Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2975033, 21 pages
https://doi.org/10.1155/2022/2975033

Review Article

Social Networking Security during COVID-19: A Systematic Literature Review

Rabia Abid,[1] **Muhammad Rizwan**,[1,2] **Peter Veselý**,[3] **Asma Basharat,**[1] **Usman Tariq**,[4] **and Abdul Rehman Javed**[5]

[1]*Department of Computer Science, Kinnaird College for Women Lahore, Pakistan*
[2]*Secure Cyber Systems Research Group, WMG, University of Warwick, Coventry CV4 7AL, UK*
[3]*Information Systems Department, Faculty of Management, Comenius University in Bratislava, Odbojárov 10, 82005 Bratislava 25, Slovakia*
[4]*College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Saudi Arabia*
[5]*Department of Cyber Security, PAF Complex, E-9, Air University, Islamabad, Pakistan*

Correspondence should be addressed to Peter Veselý; peter.vesely@fm.uniba.sk
and Abdul Rehman Javed; abdulrehman.cs@au.edu.pk

Received 13 February 2022; Revised 25 March 2022; Accepted 2 April 2022; Published 21 April 2022

Academic Editor: Kuruva Lakshmanna

During the Covid-19 Pandemic, the usage of social media networks increased exponentially. People engage in education, business, shopping, and other social activities (i.e., Twitter, Facebook, WhatsApp, Instagram, YouTube). As social networking expands rapidly, its positive and negative impacts affect human health. All this leads to social crimes and illegal activities like phishing, hacking, ransomware, password attacks, spyware, blackmailing, Middle-man-attack. This research extensively discusses the social networking threats, challenges, online surveys, and future effects. We conduct an online survey using the google forms platform to collect the responses of social networking sites (SNS) users within Pakistan to show how SNS affects health positively and negatively. According to the collected response, we analyzed that 50% of the users use SNS for education purposes, 17.5% use it for shopping purposes, 58.2% use it for entertainment, 37.1% use it for communication, and 9.8% use it for other purposes. According to the response, the excessive use of SNS affects the health that 9.8% users face the physical threat, 42.8% user faces mental health issues due to excessive or inappropriate use of SN, and 50.5% users feel moral threat using Social sites. Finally, we conclude our paper by discussing the open challenges, conclusions, and future directions.

1. Introduction

Social networking (SN) is a form of web servicing to develop virtual communication between people worldwide. In SN, many factors involve data sharing, communication, business, education, and information. Twitter, Facebook, Instagram, WhatsApp, Skype, Messenger, and others served as intermediate service platforms between multiple users [1]. These social services have become much more common because people feel friendly to share and update their personal information by viewing others' profiles and information [2, 3]. A large amount of personal data is shared on social sites and used cloud servers for the data-sharing connections. As social networking becomes that popular, it is affected by various hackers or attackers, internally and externally. Intruders can gain sensitive information of end-users by using different kinds of attacks like malware, ransomware, social bots, spam, hacking [4]. Various types of attacks compromise the security factor of many organizations, co-operations, businesses, and many other sectors. The basic concept of social networking can be shown in Figure 1.

The Covid-19 (Corona Virus) has been spread around all over the world now, and new cases and death rates are increasing day by day, which is an alarming situation for human life [5–8]. The Covid-19 pandemic shook the businesses, economy, trading, education [9, 10], healthcare, especially the daily lifestyle of everyone globally [11–13]. All world-known organizations like the world health organization (WHO), Carevac, Bointech, Moderna, Glaxo Smith, J&J, and many more are working with researchers and scientists to overcome the situation and discover vaccines. As the disease transfers from person to person, many countries imply complete or smart lockdown to limit the Corona disease. All physical working sectors have been shifted to the online workflow to decrease the corona disease. As everything shifted to online mode, the internet and social networking medium usage increased significantly [14]. The increasing usage of SN increases the challenges and threats of network security [15]. It is considered the most critical issue, which needs to be appropriately addressed.

During the Covid-19 pandemic, people are limited to their homes, which somehow cause severe mental, physical, and moral health issues [16–19]. The safety measure in the form of lockdown conducted by Governments to overcome the rapid spreading to Covid, to some extent, damage the well being and health of humans [20]. Despite that, due to idleness, SNS plays an aggressive role in increasing the rate of human health issues.

When we talk about cybercrimes, many websites, applications, software, malware attacks, and many more have been counted, violating the security element of the systems, as the internet services (like third-generation (3G), fourth-generation (4G), and fifth-generation (5G) become cheap, it is so easy to use them, which is considered the main reason to boost the cybercrimes in social networking [21]. As the technology advanced, it moved towards machine learning models, which replace humans or shorten the human interference in the system activities. Many machine learning approaches automatically or systematically help users detect cyber-attacks and alarm the systems by generating notifications. These techniques help to identify the variance problem at some ease level. This scenario is inter-connected with Deep Learning, artificial intelligence, machine learning, natural or artificial language processing, and many more.

While considering social networking threats, we mainly focus on the detailed analysis of their threats. The main agenda of our research is to study and analyze the challenges of the threat in social networking and how it can be a more efficient, secure, trustworthy network for communication. The survey will also help understand the concept of threat for every end-user and their perspective. We analyze the security issues and highlight how threats of SNS affect the health of its users, mentally [22], physically, and morally.

1.1. Motivation. In today's world, SNS are everywhere; it helps to shrink the distance and brings people on a single platform, known as social media. As long as several SNS users increase, the chances and risks of security/privacy breaching increase. All data shared online using SNS needs some security walls to protect users' privacy. During the Covid-19 pandemic, the use of SNS increased due to lockdown situations, all education sectors shifted to online classes, and work from home scenarios abound users to use SNS. As more users' data is uploaded or shared on sites, cases of intrusion, data leakage, malicious attacks also increase. Either the data leaked or data stole against some ransoms amount. By providing your data and personal details on social sites, your data may fall in the wrong place or in the wrong hand, which can be misused. There are millions of case scenarios where SNS are the cause of deaths, suicides, mental health problems, physical health problems, and many more in today's world. By considering the following situation, we decide to research about the SNS security threats, types of threats, real-time case scenario where people became a victim, online SNS security survey and their effects on the health of its users. Moreover, we try to collect the recent responses of SNS users and try to know their opinion on the SNS security risks, issues, and challenges.

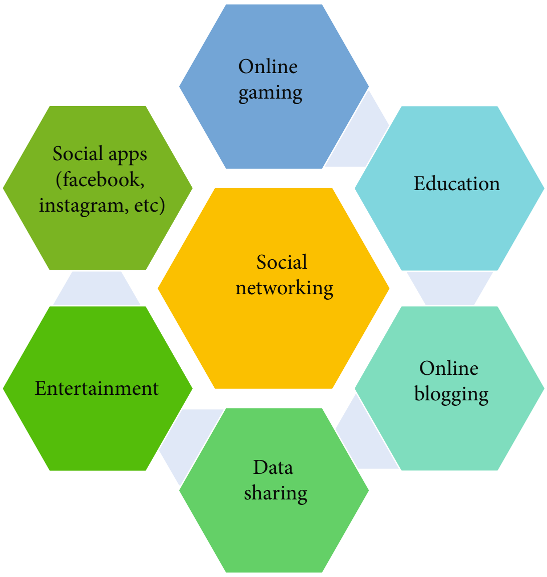


Figure 1: Essential Concept of Social Networking.

1.2. Contribution. This research discusses the security threats and the future challenges due to social networking.

(i) We analyze and provide the positive and negative impact of SNS during the Covid-19 pandemic

(ii) We identify and discuss the possible security threats that SNS faces and types of Security attacks in detail

(iii) We also examine the possible solutions, according to recent research, case scenarios

(iv) We also conducted an online survey to gather responses of SN users and make an analysis based on the submitted responses that how excessive use of SNS make a healthy person mentally or physically retarded

(v) Finally, we discuss the security challenges and future directions

1.3. Organization. The rest of the paper is organized as follows. Section 2 discusses the existing work on SNS. Section 3 discusses the security risks and its threats during Covid-19 (lockdown). Section 4 provides a detailed discussion on challenges like privacy, security, anonymity, and physical. We discussed the possible solutions for SNS security with its diagrams and tables in section 5. After that, SNS based security survey is conducted to analyze the responses of SNS users and its effects on human health in Section 6. Further on, in section 7, SNS open issues and challenges have been mentioned, which are still existing and need to work on it. Finally, the research is concluded in section 9 with future direction in Section 8. Table 1 shows the lists of acronyms of paper.

2. Related Work

Recently, much research has been conducted on healthcare and the adverse effects of social media among its users. Many researchers and scholars discuss the role and use of SNS and its impact factor on human health. According to many authors in [23, 24], considered SNS as a role model in today's advanced world to reshape and influence the opinion of its users. SNS becomes a vital platform for discussing healthcare issues with new advancements and technologies. SNS uses interaction with a common audience to empower and collaborate with them. The SNS has also practically changed the healthcare sector. It provides a direct medium to patients and doctors generally and at a large scale, related to all departments like laboratories, diagnosis, appointments, emergency cases, and many more. According to the author in [25, 26], discussed that SNS plays a meaningful role in healthcare, especially between patients and doctors' direct interactions. According to SNS in healthcare [27], it helps the users to engage themselves in online curing treatment options as online precautions and treatment available, especially during the COVID-19 pandemic.

One of the main strengths of SNS is a well-timed response to its users on their demand or requirements. According to [28], SNS is considered as the best platform to collect efficient and accurate responses with a higher rate against surveys or form. Likewise, the same is the case with the healthcare sector. In all emergency cases, SNS proves helpful to cope with the situation. According to top researches [29–31], SNS helps its users to cope in Covid-19 pandemic situation, as lockdown in many countries limited the access of doctors. In that situation, SNS proves helpful to communicate with consultants to take precautionary measures.

Networking security has been considered an essential factor in communication and data sharing. As the paper [32] discussed the SNS and its security which leads people to suffer health issues. In this literature, we review the effects of security issues in SNS. As far as privacy is concerned, every SNS sites have privacy boundaries based on context and information. Data security and privacy breaching threats leave a severe and negative impact on the mind and health of its users. In SNS, privacy and data security are also considered key elements internally or externally.

Many researchers have been worked on the privacy and data leakage topic. According to [33], self-disclosure has an adverse impact on the mental health and stability of users. Contrarily, according to [34], identify the level of intimacy, honesty, and capacity of data leakage on SNS has been concerned with privacy adversely. Similarly, according to [35], a detailed analysis on the collected data of Facebook users in Pakistan around 400 people. Furthermore, the PLS-SEM technique has been implemented to analyze which percentage of people share their data, feelings, and emotions on the SNS platform. Moreover, after analysis, around 31% of variation has been diagnosed in self-disclosure activities and user behavior. However, privacy concerns and data leakage move the large numbers of users towards health problems.

Table 1: List of Acronyms.

Notations	Meanings
G	Third generation
G	Forth generation
G	Fifth generation
AI	Artificial intelligence
XAI	Extended artificial intelligence
ANFIS	Artificial neural fuzzy inference system
ANN-DRL	Artificial neural networks - deep reinforcement learning
CIA	Confidentiality, integrity and availability)
CNN	Conventional neural networks
DDoS	Distributed denial of service
DNS-HES	Domain name system - hardware enhanced system
EPVDM	Efficient privacy violation detection model
FIA	Federal Investigation Agency
GPS	Global positioning system
HE-CRT-RSA	Homomorphic encryption Chinese remainder theorem with a Rivest-Shamir-Adleman
IBM	International business machines
IDs	Intrusion detection system
IP	Internet protocol
MEC	Mobile edge computing
MMNT	Multi-media networking threat
MNT	Media networking threat
NADRA	National database & registration authority
PLS-SEM	Partial least squares - structural equation modeling
PPC	Pakistan panel court
PSNS	Parasympathetic nervous system
SN	Social networking
SNS	Social networking sites
SNAT	Social networking application threat
SPSS 2.0	Statistical package for the social sciences
U.S	United States
U.S.A	United States of America
WBAN	Wireless body area networks
WHO	World Health Organization

Although SNS plays a magnificent role in communication and connecting people around the globe, at the same time, it has some adverse effects on human life. It provides an online platform to its user to avail well-time consultations, especially in the medical field. On the other hand, it also adversely affects the human mind and health. Though, SNS has to control and prevent role during Covid-19 alarming situation.

