences with different types of cyber-attacks. The search process was undertaken by two of the authors, and the textual data were subsequently translated and reviewed by another two authors. The video files were also transcribed and translated into English by the authors. We obtained 90 records of textual data expressing various types of cyber-attacks or attempted cyberattacks. The qualitative data reflect the actual experiences of users, as conveyed in their own words. Data cleaning procedures were applied to eliminate unnecessary information from the dataset. We employed the LDA topic modeling technique to extract the main factors and topics from the data. Sentiment analysis was conducted using Orange software. Qualitative data analysis was performed using NVivo to uncover hidden, unorganized information from the data. The research method employed in this study is illustrated in Figure 1.

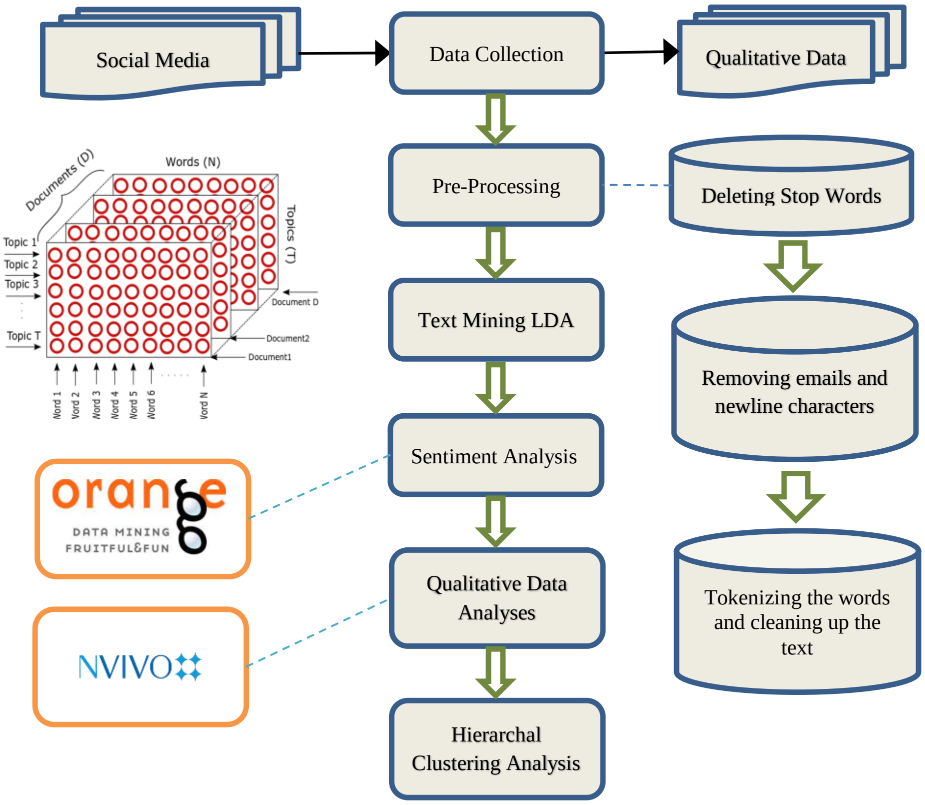
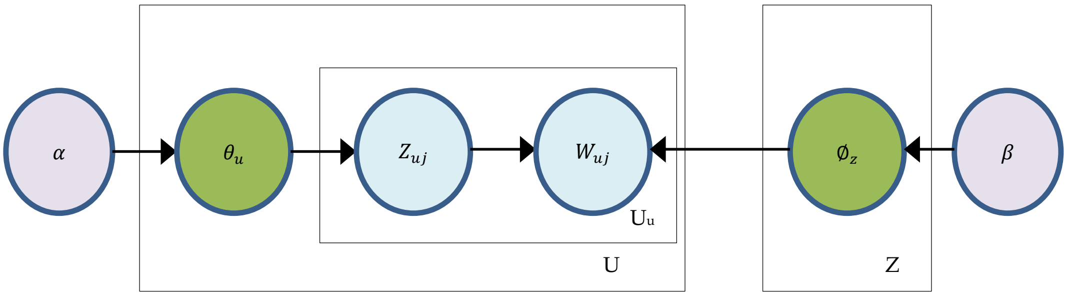


Figure 1. Flowchart of the research methodology

3-1- Deployed Method (LDA)

Topic modeling techniques utilize statistical approaches to analyze unstructured texts and investigate the underlying themes. This is accomplished by organizing the text into a number of topics that reflect its content, typically using LDA. In the LDA technique, the optimal number of topics must be determined. Several studies have indicated that 20 topics provide the best performance [40]. LDA has been employed in text mining studies to explore online reviews and capture customers' perceptions across various research domains, including marketing [41], online education [42], and accommodation business [43]. Figure 2 illustrates the generative model of LDA, while Figure 3 displays a sample word cloud representing the generated topics. Where α is the Dirichlet parameter, θ_u is the topic distribution for document u, Zuj is the sampled topic for the jth word in the uth document, W is the observed word, ∅ is the word distribution for topic Z, and β is the topic hyber parameter.



1. For each topic $z \in Z$
   - Draw a multinomial distribution $\emptyset_z \sim Dir(\vec{\beta})$.
2. For every user $u \in U$,
   - Draw a multinomial distribution$\theta_u \sim Dir(\vec{\propto})$.
   - For every Word $w \in D_u$,

(a) Draw a topic $z \sim Multinomial\left(\underset{\theta_u}{\rightarrow}\right)$.

(b) Draw a word $w \sim Multinomial\left(\underset{\emptyset_z}{\rightarrow}\right)$.

Figure 2. LDA generative procedure

Weight	Word
49	Account
28	Number
28	Link
24	Amount
23	Bank
23	Message
19	Mobile
19	Company
18	Received
18	Call
17	Riyals
17	Person
17	Fake

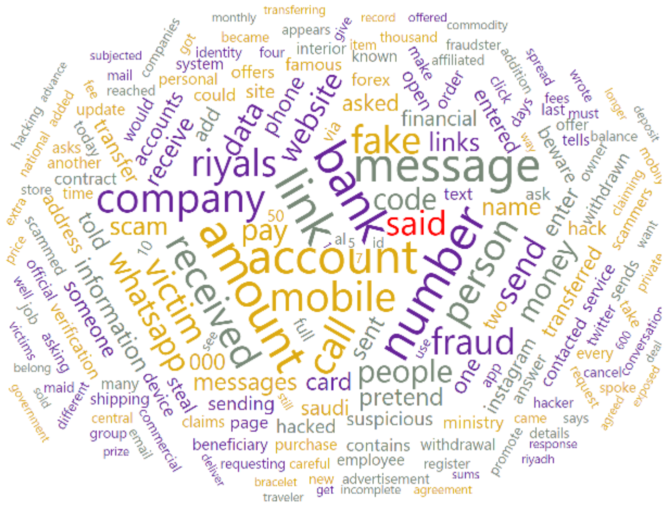
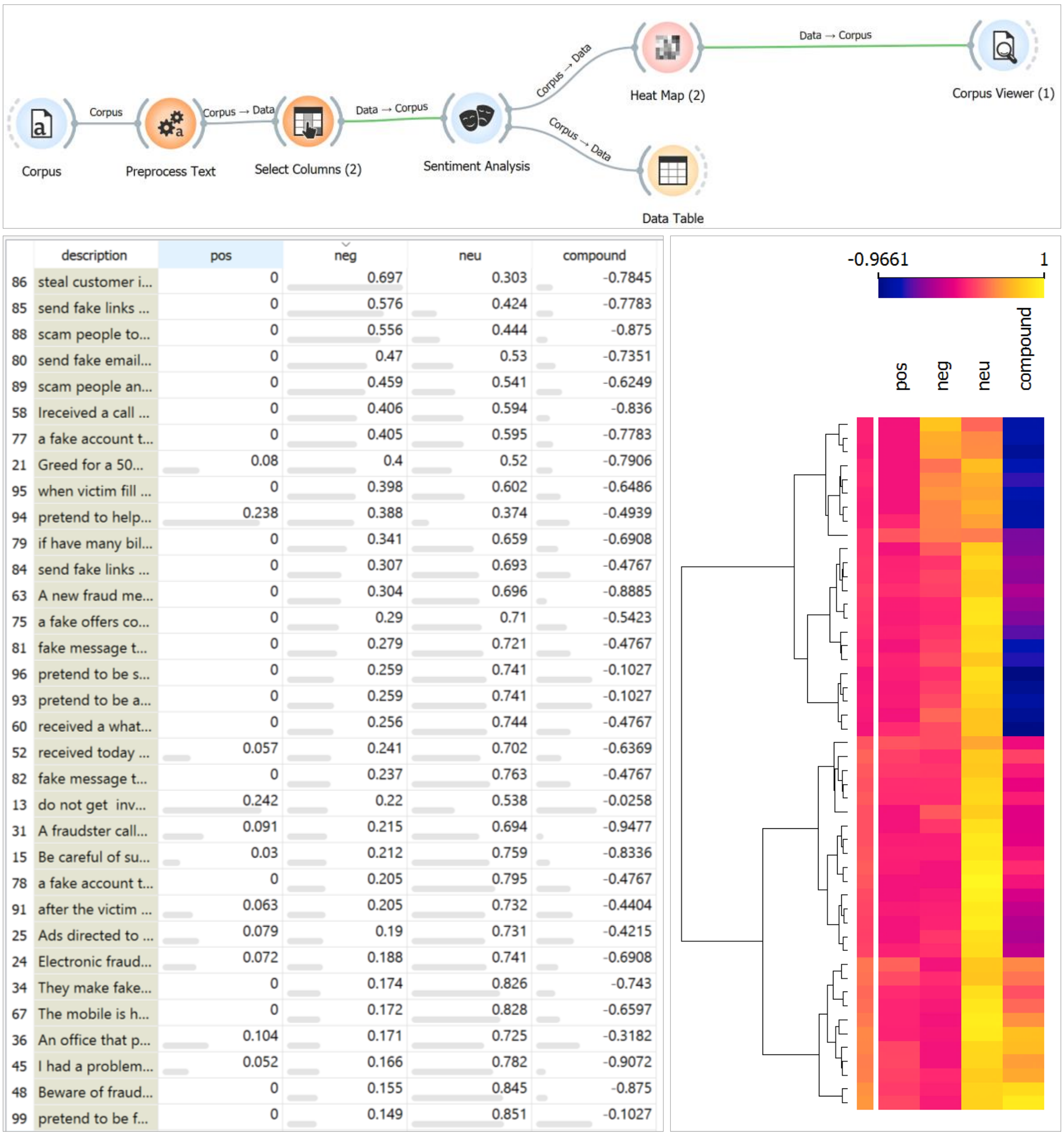


Figure 3. Sample of the word cloud for the generated topic

3-2- Sentiment Analysis

In the subsequent stage, the Orange tool was employed in the data mining process. The Orange tool, an open-source application, facilitates various machine-learning techniques, including text mining. Through visualized workflows, researchers can explore data, identify hidden patterns, classify it, and conduct different types of segmentations [44]. Various types of diagrams, such as histograms, box plots, and scatter plots, are available for visualizing the data. The Orange tool can generate more complex diagrams like tree visualizations, dendrograms, and silhouette plots. The Orange data mining tool empowers researchers to effectively explore the content of textual documents, conduct comparisons within texts, mine keywords, and investigate maps generated from the texts. The initial stage involves data preprocessing to generate tokens. This process includes converting words to lowercase, dividing them into separate words, and removing stopwords. Sentiment analysis predicts sentiments for each textual document. The results of the sentiment analysis are presented in Figure 4.