Though, the positive impact of SNS usage changes towards the negative impact. Specifically, according to the author in [36, 37], the Covid-19 pandemic builds an environment where everyone engages themselves in excessive use of SNS and leaves a negative impression. A large number of studies have been conducted to analyze the emotions and feelings of SNS users to predict their health status. According to [38], pre and post Covid-19 status and sharing of data on Twitter increased numerously. Similarly, around 4 K post has been shared on Twitter (SNS) in-country China. It takes contrast and analysis beyond the next level.

According to some scholars and their argument [39], it can be identified through the emotion of people the mental health condition of SNS users. Likewise, according to the author in [40] stated, excessive use of SNS leads to sleeping disorders, psychological problems, anxiety, stress, depression, mood swings, poor academic record. Then in [41] author discusses the mental health issues and problems like human behavior, linguistic analysis, personality traits, excessive influence of SNS. According to the [42], the SNS effects on adolescents are physical health, sleep reduction, more or less eating habits, imbalanced diet, marital relationship, personal life.

Also, [43] discussed Human Health and Wellness and its impact on social communication, psychotic issues, physical activities, moral downfall. Though, mental and health instability push its users towards various cardiac diseases. According to [44] in 2020, a large number of cases increased in cardiovascular disease, weak masculine, deficiency in sleep, reduction in resting time, heart attacks, tightening muscles, which considered in the harmful impact of SNS. And then in [45] also mentioned the mental health disturbance in Japanese, and their analysis shows that the cases of feelings of loneliness.

However, the interconnection between SNS and the healthcare domain became an arising concern. During the Covid-19 pandemic, physical, moral, and mental health issues occur in large numbers. According to the literature review, excessive use of SNS leads every individual towards serious health problems, which need to be overcome to cope with the life threats of today's generation. Table 2 shows the analysis of existing literature work, where SNS security challenges and issues have been identified. According to the many researchers, SNS faced many security issues and proposed many research studies to overcome the shortfall, but still, it exists many limitations and challenges, some of which are discussed in Table 2 in section challenges & issues.

3. SN Security Threats and Pandemic

The emerging technology and Covid-19 situation lead towards the highest rate of cyber-crime and cyber-bullying. It becomes so easy for hackers, scammers, intruders, to avail this chance when people are more frightened, susceptible, and distressed, making social networking infrastructure weak and less secure [63, 64]. According to many types of research in the Covid-19 pandemic, there were more than 900 k spam messages, 730 malicious attacks, and activities, 50 k hits on pop-up ads, which are malicious links. Many cyber security threats are listed and discussed below, along with the proposed taxonomy of the existing solutions and problems in Figure 2.

3.1. Configuration Mistake. In every professional field, there is at least a single mistake that occurs during the configuration or installation of a softer or working tool in the system. According to Software company Rapid7 (https://www.embroker.com/blog/top-cybersecurity-threats-2022/) (Which is one of the best companies in cybersecurity), issues an alarming figure of 80% of misconfiguration test occurs. It is a type of attack where intruders directly attack the internal architecture like accessing through third party or systems, and generic amount if such exploitation reaches 96%.

3.2. Distributed Denial of Service Attacks. During the Covid-19 pandemic, many governmental, economic, personal, healthcare faces DDoS attacks. A flood of hackers become active in their malicious activities like crashing systems, devices, and mobile phones [65–67]. The main agenda of DDoS attacks is to interrupt the Social communication channel [68]. There are many examples of affected systems that become victims of DDoS attacks.

3.3. Poor Cyber Hygiene. The term'cyber hygiene' refers to habits and practice of how to use technology like wifi networks and providing them security (VPN or two-step authentication) [69]. Around 60% of systems depends on human memory to keep remembering passwords, and around 42% of businesses and organizations use sticky notes to keep the system password. In the two-step authentication security process, around 54% of users avoid using it while just a small 34% try to use it to make their accounts a little bit secure.

3.4. Phishing Attack. Phishing attacks consider a type of social media networking threat. According to [70–73] in 2021 mention the effects and categories of phishing attacks as personal data leakage, account hijacking, malicious stalking, which are all concerned with media applications. A real case about a phishing attack occurred in Spain, which locked the systems and demand for ransomware (https://duo.com/blog/how-phishing-impacts-healthcare).

3.5. Spam Emails. In every business, emails matter a lot because all the activities are based on emails. Mail spamming has been used as the most intended way to scam the activities by hackers. In the current Covid-19 situation, email spamming has been analyzed mainly until December 2020. According to the survey report of WHO [74], a large number of hacking cases come into existence during the pandemic period. A spam email address with malicious activities like adding Bitcoin, donating for corona victims, etc. Similarly, many malware attacks are discussed according to some

Table 2: Analysis of existing Related Work.

Ref.	Years	Deployed category	Technique used	Challenges & issues
[46]	2022	**Productivity**	Conducted online survey and collected responses of around 8302 users during Covid-19 pandemic (in lockdown situation)	Excessive use of SNS leads towards stress and depression symptoms
[47]	2022	**Internet resources**	Proposed a technique to diagnose the internet addicted users and proposed treatment plan	Internet addiction, detecting biopsychosocial order of its user
[48]	2022	**Viruses & Malware**	Perform analysis of 387 researches to detect security gaps	Ratio of cyber crime victimisation increase rapidly
[49]	2022	**Social engineering**	Impact of SNS of Therapeutics's relations	It cause personality disorder, bipolar mania, in 18 to 25 years age and having low self-esteem in adults
[50]	2022	**Reputation & Legal liability**	Proposed Hoepmanâ€™s privacy strategies to secure digital systems	Identification and authorization issue in data protection, secured controlling systems for children
[51]	2021	**Fake accounts & biological research attacks**	A survey on E-healthcare system in WBAN with security and privacy routing mechanism	During Covid-19 pandemic fake accounts, data dependency, security, confidentiality challenges still existing
		Classical threats		
[52]	2021	Malware	Presented ghost in the cloud mechanism to detect malware attacks	Information accessing threats and undetected way
[53]	2021	Phishing attack	Fake phishing website created to target 107 SNS users and spread awareness	Email, SMS, social sites are still facing security challenges
[54]	2021	Spam attacks	Collected results of 35 users in PSNS application to analyse the trust factor of users	Presentation of negative responses on shared content make mental health of SNS users effected
[55]	2021	Web bugs	Analysing the SNS using security right and threats by collected data of around 250 users	Human right of privacy and security of data is still challenge
		Modern threats		
[56]	2021	Click jacking	An effective machine learning based approach proposed to overcome fake profile and unauthorized users	Malicious linking and fake sites causes hacking and profile data theft issues
[57]	2021	De-anonymization	Categorized the types of attacks in spam attacks, malware's and data or information theft	Limitize the issues as unauthorized, un-authentic and false threat injections in data
[58]	2021	Fake profiles	A comprehensive literature review has been discussed about fake accounts and profiles	Open and free access to SNS encourage intruder to interleave in personal space of SNS users
[59]	2021	Identity clone attacks	Multi-level authentication technique used to make SNS model trained and trustful by 15%	Hacking websites, password, emails and personal profiles of SNS users
[60]	2022	Inference attacks	Analyse comprehensive surveys for mobile edge computing (MEC) security, objectives, authorization, prons and cons	Cloud computing still facing privacy, authentication, security, efficiency and deployment challenges
[61]	2022	Information leakage	Analysed and experimented the responses of 224 college students for SNS fatigue, SNS immerse usage by using SPSS 2.0 technique	Time management, excessive usage and health fatigue cause troubles in student and with their mind
[62]	2022	User profiling	Used poisson regression methodology to evaluate the positive an negative response/posts of SNS users, to show true and false rumor	Sadness and fear of false accusation due to tweets/retweets by surfing on SNS

researchers in [75–77] are data loss, privacy breaching, account hacking, system crashing. Around 100 mailboxes of NHS workers become victims of phishing (cyber security) attack (https://duo.com/blog/how-phishing-impacts-healthcare).

3.6. Internet of Things. The alarming situation of the pandemic shifted all the office to home, where around 70% of households shifted to smart systems or devices. Surprisingly, the ratio of cyber-attacks in IoT devices will increase like 1.5B security breaches cases till 2021. By availing the situation, hackers tried around 12,000 attempts to breach IoT devices' security in a single week [78]. According to research, from 2021 to 2025, the demand for IoT-based devices will increase two times more. It will increase the accessing ranges, and more chances of security breaches will occur

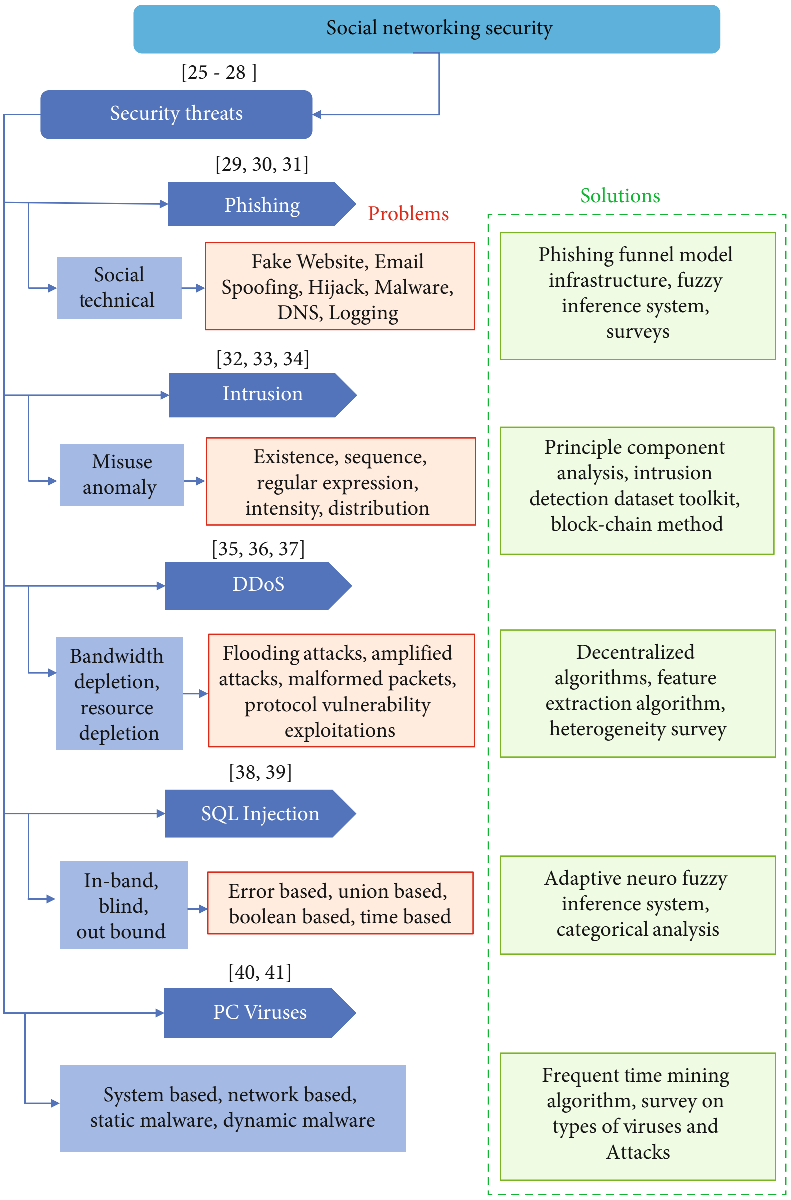

Social networking security
[25 - 28]
Security threats
[29, 30, 31]
Phishing
Problems
Solutions
Social technical
Fake Website, Email Spoofing, Hijack, Malware, DNS, Logging
Phishing funnel model infrastructure, fuzzy inference system, surveys
[32, 33, 34]
Intrusion
Misuse anomaly
Existence, sequence, regular expression, intensity, distribution
Principle component analysis, intrusion detection dataset toolkit, block-chain method
[35, 36, 37]
DDoS
Bandwidth depletion, resource depletion
Flooding attacks, amplified attacks, malformed packets, protocol vulnerability exploitations
Decentralized algorithms, feature extraction algorithm, heterogeneity survey
[38, 39]
SQL Injection
In-band, blind, out bound
Error based, union based, boolean based, time based
Adaptive neuro fuzzy inference system, categorical analysis
[40, 41]
PC Viruses
System based, network based, static malware, dynamic malware
Frequent time mining algorithm, survey on types of viruses and Attacks

Figure 2: Taxonomy of Social Networking Security Threats.