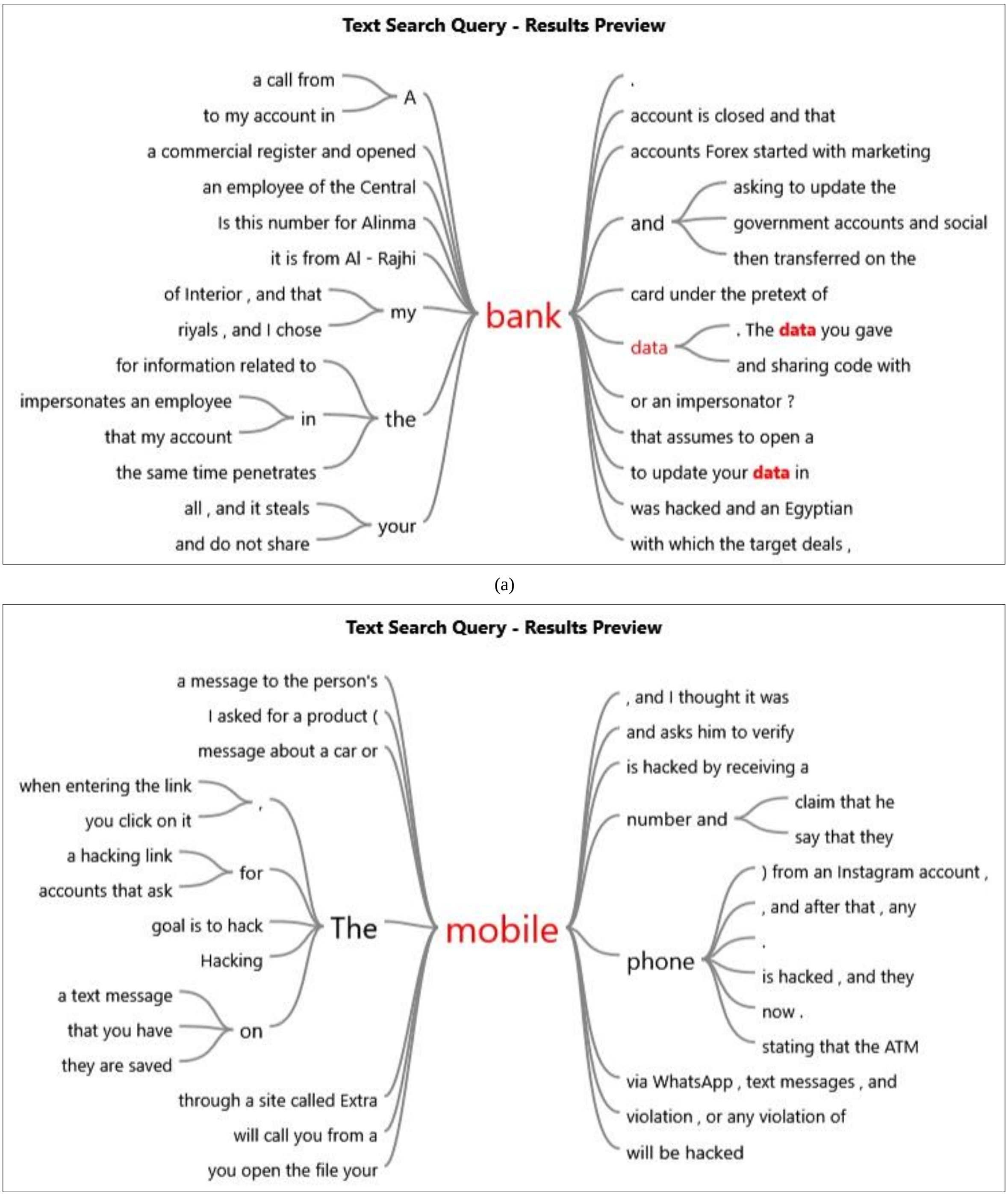


	description	pos	neg	neu	compound
86	steal customer i...	0	0.697	0.303	-0.7845
85	send fake links ...	0	0.576	0.424	-0.7783
88	scam people to...	0	0.556	0.444	-0.875
80	send fake email...	0	0.47	0.53	-0.7351
89	scam people an...	0	0.459	0.541	-0.6249
58	Ireceived a call ...	0	0.406	0.594	-0.836
77	a fake account t...	0	0.405	0.595	-0.7783
21	Greed for a 50...	0.08	0.4	0.52	-0.7906
95	when victim fill ...	0	0.398	0.602	-0.6486
94	pretend to help...	0.238	0.388	0.374	-0.4939
79	if have many bil...	0	0.341	0.659	-0.6908
84	send fake links ...	0	0.307	0.693	-0.4767
63	A new fraud me...	0	0.304	0.696	-0.8885
75	a fake offers co...	0	0.29	0.71	-0.5423
81	fake message t...	0	0.279	0.721	-0.4767
96	pretend to be s...	0	0.259	0.741	-0.1027
93	pretend to be a...	0	0.259	0.741	-0.1027
60	received a what...	0	0.256	0.744	-0.4767
52	received today ...	0.057	0.241	0.702	-0.6369
82	fake message t...	0	0.237	0.763	-0.4767
13	do not get inv...	0.242	0.22	0.538	-0.0258
31	A fraudster call...	0.091	0.215	0.694	-0.9477
15	Be careful of su...	0.03	0.212	0.759	-0.8336
78	a fake account t...	0	0.205	0.795	-0.4767
91	after the victim ...	0.063	0.205	0.732	-0.4404
25	Ads directed to ...	0.079	0.19	0.731	-0.4215
24	Electronic fraud...	0.072	0.188	0.741	-0.6908
34	They make fake...	0	0.174	0.826	-0.743
67	The mobile is h...	0	0.172	0.828	-0.6597
36	An office that p...	0.104	0.171	0.725	-0.3182
45	I had a problem...	0.052	0.166	0.782	-0.9072
48	Beware of fraud...	0	0.155	0.845	-0.875
99	pretend to be f...	0	0.149	0.851	-0.1027