[79]. The expert predicted till 2025, the whole world will shift towards smart homes, offices, businesses, and everywhere [80].

3.7. Ransomware. Attackers launch ransomware attacks on SNS by taking advantage of the pandemic. The ransomware attack affected the systems by attaching viruses in the email links by using employ credentials to exploit the vulnerability [81]. Now, it considers as the'Dark Web,' spam virus with the name of coronavirus cleansing tool, which injects the harmful virus into the website, and end-user by force bound to download the setup on their systems [82–84] Once the malware setup installed in the system, the attacker gets access to the password and breach the privacy of the systems, and blackmail targeted user for a ransom amount. Most of the underdevelopment sector is financially affected in a lockdown situation; ransom criminals become optimistic towards the organization to get a lump sum of amount.

3.8. Blockchain and Crypto-Currency. Though cryptocurrency is not as important for the single common user, it is a big deal for businesses, organizations, and government bodies. It compromises businesses' personal and confidential data, and customers exploit their relationships. These emerging technologies move the IT industry towards the next boom level, but still, it compromises many security factors and data breaching elements. Many types of attacks have been used like Sybil [85, 86] and Eclipse [87] are most common and threatening.

3.9. Malicious Domain. The availability of various irrelevant websites with fake domain names puzzled the user. As cyber criminals create countless fake news sites involved in phishing attacks, malware spreading, spam emails, false campaigns, or database servers are negotiated [88]. According to the Covid-19 pandemic, more than 4000 fake websites have been registered with coronavirus names during the risk intelligence report. Primarily, the honeypot technique has been used to target the relevant end-users. According to some researches [89–91], mention some of the effects and types of malicious domain attacks as Integrity, confidentiality, false injections, false website. The spammer gets sensitive personal data or information and uses it in illegal or intended tenacity.

3.10. Malicious Applications. Every business, organization, and other sector has systems and databases where attackers access malicious software. Like most software requires an additional installation setup, the downloaded setup access system internal settings. That access leaks the passwords, data, or personal information and violates the system or end-user credentials [92–94]. Most of the malicious application gets access to the system camera, which violate the personal financial, private data [95]. This type of attack hacks the systems and changes the systems setting, toolbars, home page setting, which becomes difficult to uninstall or remove.

3.11. Spoofing. Spam Emails consider a spoofing attack. Scammers also look forward to a Pandemic situation and start circulating spam emails whenever there is a pandemic. According to [96–98], spam mail, virus injection, scam emails, malicious site injections, attacks application layers are considered as types of threats. During the Covid-19 situation, many spam mail named on coronavirus donations or vaccine campaigns started circulating the globe [99]. As WHO is a world-known healthcare organization, at this point, spammer us their email id as spam mail start phishing over the internet to end-users.

3.12. Malicious Social Media. Nowadays, social networking and social media are pervasive, and every single end-user can avail of its services. Intruder finds it an opportunity to attack the social site and violate the end-users privacy by using fake IDs, passwords, data sharing, account hacking, and many more. The most common social site includes: Facebook, Twitter, Instagram, Snapchat, YouTube, Tiktok, WhatsApp, and many other [100] According to some previous research [101–103] in 2021, mentions some severe types of attacks, fake user id, fake account, confidentiality, privacy breaching, data loss, mental threats, data sharing, hacking, ransomware. As most of the sites are free of cost or subscription-free, we can use it by just having an internet connection [104].

3.13. Business Security Compromises. During Covid-19, a compromising attack on the business email was reported by the Agari intelligence. The old-time tortoise attack has been used to violate the companies' privacy. Most of the attacks on the business sector ask victims to change bank information and payment methodology on behalf of the organization and exploit the business structure. At the time of the attack, the attacker shows up asks the member or authority of the business or organization [105]. So, according to some authors, [106–108] data loss, system hacking, logging access, personal information leakage, confidentiality, efficiency, architecture threats are considered as serious security threats for the business community.

3.14. Mobile Device Security Threats. During the Covid-19 pandemic, many authors discuss the security issues related to mobile devices in some researches [109–111], pop-up ads, hacking, malicious software, unwanted application download, data loss, blackmailing, ransomware, privacy policy, fake pages, fake users, or accounts. The use of Mobile phones has been increased at the highest peak level. Human beings consider their life null without having smartphones. During the Covid-19 pandemic, an attack named Covid-Lock appears as a malicious app that requires bitcoin to recover the end user's phone. The threat which made users worry was the leakage of personal data or deletion of the whole phone data [112]. Similarly, if an end-user creates a backup of their smartphone's data, it can be hacked on the base of a trojan horse attack too. Likewise, while using a social app on smartphones, some pop-up ads appear on the screen, which directly moves towards the malicious website page; during all this, primarily phones get hacked with these pop-ups activities [113].

3.15. Browsing Application Threats. In the modern era of smart technology, everything moving around us is based on artificial intelligence or machine learning-based. Though with the increasing usage of the internet, data browsing in our daily life includes in our routine [114, 115]. Then, if we talk about the Covid-19 pandemic, many cyber-attacks have been diagnosed, especially in WHO, that data from the WHO app has been breached. The attacker gets access to the main server in settings that automatically open browsers and generate an alert in the app. The alert forced to download the Covid-19 information app; when the user clicks on the button, it installs the malware software in the systems and devices. By using this technique, many cookies, passwords, history, transaction information, and many other things have been accessed [116]. Other than that, many authors discuss the categories of security attacks in [117–119], which are fake accounts, fake websites, SQL injections, database servers crashing.

In taxonomy diagram Figure 2 represents the overview of social networking security [120–123], and then shows the security threats during Covid-19 pandemic in all sector (education, business, healthcare, smart technology, organizations and many more) like phishing [124–126], intrusion detection [127–129], DDoS attacks [130–132], SQL injection [133, 134], and PC Viruses [135, 136].

According to the concept of many cyber-security researchers, SNS data and privacy security are classified into many categories [137]: Social networking applications threats (SNAT), media networking threats (MNT), multimedia networking threats (MMNT). All these categories are further divided into subcategories. Table 3 discusses the categories of threats and existing relating research work.

Table 3: SNS: Security Threats Detection and their Analysis.

Ref.	Threats or issues	Techniques	Analysis
[138]	Cyber-security	Uses netflow data to measure threat ranges	38% to 40& of network traffic included in blacklisted flow
[2]	Privacy and security	Social networking theory	Discuss many different scenarios to remove threats
[139]	DDoS attacks	DNS-HES cluster designing	Uses hardware to remove security threats from systems
[140]	Malicious domain	Surveying posts on social media sites	Analysis shows impact on politics, information and researches
[141]	Malicious applications	ANN-DRL classification techniques	Enhanced the classification process and increase accuracy rate in detecting threats
[142]	Phishing attack	Conventional mechanism	Analyze result and enhance security threats detection rate
[143]	Data privacy breaching	Blockchain technology	Secure data manipulation process and data storage in healthcare
[144]	Phishing and malicious domain	Efficient privacy violation detection model (EPVDM)	Proposed model helps to increase accuracy rate with 94%
[145]	Spam mails and pop-up ads	Improved deep CNN	Proposed techniques helps to filter malicious lists of threats and identify them
[146]	Third party attacks	Support vector machine and ANFIS models	Proposed models helps to show 90.3% validation rate in intrusion detection
[147]	DDoS security attacks	HE-CRT-RSA algorithm	Proposed HE-CRT-RSA algorithms much more efficient 3-4% in security perspective than traditional RSA algorithm
[148]	Authentication	Complicated authentication techniques	Proposed multi-factor authentication process in mobile cloud computing to detect security and privacy threats

4. SN Security Challenges

In order to secure the systems and humans, some challenges of social networking security still exist, which need to sort. End-users must ensure themselves to update the systems, devices, mobile phones. Due to increasing online cyber-crime activities, security software updation becomes essential during this Covid-19 pandemic. Most of the time, end-users ignore to make updation in the software to avoid time pause in their activities. Although updation and troublesome requires some memory from internal device storage, due to this reason, people also avoid doing updation, which leads to security breach risks.

4.1. Privacy Risk. Social networking provided a proper mechanism for all application settings to make user profiles, accounts, data, personal information more secure, but still, it needs some improvement. Most end-users are unaware of using privacy setting tools in the systems, devices, or applications. Most of the systems have no flexibility. The end-user cannot customize it according to his/her own will. The end-users are unaware of how to protect data and avoid security attacks. Here is a real-time case scenario related to the privacy challenge. A report from DAWN News Pakistan (http://www.dawn.com/news/1600479):

(i) The Federal Investigation Agency (FIA) took action against the group of five people of accusing a girl living in Lahore by selling their personal WhatsApp data against ransomware

(ii) According to cyber-crime reporting of Pakistan, the gang developed a network in a rural area and blackmailed the citizen against money

(iii) The gang admitted in front of FIA that they had gathered the voice call data and ownership of specified person by hacking the NADRA records via WhatsApp group

(iv) A FIR has been registering against Shoaib Nawaz, according to sections 3, 4, 5, 6, 7, 8 and 17 of the crime Act, 2016 of PPC (Pakistan Panel Court).

4.2. Security Risk. Malicious attacks consider a security risk in SN. Most of the time, malicious applications have been developed for hacking purposes, to reveal someone's data or information. Once we download a single setup, some malicious setup automatically downloads and cracks the system's privacy. As we talk about social sites, some psychological or personality tests based on fake websites gather the user's information and blackmail the connected user for ransomware personal grudge. Many examples can be seen in this scenario, like fake user ids or emails, logging credibility, criminal cases, terrorism. Some of the cases mentioned in INSIDER magazines related to security risk in SNS. (https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4):

(i) Approximately 533 million end users' data has been stolen and hacked from Facebook (especially phone numbers and personal details).

(ii) According to Alon Gal (chief executive of cyber-crime intelligence firm) stated the data leakage incident of Facebook users. An automated bot attacked the system motherboard, which accesses users' data location. It makes data available on a free hacking forum for everyone

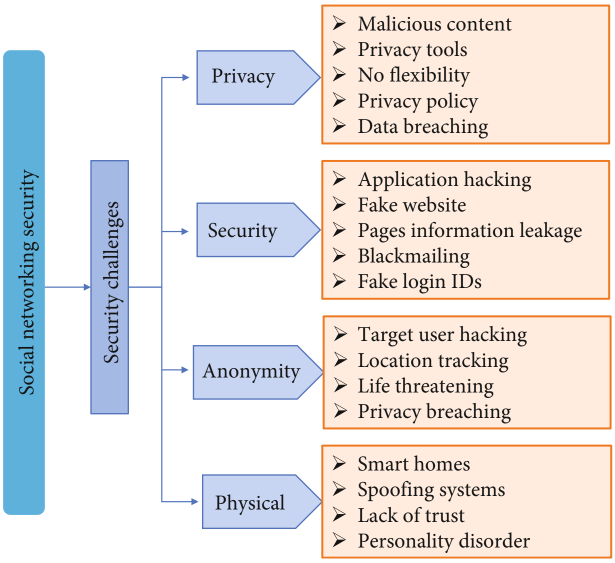
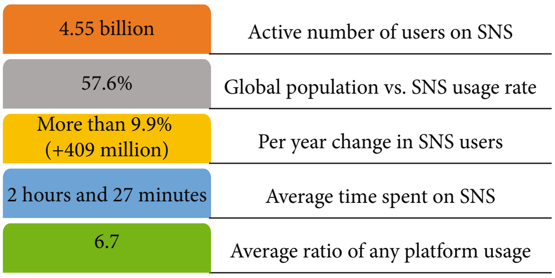


Figure 3: Taxonomy of Social Networking Security Challenges.



4.55 billion	Active number of users on SNS
57.6%	Global population vs. SNS usage rate
More than 9.9% (+409 million)	Per year change in SNS users
2 hours and 27 minutes	Average time spent on SNS
6.7	Average ratio of any platform usage

Figure 4: Statistical report on use of SNS during 2021.

4.3. Anonymity Risk. In anonymity risk, the end-user is unaware of the fake person; you cannot identify the fake personality. By targeting the user ids and data hacking, end-users use GPS location on the functionality of their devices. Many tracking has been launched to provide a way to track specific locations. If the target location of the device is on, the intruder becomes active and breaches privacy. According to International Statistics and Analysis on data breaching cases (https://www.varonis.com/blog/data-breach-statistics/), here is the list of some data breaching cases:

(i) Around 500000 fake Zoom account has been created by black hackers, whereas Zoom is considered an educational application

(ii) Recently, IBM generated the report that shows the data beaching cost around $3.86 million

(iii) According to a statistical report from Yahoo, it holds the largest amount of fake accounts and data breaching; almost 3 billion accounts have been compromised

4.4. Physical Risk. Physical risks involve a large amount of data breaching cases. All the physical risks are connected to human life itself as this is er of smart technology. Every end-user has free and easy access to the internet using a specific IP address. Here are some examples of the physical risk: businesses, healthcare centers, government departments, aviation fields, education, personal activities, entertainment, communication. On Feb 9, 2021, McLean (https://www.mcleanhospital.org/essential/it-or-not-social-media-affecting-your-mental-health) issued an article on mental health and social media. According to their statistics:

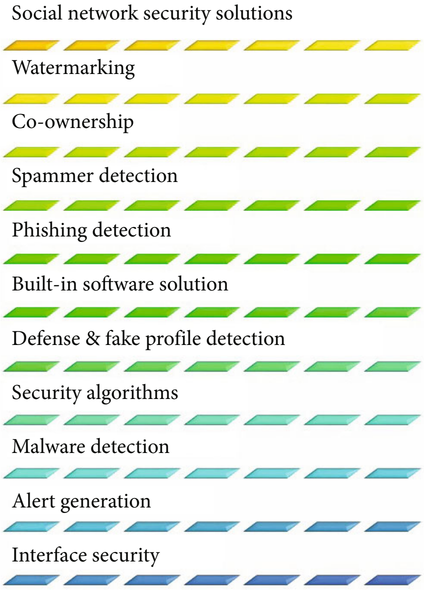


Figure 5: Possible solutions for SN security.

(i) At McLean hospital, a psychologist, Jacqueline Sperling, who works with young patients with a mental disorder, discusses the activities on Instagram: People compare themselves with others and like, comment, post according to the comparison factor, which leads towards mental health problems

(ii) According to the statistics of the Pew research center, around 69% of adults and 81% teens use social media applications in the U.S. Which large direct ratio of people towards mental health issues, like depression, anxiety, access use of social media

(iii) A university of Pennsylvania researched two groups of 143 students. One group was asked to use social media regularly multiple apps (having a happy and normal lifestyle), and the other group was not allowed to use social apps (having depression and anxiety issues). After three weeks, group one suffered from anxiety, depression, loneliness, fewer sleep issues, and many others, while on the other hand, the other group became healthy and happy and became depression-free

In taxonomy diagram Figure 3 represents the overview of social networking security challenges during the Covid-19 pandemic in all sectors (education, business, healthcare, smart technology, organizations, and many more) Like anonymity risk, privacy risks, security risks, and physical risks.

Table 4: Possible solutions or policies for SNS Security.

Ref.	Year	Solution	Description
[164, 165]	2021	Privacy policy based solution	Securing from third party interleaving and improving privacy and security setting in the systems and network resources
[166]	2021	Security and cryptography	Secure and efficient key generation on message encryption and decryption phases, as well as in networking site logging sessions
[148, 167]	2021	Authentic mechanisms	Providing secured and authenticate mechanism for the system to store and protect data and information using Blockchain technology.
[164, 168]	2021	Education research-based privacy solution	Latest research analysis on privacy and security issues will help the users to make the network resources more secure
[169]	2021	Report false users	Needs multi-factor authentication to avoid false users and improve the report setting in SN applications to avoid security risks
[170]	2021	Cyber-grooming	To keep your child safe from cyber-bullying and threats, this technique can help the person to generate security alarm.
[171]	2021	SNS user awareness	How to use SNS, awareness campaign by welfare authorities

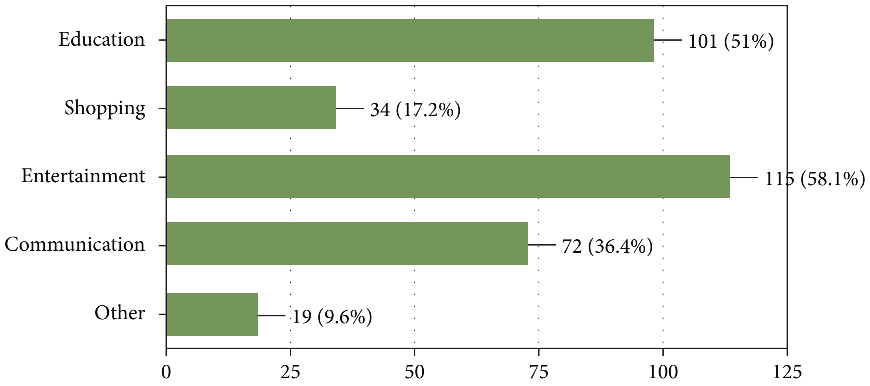


Figure 6: Graph represents the calculation of daily usage percentage of end users.

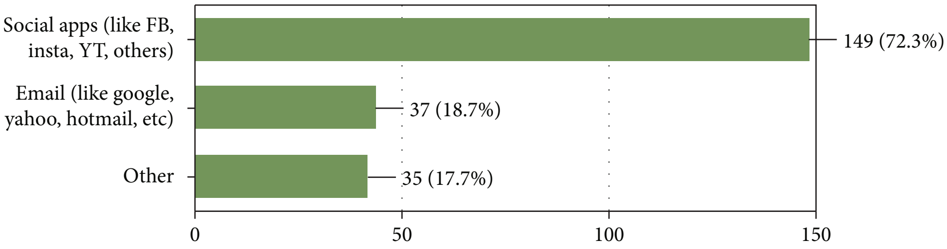


Figure 7: Graphical representation of usage the networking sites.

Researchers also try to find possible solutions to overcome the security challenges when problems occur.

4.5. Mental Health Risk. The connection between SNS and mental health issues has been discussed with the term psychological problem [149]. So far, much research has been done on excessive use of SNS and their adverse impact on the healthy mind of users. The more time spent on SNS, the more it leads towards the phases of depression, anxiety, mood swings, obesity, cardiac diseases, psychological and neural effects on human health [150, 151]. Though not much research has been conducted to measure the level of psychotic illness, the main focus is on the root cause of this risk.

During the Covid-19 pandemic, an immerse number of psychological issues has been diagnosed [152]. Everyone spend most of their time on SNS [153], it helps to communicate around the globe in such severe and stressful situation. According to many studies [154], excessive use of SNS leads to depression, anxiety, low self-esteem [155], addiction, inferiority and superiority complexes [156], a large amount of cost spending on online shopping and deliveries, through many surveys and questionnaire [157–159]. According to statistics of digital world report (https://

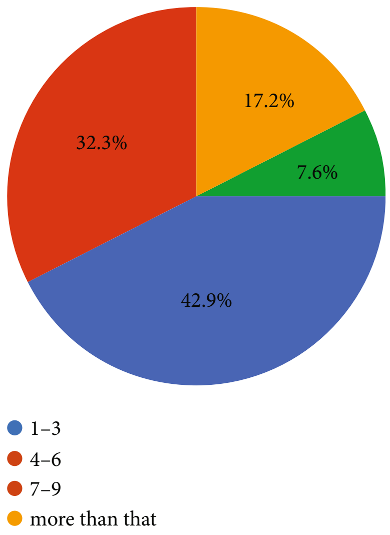


Figure 8: How many hours end users spend their time on SN sites.

datareportal.com/reports/digital-2021-pakistan), use of SNS in worldwide represented the following Figure 4.

According to a survey report (https://lisbdnet.com/the-real-social-media-addiction-stats-for-2021/) of the U.S.A., people who are using SNS more than 58 times in a single week face serious mental and health issues like depression and social isolation. In 2021, around 333 M users using SNS became seriously addicted personalities. Similarly, according to a statistical survey report (http://www.roymorgan.com/findings/8123-mental-health-conditions-australian-youth-june-2019-201909090253), around 38% SNS users facing severe mental health issues, most common symptoms are stress, depression, and anxiety.

5. Possible Solutions for SN Security Threats

Recently, many researchers and security experts have worked on social networking security. A large variety of possible solutions has been discussed previously in all sectors. Here, we discuss some of the possible solutions and methods based on the literature of SN. Figure 5 show the list of some techniques and approaches regarding security perspective.

To provide a secure and efficient cloud system, which helps secure networking sites, here are some possible approaches to overcome security threats [160, 161]. Many researches has been conducted to detect the intrusion attack in SN [162]. Similarly, in [163] proposed a model and algorithm to preserve the agriculture system and proposed a better security framework. Table 4 helps to understand the concept of existing possible solutions and privacy policy for SNS security.

6. Social Networking Security Based Online Survey

Here, in this paper, we work on the social networking-based online survey to get the adverse or positive effect of SNS on audience or end-users. We design an online survey containing some questions like:

(i) How many people get affected by SN threats or security issues?

(ii) Is SN security risks affecting the health of end-users (physical, mental, moral)?

(iii) how many end-users use SN for education, communication, entertainment, shopping, business.?

(iv) Among all, what type of attack mostly affected SN users?

(v) How do SN security issues affect daily life?

(vi) How excessive usage of SNS affects users with anxiety and depression?

Table 5: Responses related to SNS Threats.