Figure 4. Results of the sentiment analysis

3-3- Nvivo Qualitative Data Analysis

Nvivo is a software that was utilized in this study to investigate the gathered qualitative data. Qualitative data analysis is a methodology that is subjective to the researcher’s judgment and investigates the hidden information from data that might be hard to collect and evaluate. This tool helps in analyzing unstructured data and reveals valuable information from that data. The software not only excels in discerning various data directions and exploring diverse analytical approaches but also in systematically assigning codes to the acquired data [45]. Nvivo is an appropriate software for discovering relevant keynotes, visualizing the data in several patterns, and classifying the data into different categories [46, 47]. In Figure 5, a sample of the Nvivo text search query was provided. Nvivo can reveal patterns from the provided data in a systematic manner and provide visualization of the data in several structures like maps, graphs, and word clouds [48]. Validation can be achieved by several methods, such as inspection of data saturation, research boundaries, and triangulation [49].



(a)

(b)

Figure 5. Sample of Nvivo text search query; (a) Bank as a search keyword, (b) Mobile as a keyword

3-4- Hierarchal Clustering Analysis

The goal of clustering is to categorize provided instances into groups, known as clusters, where instances within the same cluster are maximally similar and those in different clusters are as dissimilar as possible [50]. In this process, each instance is assigned a label indicating its membership in a specific group. While various clustering methods generally share similar principles, they may differ in the techniques used for similarity/distance calculation and label allocation [51]. Hierarchical clustering, as one such approach, endeavors to designate each sample as an individual category [52]. The distance between categories becomes a critical criterion for gauging their similarity. Smaller distances signify greater similarity between categories. Hierarchical clustering amalgamates two akin categories into a new group, and the distance between this merged category and others is measured. This iterative process continues with the calculation of new distances and the merging of similar categories until all comparable categories are unified into a single category. This systematic approach ensures the progressive consolidation of similar categories throughout the clustering process.

4- Discussion

Sentiment analysis has been explored in the literature in several contexts currently, trying to emphasize the perceptions of the end user and understand the user's experience [53, 54]. In the work by Chen et al. [55], the authors used deep learning to analyze emotional cues in earnings conference call audio, finding that positive emotions in statements positively influence analysts' report issuance, negative emotions have the opposite effect, and non-negative emotions in questions and responses positively impact analysts. Another study by Okey et al. [12] has examined ChatGPT users' opinions on cybersecurity using the LDA for topic extraction and sentiment analysis tools. Data from over 700,000 tweets with specific search terms is collected from Twitter. However, in the context of sentiment analysis, the rationale of the study, along with the used data, has a major impact on the results of the study. The specific goal of this study is to explore the perceptions of victims of attacks. The results of our study stressed that victims express fear and detail their experiences to spread awareness. The analysis indicates a strong relationship between negative sentiments and the risk level of the attack. Many victims lack sufficient knowledge about web platform security, making them vulnerable to phishing methods. Surprisingly, attackers often pretend to be cybersecurity specialists, capitalizing on victims' fear of attacks. In one scenario, an attacker poses as a government or bank employee, claiming an attack on the victim's account and requesting information. Strikingly, victims not only provide account information but also the verification security code received on their mobiles, enabling attackers to access and transfer funds easily.

In the collected data, users also reported several types of attacks targeting them for financial gain or personal information. Attackers commonly employ multiple approaches simultaneously to manipulate victims. Despite many victims having a sufficient education level, they fall prey to fraudulent attacks. Methods range from sending emails and making phone calls to deceiving victims through websites developed specifically for fraudulent activities. Victims trust these websites, believing them to be official e-commerce platforms. Attackers also create websites supposedly affiliated with popular e-commerce sites and advertise them on social media platforms. Instances where attackers pretend to be employees of official government or charity organizations are reported, with victims easily providing personal and bank account information. In some cases, attackers send a link to induce victims to click, leading to the hacking of their devices. Attackers may persuade victims to invest in a fraudulent business, ultimately extorting money. Fraud through social media platforms, such as Instagram or Facebook, involves users ordering from pages, transferring money, and subsequently being blocked without receiving the purchased product.

The Nvivo software's data analysis, using specific keywords, allowed the researcher to understand relationships within the textual data. The focus on the keywords "mobile" and "bank" revealed a significant number of attacks conducted through mobile devices, targeting information related to bank accounts. The hierarchical clustering results present nine clusters, which we will elaborate on. Cluster 1 (C1) encompasses instances where individuals experienced issues related to canceled bills and compromised card information. Victims reported incidents involving financial transactions that were either disrupted or involved unauthorized access to their card details. In Cluster 2 (C2), victims reported varied experiences, including missed calls, the receipt of non-original products after purchase, and attempts to update their accounts. These incidents highlight different forms of deceptive practices, ranging from communication tactics to product misrepresentation. Cluster 3 (C3) covers a wide range of fraudulent activities, from warnings about deceptive Snap Ads to impersonation attempts by individuals claiming to be from governmental organizations. The cluster also includes cases of fake services, job offers, and fraudulent links leading to potential security threats. Cluster 4 (C4) focuses on themes related to financial victimization, including several themes such as "green victims", "money theft", and "unauthorized money transfers". Cluster 5 (C5) reveals a multitude of fraudulent schemes, including fake job applications, links, travel offers, WhatsApp groups, courses, charity accounts, competitions, and investments. These incidents involve deceptive practices aimed at extracting personal information or financial resources. Cluster 6 (C6) concentrates on the overarching theme of cybersecurity, reflecting concerns and experiences related to the broader landscape of online security. Cluster 7 (C7) highlights incidents involving Saudi citizenship and experiences with Forex companies, shedding light on specific areas of vulnerability and potential scams targeting individuals. Cluster 8 (C8) focuses on the creation and use of fake accounts, showcasing the prevalence of deceptive online personas. Cluster 9 (C9) encompasses diverse fraudulent activities, including impersonation, fake links related to particular applications such as "Sadad" and "Absher", fake commerce websites, and instances where individuals added beneficiaries for deceptive e-commerce purposes. The cluster illustrates the range of deceptive practices victims encountered across various platforms and scenarios.

5- Conclusions

With recent technological advancements, the proliferation of portable devices, and the widespread use of social media sites like Facebook, Twitter, LinkedIn, and others, where users frequently share sensitive information, many individuals are increasingly vulnerable to security risks. This susceptibility is particularly prevalent among users residing in high-income countries such as Saudi Arabia, who engage in various critical daily activities over the Internet involving personal information, including bank account details and online payment services. Despite the convenience of these web services, they are not entirely secure, and numerous users regularly fall victim to scams and cybersecurity attacks. Cybercrimes are broadly classified into two categories: cyber-dependent and cyber-enabled crimes [4]. The former involves violations achieved through a system or technology [56], while the latter encompasses traditional offenses empowered by the use of systems or technology [56]. The classification can be further subdivided to include hacking, malware, and denial of services for cyber-dependent crimes. In contrast, cyber-enabled crimes include financial fraud, phishing, pharming, and extortion. Often, various types of attacks are interconnected; for instance, a phishing message or email may lead users to a fraudulent portal where their data is collected, or malware is downloaded for financial extortion (Table 2).

Table 2. Types of attacks along with examples from the qualitative data

Type	Definition	Example
Hacking	Act of finding weak points in a network or computer system to access data without permission.	• A call from a fixed phone starting with 011 or 012 from Riyadh or Jeddah. When you reply, the caller tells you that you need to open a file on WhatsApp, and when you open the file, your mobile will be hacked.
Malware	Malicious software is developed to harm and break down computer systems and devices.	• The user is attacked by ransomware, which has spread widely over the past three years, penetrates, and controls the victims' devices, and asks the victim to transfer certain amounts to the hackers.
Denial of services	Cyber-attacks aim to turn off, disorder, or intrude on a website, service, or network.	• A university reported several types of attacks that targeted employees by sending emails to them with malicious attachments.
Financial fraud	Taking property or money from others by criminal or deceptive means.	• Someone contacted me through WhatsApp, posing as an employee in ….. bank and offered me a soft loan. -He asked me to fill out a particular application. • A scammer contacted me as an official account of the delivery company and tried to collect my credit card information. • A fake message with a link to register in a driving training school.
Phishing	Cyber-attacks aim to gain victims' critical information through deception.	• A charity account offers financial assistance, directing the individual to fill in the account information, leading to hacking. • A post from a fake account of a celebrity offers prizes and asks for personal information. • A miscall from the Maldives charges a huge cost for the call. • A fraudulent account steals card information. • A School of driving education offered jobs, and after the applicant fills in the information, online purchases were performed from his bank account. • The attacker pretends to be an employee from the central bank, asking for personal information to investigate a fraud attempt.
Pharming	Similar to phishing, uses malicious code to obtain sensitive information from users.	• You have a package in the postal office, and you need to pay for the delivery fees to receive it within 24 hours. The user has to pay the fees by clicking a link that will direct him to a fraud payment page.
Extortion	A method where the attacker tries to persuade, induce, or intimidate a victim to quit either money or confidential data, or both.	• Fake perfume website sells online but does not send the products to customers. • Start your investment journey with only 150 SR in global companies through the following link.

Saudi Arabia has become a prime target in cyber warfare due to increased economic activities, facilitated by innovation, digital transformation, widespread technology adoption by both individuals and businesses, and the expansion of the oil and gas sector. These economic developments have heightened the vulnerability of Saudi citizens to cyberattacks. Therefore, it is crucial to conduct a thorough study and investigation into the experiences of victims who have suffered from scam attacks. Such an analysis provides decision-makers with valuable insights to enhance citizen awareness of serious cyber threats.

This article presents a case study of security attacks on Saudi organizations and individuals, exploring and analyzing the incidents as described by the victims through various mediums, including text, video, and audio. The investigation encompasses both qualitative and quantitative analyses, involving the application of topic modeling techniques such as LDA and the use of NVivo to analyze unstructured data. Online purchase scams were reported, with users facing issues on platforms like Instagram. They ordered products, transferred money, and then got blocked. Instances of misrepresented products and financial losses were prevalent.

The research yields recommendations for decision-makers in Saudi Arabia to address the escalating security risks, formulate robust cybersecurity strategies, and gain a better understanding of scammers' behaviors toward victims. These recommendations are not only pertinent to decision-makers but also essential for public awareness. Consequently, increased awareness among citizens on protecting themselves from cyberattacks is anticipated. Moreover, promoting security consciousness when dealing with critical data will contribute to a more resilient and cyber-aware society.