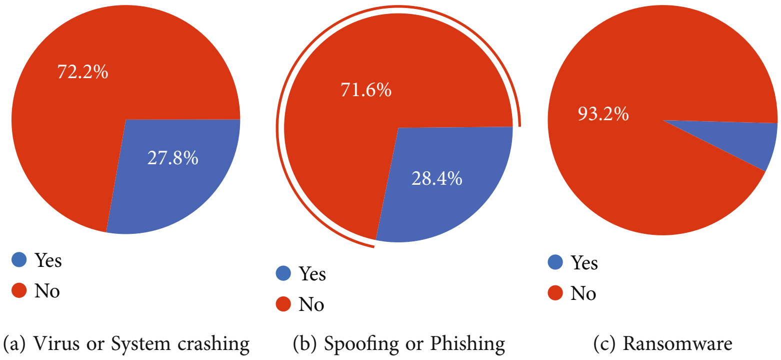
Questions	Yes	No
Do you experience device or system crashing due to any virus attack?	27.8%	72.2%
Do you ever receive spam emails or message which stuck your device?	28.4%	71.6%
Does your data ever been hacked against some ransom amount?	6.8%	93.2%
Has your name ever been used for any fake account activity?	15%	85%
Have your systems or device automatically download unwanted applications?	24.7%	75.3%
Do any irrelevant pop-up ads appear on your systems or device while surfing the internet?	70.6%	29.4%

6.1. Results and Discussion. We gather online survey results of 194 people on social networking security issues, threats, and challenges, which is solved by age group of 10-20 years (57.7%), age group of 21-30 (35.6%) and above than it (6.7%). Based on the daily usage of SNS, people submit responses where 50.5% use it for education purposes, 17.5% use it for shopping purposes, 58.2% use it for entertainment, 37.1% use it for communication, and 9.8% use it for other purposes. Here Figure 6 represents the graph calculation of responses for daily usage of SNS.

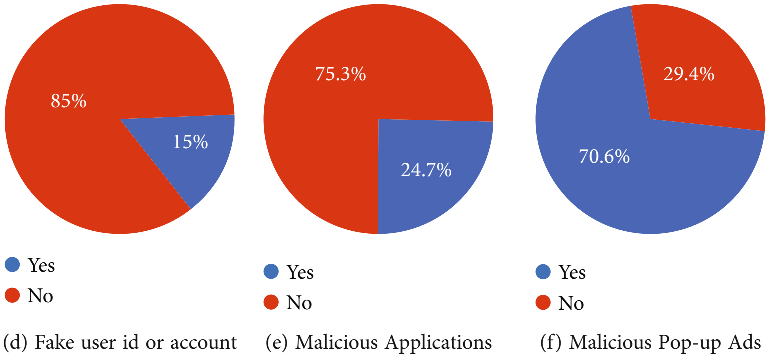
When we talk about SN sites that end users mostly use in their daily routine of surfing. Almost 75.8% of people use social Apps like Facebook, Instagram, YouTube, Twitter, Snapchat, TikTok. While 18.6% people use it for emailing (yahoo, Gmail, Hotmail.) like business, institutes, personal use, trading, and 17% use its other purposes. Figure 7 provides the graphical representation of usage of the networking sites.

The usage of SNS is increasing day by day. The question arises of how many hours end users spend on SN sites. The responses from the survey represent in Figure 8.

AS SNS has many issues, threats, and challenges. Based on some threats and issues, we asked some questions from end-users to share their experience and submit a response. Their responses are shown in Table 5 and the Figure 9 represents the chart of their incidents. In Figure 9(a) show the responses of facing systems crashing and virus attack,

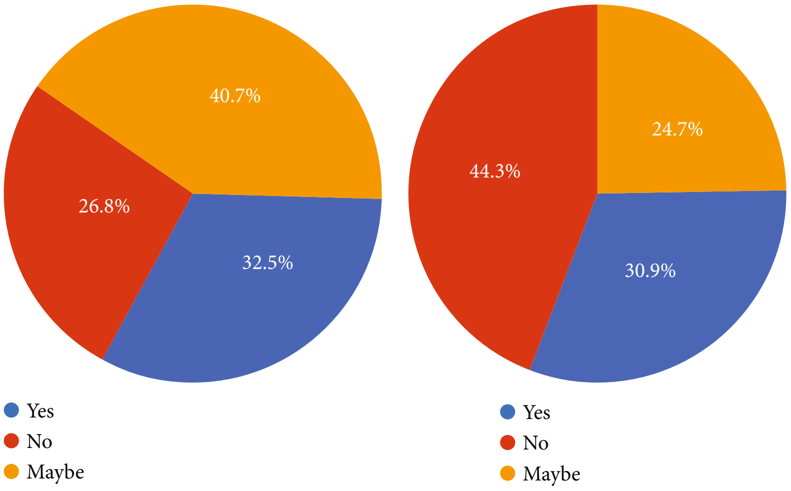


(a) Virus or System crashing (b) Spoofing or Phishing (c) Ransomware



(d) Fake user id or account (e) Malicious Applications (f) Malicious Pop-up Ads

Figure 9: Chart results of SN security attacks of online survey.



(a) SN sites Addiction Rate (b) Facing anxiety or Depression

Figure 10: Charts represents the (a) addiction level of using SN sites and (b) level of anxiety of depression.

Figure 9(b) shows the spoofing and phishing attacks, part (c) shows the ransomware attack, Figure 9(d) shows the responses of fake user IDs or accounts percentage, Figure 9(e) represents the chart of unwanted application downloading attacks. Figure 9(f) shows the pop-up ads or advertisement ads on the window or screen of the devices.

As excessive use of everything is terrible. Free internet availability and easy access to Social networking apps or sites make people addicted. It brings much change to the daily activities of end-users. Figure 10(a) shows the responses of people who become addicted to using SN sites or platforms. A person addicted to SN sites has variant and adverse mood swings, which badly impact their family and social environment. The Covid-19 pandemic makes people lazy and addicted to Social activities, which leads them to anxiety and depression. Figure 10(b) shows the chart of the responses rate of those who suffer from health issues.

Is social networking Sites become a threat to their users. Our online survey asks about the moral, physical, and mental threats due to SN sites. Figure 11 show the graph of responses that 9.8% users feel or face a physical threat as a side effect of SN, 42.8% user faces mental health issues due to excessive or inappropriate use of SN, and 50.5% users feel moral threat by using Social sites.

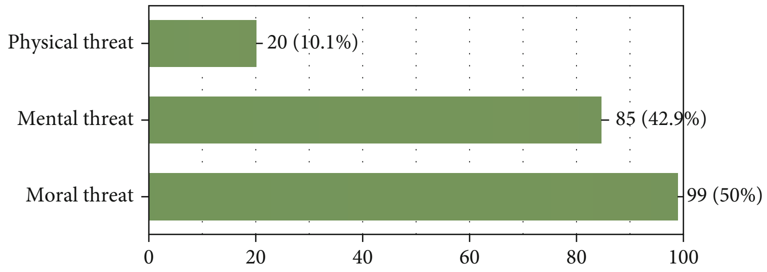


Figure 11: Graph represents the Physical, Mental and moral threat rate as response of online survey.

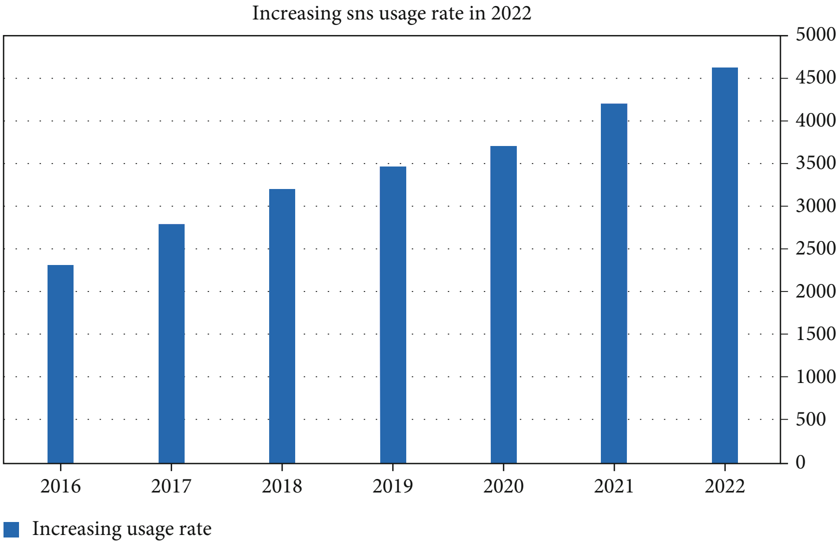


Figure 12: Graph represent the SNS usage increasing rate in 2022.

To conclude our online survey discussion, SNS affects the moral health (with a higher rate 50.5% out of 100%) of users, which leads them towards the inferiority complex, dishonesty, disappointment, anxiety, and depression.

According latest report of Data Reportal organization (https://datareportal.com/reports/digital-2022-global-overview-report), the use of SNS sites increase rapidly which increase the security threats. Figure 12 represent the increasing rate of SNS usage around the globe in year 2022.

Similarly, the changing trend of data hacking & security issues, an online journal illustrates the year 2022 security analysis in their report. Figure 13 represents the most common threats experience by the users, the most common fraud type and increase rate of SNS security issues.

7. Open Research Issues and Challenges of SNS Security

As advancement in Information Technology and Artificial Intelligence increases, Security risks and challenges also Increase. In this research survey, SNS security threats are discussed in-depth. However, researchers and scientists can still provide complete security threat-proof research to make the systems and network threat-free. Here is a list of still existing open issues and Challenges:

(i) Cloud Attacks: Data-centers or cloud-servers-rooms are the main targets of attackers

(ii) Healthcare: SNS has increased the risk of human health; due to excessive use of SNS, the risk for anxiety, depression, less sleep, discomforts, self-harm, mental, physical, immoral, negative thoughts increases rapidly

(iii) Third Party Applications: Most of the time, hackers target the trending keywords or scenarios to target the users

(iv) Phishing Attacks and Scamming: scam emails and messages or pop-ads are the attacker's main hitting point; the attacker will get into the private zone once open

(v) Hacking and Malware Attacks: Fake accounts and users' account hacking will give access to the account to the attacker, and they will handle or run it

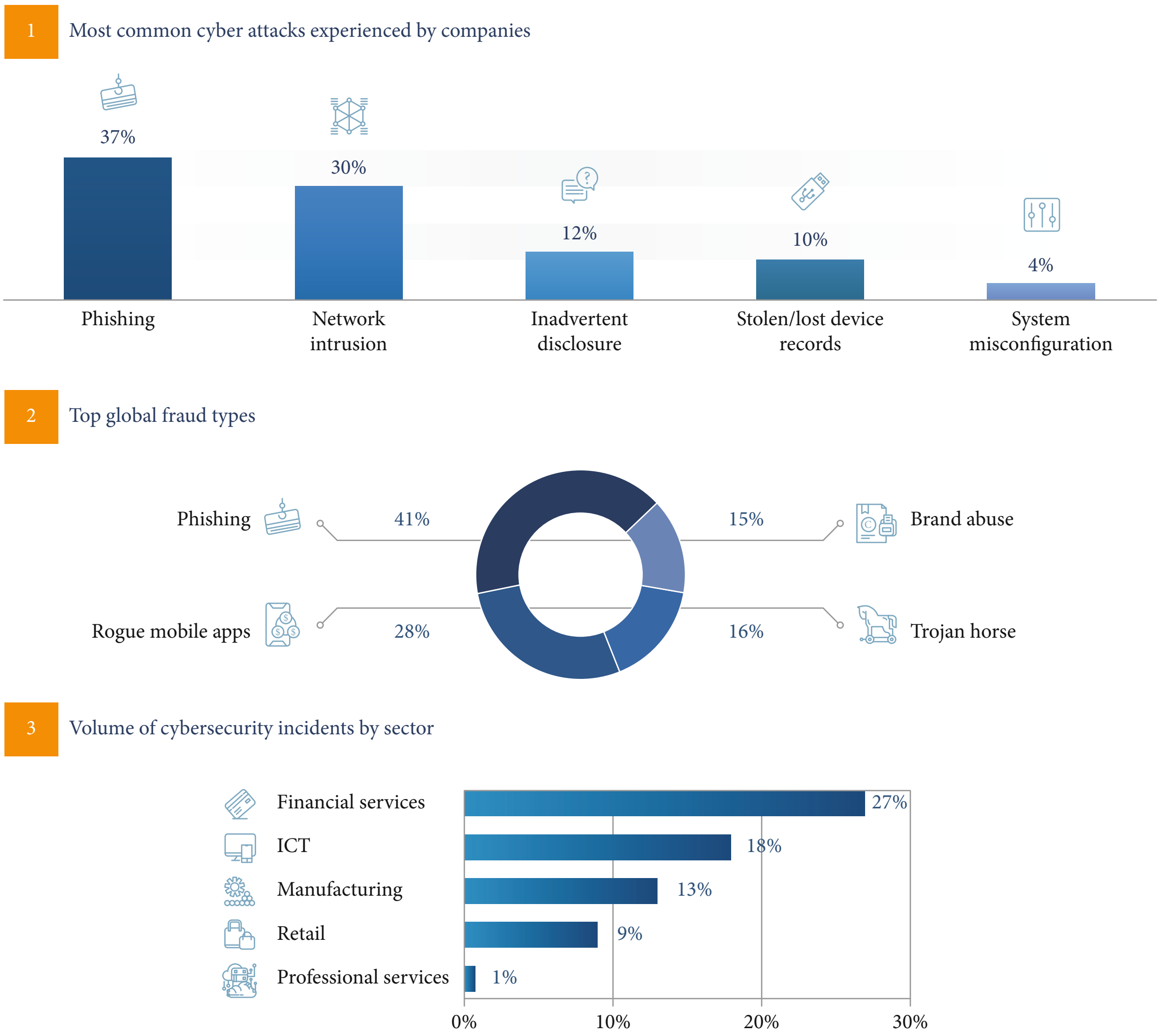


Figure 13: Graph represent the SNS usage increasing rate in 2022.

(vi) Privacy settings and System Updating: Every Application and SNS site has its privacy policy and settings, awareness of its usage and setting is important

8. Future Directions

Social Networking Sites are considered the critical element of today's life. It provides ease to its users at all levels like education, communication, businesses, entertainment, knowledge, sharing platform. Every age group of users is involved in its consumption. As it provides many advantages, it also has similar disadvantages, which can not be ignored. As in our research, we try to discuss all aspects of SNS. So, for future work or directions, we recommend researchers make such advancements which are AI and XAI based including Machine learning and Federated Machine Algorithmic approach to avoid security and privacy threats. Some of the critical directions areas:

(i) Advanced Security Algorithm: many security algorithms exist to control the malware attacks, and from time to time, updation in the security algorithms and the system can keep the systems secured. Including the advanced security and cryptographic techniques makes communication secure by avoiding third party interleaving

(ii) Trust-worthy and Confident Interface:, the process of designing the SNS interface is based on the most important pillar of the strategy, i.e., CIA (confidentiality, integrity, and availability). Establishing efficient security policies by following the CIA strategic methodology can help the devices and system avoid security risks

(iii) Update privacy setting policy: By making solid and dynamic security policies from time to time can help the users to take the initiative at the spur of attacking moment. Setting and designing the parameters, preferences, and priorities helps to make the better performance of Static policies

(iv) User-awareness (most important): One of the most important steps to avoid security threats is to train its users and spread awareness through seminars, online campaigns, events. How to use SNS to avoid privacy breaching and data leakage cases in the future. As we all live in the age of the advanced technological world, SNS is so every day due to easy access to internet facilities. The Covid-19 pandemic itself is a mind-bursting situation for any individual, and they find SNS the best source of entertainment and make them busy; along with that, security countermeasures are most necessary now

(v) Enhanced Security Checking Firewall: Keep your systems and data under protecting shield-like firewall feature, itself an effective way to avoid security threats. Security and Virus detecting systems automatically block suspicious activities and keep your systems and devices threat-free before any damaging situation

(vi) Generating warning and collecting responses: Whenever the system or device detects the threats or warning security or firewall protection shield should be activated automatically to deal with the situation and make the system free from threats. This technique of early warning and collecting responses at the right time helps the researchers and security controlling authority deal with the cases attentively and correctly

(vii) Password protection: Keeping the same password for a long time can make the systems or devices more vulnerable to attack. It is important to change the settings and password after a short period of time to avoid security threats or risks. Try to make the password with a variant and a different name to avoid hacker attacks

(viii) System Access Management: In the organized business or organization, every single end-user needs to have a new and different login facility to the application to avoid double accessing chances. Having separate login and password makes the user more secure and private. Increasing the security techniques improves the system performance and makes a secure environment. Managing the administration and business staff rights must be at the extent level, and data availability and confidentiality are also maintained. Many AI-based machine learning cryptography algorithms have made the system more secure and efficient

9. Conclusion

During the severe pandemic of Covid-19, security becomes the hot topic among all technology researchers. This survey focused on the social networking security threats, issues, and challenges as the world move towards smart technology and human life based on these advancements. As discussed in detail, most possible threats, challenges, and case scenarios happened in Covid-19. We conduct online social networking security-based survey to collect responses of almost 194 people and discuss the possible happening events. We analyze that the Covid-19 pandemic and lockdown situation becomes one of the most challenging periods, affecting users' mental health and morale. For future findings, Machine Learning, deep learning, federated learning, explainable AI, and many other technologies can help the researcher make the social networking infrastructure more secure and efficient as its users feel trustful and confident.

Data Availability

No data were used to support this study. 4

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Abbasi, A. R. Javed, C. Chakraborty, J. Nebhen, W. Zehra, and Z. Jalil, "Elstream: An ensemble learning approach for concept drift detection in dynamic social big data stream learning," *IEEE Access*, vol. 9, pp. 66408–66419, 2021.

[2] C. Sushama, M. S. Kumar, and P. Neelima, "Privacy and Security Issues in the Future: A Social Media," *Materials Today Proceedings*, 2021.

[3] C. M. Gapinski, J. Hermes, and C. von Haaren, "Why people like or dislike large wood in rivers—a representative survey of the general public in Germany," *River Research and Applications*, vol. 37, no. 2, pp. 187–197, 2021.

[4] A. H. Shaikh and B. B. Meshram, "Security issues in cloud computing," in *Intelligent Computing and Networking*, pp. 63–77, Springer, 2021.

[5] A. Ayoub, K. Mahboob, A. R. Javed et al., "Classification and categorization of covid-19 outbreak in pakistan," *Computers, Materials and Continua*, vol. 69, no. 1, pp. 1253–1269, 2021.

[6] T. Issa, M. Al Jaafari, A. S. Alqahtani et al., "Benefits and challenges of social networking during covid-19: personal perspective," *International Journal of Web Based Communities*, vol. 17, no. 2, pp. 135–148, 2021.

[7] C. Iwendi, K. Mahboob, Z. Khalid, A. R. Javed, M. Rizwan, and U. Ghosh, "Classification of covid-19 individuals using adaptive neuro-fuzzy inference system," *Multimedia Systems*, vol. 1–15, 2021.

[8] Z. Jalil, A. Abbasi, A. R. Javed et al., "Covid-19 related sentiment analysis using state-of-the-art machine learning and deep learning techniques," *Frontiers in Public Health*, vol. 9, 2022.

[9] M. Ebibi and M. Fetaji, *Use of social networking tools in online education during the pandemic from covid19*, Skopje, North Macedonia, 2021.

[10] A. Shabbir, M. Shabbir, A. R. Javed, M. Rizwan, C. Iwendi, and C. Chakraborty, "Exploratory data analysis, classification, comparative analysis, case severity detection, and internet of things in covid-19 telemonitoring for smart hospitals," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 1, p. 28, 2022.

[11] K. Saleem, M. Saleem, R. Zeeshan et al., "Situation-Aware Bdi Reasoning to Detect Early Symptoms of Covid 19 Using Smartwatch," *IEEE Sensors Journal*, vol. 1, 2022.

[12] A. Gleiss, M. Kohlhagen, and K. Pousttchi, "An apple a day–how the platform economy impacts value creation in the healthcare market," *Electronic Markets*, vol. 31, no. 4, pp. 849–876, 2021.

[13] M. Rizwan, A. Shabbir, A. R. Javed et al., "Risk monitoring strategy for confidentiality of healthcare information," *Computers & Electrical Engineering*, vol. 100, article 107833, 2022.

[14] P. Mehta, S. Pandya, and K. Kotecha, "Harvesting social media sentiment analysis to enhance stock market prediction using deep learning," *PeerJ Computer Science*, vol. 7, article e476, 2021.

[15] N. Cavus, A. S. Sani, Y. Haruna, and A. A. Lawan, "Efficacy of social networking sites for sustainable education in the era of covid-19: A systematic review," *Sustainability*, vol. 13, no. 2, p. 808, 2021.

[16] J. Simon, T. M. Helter, R. G. White, C. van der Boor, and A. Łaszewska, "Impacts of the covid-19 lockdown and relevant vulnerabilities on capability well-being, mental health and social support: an austrian survey study," *BMC Public Health*, vol. 21, no. 1, pp. 1–12, 2021.

[17] K. Shah, D. Kamrai, H. Mekala, B. Mann, K. Desai, and R. S. Patel, "Focus on mental health during the coronavirus (covid-19) pandemic: applying learnings from the past outbreaks," *Cureus*, vol. 12, no. 3, 2020.

[18] A. R. Javed, L. G. Fahad, A. A. Farhan et al., "Automated cognitive health assessment in smart homes using machine learning," *Sustainable Cities and Society*, vol. 65, article 102572, 2021.

[19] A. R. Javed, M. U. Sarwar, M. O. Beg, M. Asim, T. Baker, and H. Tawfik, "A collaborative healthcare framework for shared healthcare plan with ambient intelligence," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–21, 2020.

[20] R. Rossi, V. Socci, D. Talevi et al., "Covid-19 pandemic and lockdown measures impact on mental health among the general population in italy," *Frontiers in psychiatry*, vol. 11, p. 790, 2020.

[21] R. Nawghare, S. Tripathi, and M. Vardhan, "A survey on social networking using concept of evolutionary algorithms and big data analysis," in *Advances in Computational Intelligence and Communication Technology*, pp. 277–292, Springer, 2021.

[22] E. Michinov and N. Michinov, "Stay at home! When personality profiles influence mental health and creativity during the covid-19 lockdown," *Current Psychology*, pp. 1–12, 2021.

[23] S. Sharma, S. Singh, F. Kujur, and G. Das, "Social media activities and its influence on customer-brand relationship: an empirical study of apparel retailers' activity in India," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 16, no. 4, pp. 602–617, 2021.

[24] H. Shahbaznezhad, R. Dolan, and M. Rashidirad, "TThe Role of Social Media Content Format and Platform in Users' Engagement Behavior," *Journal of Interactive Marketing*, vol. 53, pp. 47–65, 2021.

[25] S. Chen, X. Guo, W. Tianshi, and J. Xiaofeng, "Exploring the Influence of Doctor– Patient Social Ties and Knowledge Ties on Patient Selection," *Internet Research*, 2022.

[26] M. Farooqi, I. Ullah, M. Irfan et al., "The revival of telemedicine in the age of covid-19: benefits and impediments for pakistan," *Annals of Medicine and Surgery*, vol. 69, article 102740, 2021.