5-1- Practical Conclusion

The findings of this research offer recommendations for decision-makers in Saudi Arabia to counter the behaviors of cyber attackers. Scammers employ specific tactics, leveraging social media to illicitly acquire critical information from citizens. This study delves into the experiences of victims who have fallen prey to scammers on various social media platforms. The outcomes contribute to the cyber security literature by analyzing victims' experiences conveyed through text, audio, and video formats. It is crucial to identify the predominant behaviors and methods employed by scammers, particularly within the context of Saudi Arabia. Scammers often adopt impersonation strategies, creating fake accounts on social media to gain the trust of their victims. The deceptive behaviors presented in this study highlight the need to understand these tactics. As gleaned from the results, scammers predominantly exploit popular social media platforms such as WhatsApp, Facebook, Instagram, Twitter, and other modern communication channels. Consequently, social media users in Saudi Arabia, particularly those in critical positions, should be equipped with the latest insights into the methods employed by scammers to safeguard their credentials and finances. Awareness of cybersecurity policies should be heightened, and citizens should exercise caution when dealing with messages and links from unknown or anonymous users. Strengthening national defense capabilities against cybersecurity threats, incorporating recent innovations in recovery plans, and harnessing advancements in AI and quantum computing for implementing security measures against fraudulent content is imperative.

High-level cyber education initiatives must be implemented to mitigate risks and enhance public awareness of the significance of cybersecurity, thereby thwarting the efforts of scammers to exploit citizens. This is crucial in countering evolving online threats, including social engineering, catfishing methods, pharming, and credit card redirection. Additionally, promoting innovations and investments in the domestic cybersecurity industry, coupled with the development of specialized national capacities in cybersecurity disciplines through participation in educational and training programs, is essential. This not only helps establish professional industry standards and secure Saudi cyberspace but also protects citizens lacking the requisite educational background from falling victim to scams. Finally, concerted efforts should be made to achieve the desired level of security by enhancing cybersecurity cooperation with international organizations, supported by sophisticated information exchange mechanisms, thereby increasing security awareness through the sharing of relevant experiences with global institutions.

5-2- Limitations

One limitation of this study is the comparison of our results with previous outcomes. However, we argue that the nature of this study, which relies on the experiences of victims of cyber-attacks as described by the victims, in which we tried to explore these qualitative data, inherently makes direct comparisons challenging. The unique and evolving nature of cyber threats, coupled with the dynamic tactics employed by perpetrators, contributes to a constantly shifting landscape in which no two cyber-attacks are precisely alike. Moreover, the diversity of cyber-attack scenarios captured in our qualitative data, ranging from financial fraud to deceptive online practices, introduces a level of complexity that may not be directly comparable to more narrowly focused studies. Cyber-attacks manifest in various forms, each demanding distinct strategies for prevention and mitigation. Consequently, attempting a direct comparison with previous outcomes may oversimplify the nuanced findings derived from the rich narratives of the victims in our study.

6- Declarations

6-1- Author Contributions

Conceptualization, R.A.A., M.A., and N.E-H.; methodology, R.A.A., M.A., and N.E-H.; software, R.A.A. and M.A.; validation, R.A.A., M.A., N.E-H., A.A., Z.M.A., and S.S.A.; formal analysis, R.A.A. and M.A.; investigation, R.A.A., M.A., and N.E-H.; resources, R.A.A., M.A., N.E-H., and A.A.; data curation, N.E-H., A.A., and Z.M.A.; writing—original draft preparation, R.A.A., M.A., N.E-H., A.A., Z.M.A., and S.S.A.; writing—review and editing, R.A.A.; visualization, M.A.; supervision, R.A.A. and M.A.; project administration, R.A.A.; funding acquisition, S.S.A. and A.A. All authors have read and agreed to the published version of the manuscript.

6-2- Data Availability Statement

Data sharing is not applicable to this article.

6-3- Funding

We would like to thank the SAUDI ARAMCO Cybersecurity Chair for funding this project.

6-4- Institutional Review Board Statement

Not applicable.

6-5- Informed Consent Statement

Not applicable.

6-6- Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

7- References

[1] Horng, S. J., Su, M. Y., Chen, Y. H., Kao, T. W., Chen, R. J., Lai, J. L., & Perkasa, C. D. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. Expert Systems with Applications, 38(1), 306–313. doi:10.1016/j.eswa.2010.06.066.

[2] Songma, S., Chimphlee, W., Songma, S., Chimphlee, W., Maichalernnukul, K., & Sanguansat, P. (2012). Implementation of Fuzzy c-Means and Outlier Detection for Intrusion Detection with KDD Cup 1999 Data Set. International Journal of Engineering Research and Development, 2(2), 44–48.

[3] Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. Computers in Human Behavior, 121, 106791. doi:10.1016/j.chb.2021.106791.

[4] Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248. doi:10.1016/j.cose.2021.102248.

[5] Shi, F. (2020). Threat spotlight: Coronavirus-related phishing. Barracuda Networks: Campbell, United States.

[6] Lush, R. (2020). Helping defend against a 30,000% increase in phishing attacks related to COVID-19 scams. CGI, Brussels, Belgium. Available online: https://www.cgi.com/uk/en-gb/blog/cyber-security/helping-defend-against-a-30000-increase-in-phishing-attacks-related-to-covid-19-scams (accessed on January 2024).

[7] Cyberlands.io. (2024). Top-9 Cybersecurity Breaches in Saudi Arabia. Cyberlands.io, Rotterdam, Netherlands. Available online: https://www.cyberlands.io/topsecuritybreachessaudiarabia (accessed on January 2024).