[27] L. Evald, I. Wilms, and M. Nordfang, "Assessment of spatial neglect in clinical practice: a nationwide survey," *Neuropsychological Rehabilitation*, vol. 31, no. 9, pp. 1374–1389, 2021.

[28] E. Á. Horvát and E. Hargittai, "Birds of a feather flock together online: Digital inequality in social media repertoires," *Social Media+ Society*, vol. 7, no. 4, article 20563051211052897, 2021.

[29] T. P. Sinha, R. L. Brunda, S. Yadav, and S. Bhoi, "Practice changing innovations for emergency care during the covid-19 pandemic in resource limited settings," *SARS-CoV-2 Origin and COVID-19 Pandemic Across the Globe*, vol. 195, 2021.

[30] H. Gupta and D. Mehrotra, "Socialization between quarantine vehicle and road side unit for handling covid-19: A concept," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1–5, Noida, India, 2021.

[31] R. Aydin and E. Bulut, "Experiences of Nurses Diagnosed with Covid-19 in Turkey: A Qualitative Study," *International Nursing Review*, 2021.

[32] T. Yuanfei, G. Yang, J. Wang, and S. Qingjian, "A secure, efficient and verifiable multimedia data sharing scheme in fog networking system," *Cluster Computing*, vol. 24, no. 1, pp. 225–247, 2021.

[33] E. Ozkan, "Why do consumers behave differently in personal information disclosure and selfdisclosure. The role of personality traits and privacy concern," *Alphanumeric Journal*, vol. 6, pp. 257–276, 2018.

[34] R. Zhang and J. S. Fu, "Privacy management and self-disclosure on social network sites: the moderating effects of stress and gender," *Journal of Computer-Mediated Communication*, vol. 25, no. 3, pp. 236–251, 2020.

[35] A. Sharif, S. H. Soroya, S. Ahmad, and K. Mahmood, "Antecedents of self-disclosure on social networking sites (snss): A study of facebook users," *Sustainability*, vol. 13, no. 3, p. 1220, 2021.

[36] C. Shen, A. Chen, C. Luo, J. Zhang, B. Feng, and W. Liao, "Using reports of symptoms and diagnoses on social media to predict covid-19 case counts in mainland china: Observational infoveillance study," *Journal of medical Internet research*, vol. 22, no. 5, article e19421, 2020.

[37] R. Zhang, N. N. Bazarova, and M. Reddy, "Distress disclosure across social media platforms during the covid-19 pandemic: Untangling the effects of platforms, affordances, and audiences," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–15, Yokohama Japan, 2021.

[38] K. Saha, J. Torous, E. D. Caine, and M. De Choudhury, "Psychosocial effects of the covid-19 pandemic: Large-scale quasiexperimental study on social media," *Journal of medical internet research*, vol. 22, no. 11, article e22600, 2020.

[39] A. Goldenberg, J. J. Gross, and J. J. Gross, "Digital Emotion Contagion," *Trends in Cognitive Sciences*, vol. 24, no. 4, pp. 316–328, 2020.

[40] R. K. Swain and A. K. Pati, "Use of social networking sites (snss) and its repercussions on sleep quality, psychosocial behavior, academic performance and circadian rhythm of

humans – a brief review," *Biological Rhythm Research*, vol. 52, no. 8, pp. 1139–1178, 2021.

[41] M. Gulhane and T. Sajana, "A study of social media data analysis for detecting the effects on human health," *Turkish Journal of Physiotherapy and Rehabilitation*, vol. 32, 2015.

[42] A. Serenko, O. Turel, and H. Bohonis, "The impact of social networking sites use on health-related outcomes among uk adolescents," *Computers in Human Behavior Reports*, vol. 3, article 100058, 2021.

[43] R. R. Wright, A. Evans, C. Schaeffer, R. Mullins, and L. Cast, "Social networking site use: Implications for health and wellness," *Psi Chi Journal of Psychological Research*, vol. 26, no. 2, pp. 165–175, 2021.

[44] B. J. Holmer, S. S. Lapierre, D. E. Jake-Schoffman, and D. D. Christou, "Effects of sleep deprivation on endothelial function in adult humans: a systematic review," *Gero-Science*, vol. 43, no. 1, pp. 137–158, 2021.

[45] R. Sakurai, Y. Nemoto, H. Mastunaga, and Y. Fujiwara, "Who is mentally healthy? mental health profiles of japanese social networking service users with a focus on line, facebook, twitter, and instagram," *Plos one*, vol. 16, no. 3, article e0246090, 2021.

[46] J. Brailovskaia, J. Margraf, and S. Schneider, "Social Media as Source of Information, Stress Symptoms, and Burden Caused by Coronavirus (Covid-19)," *European Psychologist*, 2021.

[47] G. Talis, "Internet addiction," in *Substance and Non-Substance Related Addictions*, pp. 99–107, Springer, 2022.

[48] H. T. N. Ho and H. T. Luong, "Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis," *SN Social Sciences*, vol. 2, no. 1, pp. 1–32, 2022.

[49] N. Mendez-Diaz, G. Akabr, and L. Parker-Barnes, "The evolution of social media and the impact on modern therapeutic relationships," *The Family Journal*, vol. 30, no. 1, pp. 59–66, 2022.

[50] T. Crepax, V. Muntes-Mulero, J. Martinez, and A. Ruiz, "Information technologies exposing children to privacy risks: domains and children-specific technical controls," *Computer Standards & Interfaces*, vol. 82, p. 103624, 2022.

[51] M. R. Vignesh and S. Sivakumar, *Healthcare sensors issues, challenges & security threats in wireless body area network: A comprehensive survey*, 2021.

[52] S. Ghasemshirazi and G. Shirvani, "Gitcbot: A novel approach for the next generation of c&c malware," in *2021 26th International Computer Conference, Computer Society of Iran (CSICC)*, pp. 1–6, Tehran, Iran, 2021.

[53] E. B. Blancaflor, A. B. Alfonso, and K. N. Banganay, "Let's go phishing: A phishing awareness campaign using smishing, email phishing, and social media phishing tools," in *Proceedings of the International Conference on Industrial Engineering and Operations Management*, 2021.

[54] Y. Kano and T. Nakajima, "Trust factors of social engineering attacks on social networking services," in *2021 IEEE 3rd global conference on life sciences and technologies (LifeTech)*, pp. 25–28, Nara, Japan, 2021.

[55] A. Zahid, Q. Zhu, and A. Sohail, "Impact of social networking sites (sns) on human basic privacy rights in pakistan," *Asian Journal of Social Sciences & Humanities*, vol. 10, 2021.

[56] V. D. Sharma, S. K. Yadav, S. K. Yadav, K. N. Singh, and S. Sharma, "An effective approach to protect social media account from spam mail - A machine learning approach," *Materials Today: Proceedings*, 2021.

[57] E. F. E. Ahmet and H. Suliman, "How privacy is threatened from social media communication?," *Computer Science*, vol. 6, no. 1, pp. 32–45, 2021.

[58] A. S. Spoorthy, "Trust based fake node identification in social networking sites," in *IOP Conference Series: Materials Science and Engineering*, vol. 1123, article 012036, IOP Publishing, 2021.

[59] H. Mehraj, D. Jayadevappa, S. L. Haleem et al., "Protection motivation theory using multi-factor authentication for providing security over social networking sites," *Pattern Recognition Letters*, vol. 152, pp. 218–224, 2021.

[60] A. Singh, S. C. Satapathy, A. Roy, and A. Gutub, "Ai-based mobile edge computing for iot: Applications, challenges, and future scope," *Arabian Journal for Science and Engineering*, pp. 1–31, 2022.

[61] S. Min and S.-Y. Yun, "The relationship between sns fatigue, sns immersion and social support recognized by sns due to smart intelligence," in *Smart Healthcare Analytics: State of the Art*, pp. 165–180, Springer, 2022.

[62] M. Koohikamali and N. Gerhart, "False rumor (fake) and truth news spread during a social crisis," in *Proceedings of the 55th Hawaii International Conference on System Sciences*, Hawaii, 2022.

[63] P. Christopher, "Cyberbullying perpetration in the covid-19 era: an application of general strain theory," *The Journal of Social Psychology*, vol. 161, no. 4, pp. 466–476, 2021.

[64] A. Oksanen, R. Oksa, N. Savela, E. Mantere, I. Savolainen, and M. Kaakinen, "Covid-19 crisis and digital stressors at work: a longitudinal study on the finnish working population," *Computers in Human Behavior*, vol. 122, p. 106853, 2021.

[65] R. Yadav, "Cyber security threats during covid-19 pandemic," *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, vol. 12, no. 3, 2021.

[66] A. Banitalebi Dehkordi, M. Soltanaghaei, and F. Z. Boroujeni, "The ddos attacks detection through machine learning and statistical methods in sdn," *The Journal of Supercomputing*, vol. 77, no. 3, pp. 2383–2415, 2021.

[67] W. Ahmed, A. Rasool, A. R. Javed et al., "Security in Next Generation Mobile Payment Systems: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 115932–115950, 2021.

[68] B. Pranggono and A. Arabo, "Covid-19 pandemic cybersecurity issues," *Internet Technology Letters*, vol. 4, no. 2, article e247, 2021.

[69] A. B. Pandey, A. Tripathi, and P. C. Vashist, "A survey of cyber security trends, emerging technologies and threats," in *Cyber Security in Intelligent Computing and Communications*, pp. 19–33, Springer, 2022.

[70] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, pp. 1–39, 2021.

[71] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of ai-enabled phishing attacks detection techniques," *Telecommunication Systems*, vol. 76, no. 1, pp. 139–154, 2021.

[72] P. Bayl-Smith, R. Taib, Y. Kun, and M. Wiggins, "Response to a Phishing Attack: Persuasion and Protection Motivation in an Organizational Context," *Information & Computer Security*, vol. 30, no. 1, pp. 63–78, 2022.

[73] M. Ö. Başeskioğlu and A. Tepecik, "Cybersecurity, computer networks phishing, malware, ransomware, and social engineering anti-piracy reviews," in *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–5, Ankara, Turkey, 2021.

[74] T. Osama, M. S. Razai, and A. Majeed, "Covid-19 vaccine passports: access, equity, and ethics," *BMJ*, vol. 373, 2021.

[75] S. Abijah Roseline and S. Geetha, "A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks," *Computers & Electrical Engineering*, vol. 92, article 107143, 2021.

[76] A. Abusitta, M. Q. Li, and B. C. M. Fung, "Malware classification and composition analysis: A survey of recent developments," *Journal of Information Security and Applications*, vol. 59, article 102828, 2021.

[77] I. V. Alusa, *Data Privacy and Security in Online Social Networks (OSNs)*, PhD thesis, Chuka University, 2021.

[78] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications*, pp. 1–17, 2022.

[79] K. S. Arikumar, S. B. Prathiba, M. Alazab et al., "Fl-pmi: Federated learning-based person movement identification through wearable devices in smart healthcare systems," *Sensors*, vol. 22, no. 4, p. 1377, 2022.

[80] M. Majid, S. Habib, A. R. Javed et al., "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review," *Sensors*, vol. 22, no. 6, p. 2087, 2022.

[81] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2, article 100013, 2021.

[82] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A survey on ransomware: Evolution, taxonomy, and defense solutions," 2021, https://arxiv.org/abs/2102.06249.

[83] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: evolution, mitigation and prevention," *Egyptian Informatics Journal*, vol. 22, no. 1, pp. 105–117, 2021.

[84] S. Dalal, Z. Wang, and S. Sabharwal, "Identifying ransomware actors in the bitcoin network," 2021, https://arxiv.org/abs/2108.13807.