[8] Aljedaani, B., Ahmad, A., Zahedi, M., & Babar, M. A. (2023). End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers. Journal of Systems and Software, 195, 111519. doi:10.1016/j.jss.2022.111519.

[9] I.S.B.S. (1996). Computer Fraud & Security: Information Security Breaches Survey, 1996, 4. doi:10.1016/s1361-3723(97)82578-x.

[10] Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. International Journal of Information Management, 52, 102063. doi:10.1016/j.ijinfomgt.2019.102063.

[11] Klobas, J. E., McGill, T., & Wang, X. (2019). How perceived security risk affects intention to use smart home devices: A reasoned action explanation. Computers and Security, 87, 101571. doi:10.1016/j.cose.2019.101571.

[12] Okey, O. D., Udo, E. U., Rosa, R. L., Rodríguez, D. Z., & Kleinschmidt, J. H. (2023). Investigating ChatGPT and cybersecurity: A perspective on topic modeling and sentiment analysis. Computers and Security, 135, 103476. doi:10.1016/j.cose.2023.103476.

[13] Tayouri, D. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. Procedia Manufacturing, 3, 1096–1100. doi:10.1016/j.promfg.2015.07.181.

[14] Khalil, L., & Karam, N. A. (2015). Security Management: Real versus Perceived Risk of Commercial Exploitation of Social Media Personal Data. Procedia Computer Science, 65, 304–313. doi:10.1016/j.procs.2015.09.087.

[15] Beigi, G., Shu, K., Zhang, Y., & Liu, H. (2018). Securing Social Media User Data. Proceedings of the 29th on Hypertext and Social Media. doi:10.1145/3209542.3209552.

[16] Yu, S., Vorobeychik, Y., & Alfeld, S. (2018). Adversarial classification on social networks. arXiv Preprint, arXiv:1801.08159. doi:10.48550/arXiv.1801.08159.

[17] Gong, N. Z., & Liu, B. (2018). Attribute inference attacks in online social networks. ACM Transactions on Privacy and Security, 21(1), 1–30. doi:10.1145/3154793.

[18] Jia, J., Wang, B., Zhang, L., & Gong, N. Z. (2017). AttriInfer. Proceedings of the 26th International Conference on World Wide Web. doi:10.1145/3038912.3052695.

[19] Jia, J., & Gong, N. Z. (2018). AttriGuard: A practical defense against attribute inference attacks via adversarial machine learning. Proceedings of the 27th USENIX Security Symposium, 15-17 August, 208, Baltimore, United States.

[20] Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, December, 18.

[21] Jakobsson, M., & Myers, S. (2006). Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons, Hoboken, United States. doi:10.1002/0470086106.

[22] He, W. (2012). A review of social media security risks and mitigation techniques. Journal of Systems and Information Technology, 14(2), 171–180. doi:10.1108/13287261211232180.

[23] Gallagher, S., & Brandt, A. (2020). Facing down the myriad threats tied to COVID-19. Sophos, Abingdon, United Kingdom. Available online: https://news.sophos.com/en-us/2020/04/14/covidmalware/ (accessed on January 2024).

[24] Valdez, C. R., Walsdorf, A. A., Wagner, K. M., Salgado de Snyder, V. N., Garcia, D., & Villatoro, A. P. (2022). The intersection of immigration policy impacts and COVID- 19 for Latinx young adults. American Journal of Community Psychology, 70(3-4), 420-432. doi:10.1002/ajcp.12617.

[25] Franco, E. G., Lukacs, R., Müller, M. S., Shetler-Jones, P., & Zahidi, S. (2020, May). COVID-19 risks outlook: A preliminary mapping and its implications. World Economic Forum, Cologny, Switzerland.

[26] Kumaran, N., & Lugani, S. (2020). Protecting businesses against cyber threats during COVID-19 and beyond. Google Cloud, 16.

[27] European Union Agency for Law Enforcement Cooperation (EUROPOL). (2020). Pandemic profiteering: how criminals exploit the COVID- 19 crisis. European Union Agency for Law Enforcement Cooperation (EUROPOL), The Hague, Netherlands.

[28] Chen, L., Ye, Y., & Bourlai, T. (2017). Adversarial Machine Learning in Malware Detection: Arms Race between Evasion Attack and Defense. 2017 European Intelligence and Security Informatics Conference (EISIC), Athens, Greece. doi:10.1109/eisic.2017.21.

[29] Yan, Q., Li, Y., Li, T., & Deng, R. (2009). Insights into Malware Detection and Prevention on Mobile Phones. Security Technology, SecTech 2009. Communications in Computer and Information Science, 58. Springer, Berlin, Germany. doi:10.1007/978-3-642-10847-1_30.

[30] La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. IEEE Communications Surveys and Tutorials, 15(1), 446–471. doi:10.1109/SURV.2012.013012.00028.

[31] Chiang, H.-S., & Tsaur, W.-J. (2010). Mobile Malware Behavioral Analysis and Preventive Strategy Using Ontology. 2010 IEEE Second International Conference on Social Computing, Minneapolis, United States. doi:10.1109/socialcom.2010.160.

[32] Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on mobile user's data privacy threats and defense mechanisms. Procedia Computer Science, 56(1), 376–383. doi:10.1016/j.procs.2015.07.223.

[33] Schultz, E. E. (2006). Where have the worms and viruses gone?-new trends in malware. Computer Fraud & Security, 2006(7), 4–8. doi:10.1016/S1361-3723(06)70398-0.

[34] Bayer, U., Habibi, I., Balzarotti, D., Kirda, E., & Kruegel, C. (2009). A View on Current Malware Behaviors: LEET. Available online: https://www.usenix.org/legacy/event/leet09/tech/full_papers/bayer/bayer_html/ (accessed on May 2023).

[35] Potlapally, N. (2011). Hardware security in practice: Challenges and opportunities. 2011 IEEE International Symposium on Hardware-Oriented Security and Trust, San Diego, United States. doi:10.1109/hst.2011.5955003.

[36] Li, Q., Gao, H., Xu, B., & Jiao, Z. (2008). Hardware Threat: The Challenge of Information Security. 2008 International Symposium on Computer Science and Computational Technology, Shanghai, China. doi:10.1109/iscsct.2008.217.

[37] Chen, X., & Shi, S. (2009). A Literature Review of Privacy Research on Social Network Sites. 2009 International Conference on Multimedia Information Networking and Security, Wuhan, China. doi:10.1109/mines.2009.268.

[38] Raji, F., Miri, A., & Davarpanah Jazi, M. (2012). Preserving Privacy in Online Social Networks. Foundations and Practice of Security. FPS 2011. Lecture Notes in Computer Science, 6888, Springer, Berlin, Germany. doi:10.1007/978-3-642-27901-0_1.

[39] Srivastava, A., & Geethakumari, G. (2013). Measuring privacy leaks in Online Social Networks. 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Mysore, India. doi:10.1109/icacci.2013.6637504.

[40] Williams, T., & Betak, J. (2018). A Comparison of LSA and LDA for the Analysis of Railroad Accident Text. Procedia Computer Science, 130, 98–102. doi:10.1016/j.procs.2018.04.017.

[41] Huang, S., Zhang, J., Yang, C., Gu, Q., Li, M., & Wang, W. (2022). The interval grey QFD method for new product development: Integrate with LDA topic model to analyze online reviews. Engineering Applications of Artificial Intelligence, 114, 105213. doi:10.1016/j.engappai.2022.105213.

[42] Wei, X., & Taecharungroj, V. (2022). How to improve learning experience in MOOCs an analysis of online reviews of business courses on Coursera. International Journal of Management Education, 20(3), 100675. doi:10.1016/j.ijme.2022.100675.

[43] Sim, Y., Lee, S. K., & Sutherland, I. (2021). The impact of latent topic valence of online reviews on purchase intention for the accommodation industry. Tourism Management Perspectives, 40, 100903. doi:10.1016/j.tmp.2021.100903.

[44] Alzahrani, S. S. (2022). Data Mining Regarding Cyberbullying in the Arabic Language on Instagram Using KNIME and Orange Tools. Engineering, Technology &amp; Applied Science Research, 12(5), 9364–9371. doi:10.48084/etasr.5184.

[45] Thummala, V., & Hiremath, R. B. (2022). Green aviation in India: Airline's implementation for achieving sustainability. Cleaner and Responsible Consumption, 7, 100082. doi:10.1016/j.clrc.2022.100082.

[46] Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. International Journal of Qualitative Methods, 16(1), 1609406917733847. doi:10.1177/1609406917733847.

[47] Paulus, T., Woods, M., Atkins, D. P., & Macklin, R. (2017). The discourse of QDAS: reporting practices of ATLAS.ti and NVivo users with implications for best practices. International Journal of Social Research Methodology, 20(1), 35–47. doi:10.1080/13645579.2015.1102454.

[48] Claps, G. G., Berntsson Svensson, R., & Aurum, A. (2015). On the journey to continuous deployment: Technical and social challenges along the way. Information and Software Technology, 57(1), 21–31. doi:10.1016/j.infsof.2014.07.009.

[49] Yin, R. K. (2013). Validity and generalization in future case study evaluations. Evaluation, 19(3), 321–332. doi:10.1177/1356389013497081.

[50] Sabzi, M., Kamarei, M., Haghighi, T. R., & Mahe, Y. (2020). Analysis and Design of X-Band LNA Using Parallel Technique. 2020 28th Iranian Conference on Electrical Engineering (ICEE), Tabriz, Iran. doi:10.1109/icee50131.2020.9260604.

[51] Abbasi, S. olah, Nejatian, S., Parvin, H., Rezaie, V., & Bagherifard, K. (2019). Clustering ensemble selection considering quality and diversity. Artificial Intelligence Review, 52(2), 1311–1340. doi:10.1007/s10462-018-9642-2.

[52] Hu, X., Li, Y., Chen, G., Zhao, Z., & Qu, X. (2022). Identification of balance recovery patterns after slips using hierarchical cluster analysis. Journal of Biomechanics, 143, 111281. doi:10.1016/j.jbiomech.2022.111281.

[53] Fatouros, G., Soldatos, J., Kouroumali, K., Makridis, G., & Kyriazis, D. (2023). Transforming sentiment analysis in the financial domain with ChatGPT. Machine Learning with Applications, 14, 100508. doi:10.1016/j.mlwa.2023.100508.

[54] Md Suhaimin, M. S., Ahmad Hijazi, M. H., Moung, E. G., Nohuddin, P. N. E., Chua, S., & Coenen, F. (2023). Social media sentiment analysis and opinion mining in public security: Taxonomy, trend analysis, issues and future directions. Journal of King Saud University - Computer and Information Sciences, 35(9), 101776. doi:10.1016/j.jksuci.2023.101776.

[55] Chen, Y., Han, D., & Zhou, X. (2023). Mining the emotional information in the audio of earnings conference calls: A deep learning approach for sentiment analysis of securities analysts’ follow-up behavior. International Review of Financial Analysis, 88, 102704. doi:10.1016/j.irfa.2023.102704.

[56] McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications. Home Office Research Report, 75, 1-35.