[85] B. Barani Sundaram, T. Kedir, M. K. Mishra, S. H. Yesuf, S. M. Tiwari, and P. Karthika, "Security analysis for sybil attack in sensor network using compare and matchposition verification method," in *Mobile Computing and Sustainable Informatics*, pp. 55–64, Springer, 2022.

[86] R. Almesaeed and E. Al-Salem, "Sybil attack detection scheme based on channel profile and power regulations in wireless sensor networks," *Wireless Networks*, vol. 28, no. 4, pp. 1361–1374, 2022.

[87] S. Kawuma and E. Nabaasa, "An empirical study of bugs in eclipse stable internal interfaces," 2022, https://arxiv.org/abs/2203.09134.

[88] H. Wenninger, C. M. K. Cheung, and M. Chmielinski, "Understanding envy and users' responses to envy in the context of social networking sites: A literature review," *International Journal of Information Management*, vol. 58, article 102303, 2021.

[89] H. T. Reda, A. Anwar, and A. Mahmood, "Comprehensive survey and taxonomies of false injection attacks in smart grid: Attack models, targets, and impacts," 2021, https://arxiv.org/abs/2103.10594.

[90] N. Jose, "Detecting malicious behavior in social platforms via hybrid knowledge- and data-driven systems," *Future Generation Computer Systems*, vol. 125, pp. 232–246, 2021.

[91] J. Jia, Z. Dong, J. Li, and J. W. Stokes, "Detection of malicious dns and web servers using graph-based approaches," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2625–2629, Toronto, ON, Canada, 2021.

[92] M. A. Omer, S. R. Zeebaree, M. A. Sadeeq et al., "Efficiency of malware detection in android system: A survey," *Asian Journal of Research in Computer Science*, pp. 59–69, 2021.

[93] M. Senthil Raja and L. Arun Raj, "Detection of malicious profiles and protecting users in online social networks," *Wireless Personal Communications*, pp. 1–18, 2021.

[94] F. Al-Turjman and R. Salama, "Cyber security in mobile social networks," in *Security in IoT Social Networks*, pp. 55–81, Elsevier, 2021.

[95] D. Voramontri and L. Klieb, "Impact of Social media on Consumer Behaviour," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 5, pp. 1216–1225, 2021.

[96] N. Tripathi and N. Hubballi, "Application layer denial-of-service attacks and defense mechanisms: a survey," *ACM Computing Surveys (CSUR)*, vol. 54, no. 4, pp. 1–33, 2021.

[97] S. L. Kumar, Y. S. Asish, and S. Ganapathy, *A new hybrid cnn-lstm model with non-softmax functions for face spoof detection*, 2021.

[98] P. R. Patil and S. S. Kulkarni, "Survey of non-intrusive face spoof detection methods," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 14693–14721, 2021.

[99] S. S. Khalil, S. M. Youssef, and S. N. Saleh, "iCaps-dfake: An integrated capsule-based model for deepfake image and video detection," *Future Internet*, vol. 13, no. 4, p. 93, 2021.

[100] W. Ren, X. Zhu, and H. Yi, "Differential effects of traditional and social media use on covid-19 preventive behaviors: the mediating role of risk and efficacy perceptions," *Journal of Health Psychology*, p. 135910532110031, 2021.

[101] S. Altalhi and A. Gutub, "A survey on predictions of cyber-attacks utilizing real-time twitter tracing recognition," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 11, pp. 10209–10221, 2021.

[102] A. Stephen and L. Arockiam, "Attacks against rplin iot: a survey," *Annals of the Romanian Society for Cell Biology*, pp. 9767–9786, 2021.

[103] M. Kolomeets and A. Chechulin, "Analysis of the malicious bots market," in *2021 29th conference of open innovations association (FRUCT)*, pp. 199–205, 2021.

[104] J. A. Bapaye and H. A. Bapaye, "Demographic factors influencing the impact of coronavirus-related misinformation on whatsapp: Cross-sectional questionnaire study," *JMIR Public Health and Surveillance*, vol. 7, no. 1, article e19858, 2021.

[105] A. Majeed, "Towards privacy paradigm shift due to the pandemic: A brief perspective," *Inventions*, vol. 6, no. 2, p. 24, 2021.

[106] A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay, "A survey on adversarial attacks and

defences," *CAAI Transactions on Intelligence Technology*, vol. 6, no. 1, pp. 25–45, 2021.

[107] L. P. Rondon, L. Babun, A. Aris, K. Akkaya, and A. S. Uluagac, "Survey on enterprise internet-of-things systems (e-iot): A security perspective," 2021, https://arxiv.org/abs/2102.10695.

[108] T. Jones, *Social Media and the Effects on the Everyday User*, PhD thesis, Utica College, 2021.

[109] M. Devi and A. Majumder, "Sidechannel attack in internet of things: A survey," in *Applications of Internet of Things*, pp. 213–222, Springer, 2021.

[110] M. Bhattacharya, S. Roy, S. Banerjee, and S. Chattopadhyay, "Cryptanalysis of a centralized location-sharing scheme for mobile online social networks," in *Advanced Computing and Systems for Security*, pp. 17–30, Springer, 2021.

[111] C. Lyu, D. Huang, Q. Jia et al., "Predictable model for detecting sybil attacks in mobile social networks," in *2021 IEEE wireless communications and networking conference (WCNC)*, pp. 1–6, Nanjing, China, 2021.

[112] S. N. Al-Humairi and A. A. Kamal, "Design a smart infrastructure monitoring system: a response in the age of covid-19 pandemic," *Innovative Infrastructure Solutions*, vol. 6, no. 3, pp. 1–10, 2021.

[113] S. N. Al-Humairi and A. A. Kamal, "Opportunities and challenges for the building monitoring systems in the age-pandemic of covid-19: review and prospects," *Innovative Infrastructure Solutions*, vol. 6, no. 2, pp. 1–10, 2021.

[114] M. A. Throuvala, M. D. Griffiths, M. Rennoldson, and D. J. Kuss, "Perceived challenges and online harms from social media use on a severity continuum: a qualitative psychological stakeholder perspective," *International journal of environmental research and public health*, vol. 18, no. 6, p. 3227, 2021.

[115] M. Y. Alemdar, "Instagram Teachings and Relative Poverty," in *New Challenges for Future Sustainability and Wellbeing*, Emerald Publishing Limited, 2021.

[116] A. Guinchard, "Our digital footprint under covid-19: should we fear the Uk digital contact tracing app?," *International Review of Law, Computers & Technology*, vol. 35, no. 1, pp. 84–97, 2021.

[117] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: a survey," *IEEE Communication Surveys and Tutorials*, vol. 20, no. 2, pp. 1397–1417, 2018.

[118] D. Alfred, "Personal information privacy settings of online social networks and their suitability for mobile internet devices," 2013, https://arxiv.org/abs/1305.2770.

[119] M. Thangavel, M. Divyaprabha, and C. Abinaya, "Threats and vulnerabilities of mobile applications," in *Research Anthology on Securing Mobile Technologies and Applications*, pp. 560–580, IGI Global, 2021.

[120] S. R. Sahoo and B. B. Gupta, "Multiple features based approach for automatic fake news detection on social networks using deep learning," *Applied Soft Computing*, vol. 100, article 106983, 2021.

[121] C. Wentao, L. Kuok-Tiung, L. Wei, P. Bhambri, and S. Kautish, "Predicting the security threats of internet rumors and spread of false information based on sociological principle," *Computer Standards & Interfaces*, vol. 73, article 103454, 2021.

[122] Z. Yan, L. Peng, W. Feng, and L. T. Yang, "Social-Chain," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 1, pp. 1–28, 2021.

[123] Y. Sadqi and Y. Maleh, "A systematic review and taxonomy of web applications threats," *Information Security Journal: A Global Perspective*, pp. 1–27, 2022.

[124] A. Abbasi, D. Dobolyi, A. Vance, and F. M. Zahedi, "The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites," *Information Systems Research*, vol. 32, no. 2, pp. 410–436, 2021.

[125] P. A. Barraclough, G. Fehringer, and J. Woodward, "Intelligent cyber-phishing detection for online," *Computers & Security*, vol. 104, article 102123, 2021.

[126] M. Canham, C. Posey, D. Strickland, and M. Constantino, "Phishing for long tails: Examining organizational repeat clickers and protective stewards," *SAGE Open*, vol. 11, no. 1, p. 2158244021990656, 2021.

[127] K. Pradeep Mohan Kumar, M. Saravanan, M. Thenmozhi, and K. Vijayakumar, "Intrusion detection system based on ga-fuzzy classifier for detecting malicious attacks," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 3, article e5242, 2021.

[128] A. O. Alzahrani and M. J. F. Alenazi, "Designing a network intrusion detection system based on machine learning for software defined networks," *Future Internet*, vol. 13, no. 5, p. 111, 2021.

[129] M. Mohammadi, T. A. Rashid, S. H. Karim et al., "A comprehensive survey and taxonomy of the svm-based intrusion detection systems," *Journal of Network and Computer Applications*, vol. 178, article 102983, 2021.

[130] C.-J. Chew, Y.-C. Chen, J.-S. Lee, C.-L. Chen, and K.-Y. Tsai, "Preserving indomitable ddos vitality through resurrection social hybrid botnet," *Computers & Security*, vol. 106, article 102284, 2021.

[131] P. M. Rao and P. Saraswathi, "Evolving cloud security technologies for social networks," in *Security in IoT Social Networks*, pp. 179–203, Elsevier, 2021.

[132] H. Huang, J. Chu, and X. Cheng, "Trend analysis and countermeasure research of ddos attack under 5g network," in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, pp. 153–160, Zhuhai, China, 2021.

[133] D. Parashar, L. M. Sanagavarapu, and Y. R. Reddy, "Sql injection vulnerability identification from text," in *14th Innovations in Software Engineering Conference (formerly known as India Software Engineering Conference)*, pp. 1–5, 2021.

[134] U. Farooq, "Ensemble machine learning approaches for detection of sql injection attack," *Tehniˇcki glasnik*, vol. 15, no. 1, pp. 112–120, 2021.

[135] A. J. Gabriel, A. Darwish, and A. E. Hassanien, "Cyber security in the age of covid-19," *Studies in systems decision and Control*, vol. 322, pp. 275–295, 2021.

[136] D. Alharthi, "Amelia ReganSocial engineering infosec policies (se-ips)," in *The 14th International Conference on Network Security & Applications (CNSA 2021)*, pp. 521–541, 2021.

[137] V. Okditazeini and I. Irwansyah, "Ancaman privasi dan data mining di era digital: Analisis meta-sintesis pada social networking sites (sns)," *Jurnal Studi Komunikasi Dan Media*, vol. 22, no. 2, pp. 109–122, 2018.

[138] M. F. Andersen, J. M. Pedersen, and E. Vasilomanolakis, “Using netflow to measure the impact of deploying dnsbased blacklists,” in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering: Security and Privacy in Communication Networks. SecureComm 2021*, Springer, 2021.

[139] D. Arsenault, *Securing dns services through system self cleansing and hardware enhancements*.

[140] J. Liu and J. Zhao, “More than plain text: censorship deletion in the chinese social media,” *Journal of the Association for Information Science and Technology*, vol. 72, no. 1, pp. 18–31, 2021.

[141] N. Yuvaraj, K. Srihari, G. Dhiman et al., “Nature-inspired-based approach for automated cyberbullying classification on multimedia social networking,” *Mathematical Problems in Engineering*, vol. 2021, 12 pages, 2021.

[142] K. Srinivasan, G. Rathee, M. R. Raja, N. Jaglan, T. V. Mahendiran, and T. Palaniswamy, “Secure multimedia data processing scheme in medical applications,” *Multimedia Tools and Applications*, pp. 1–12, 2022.

[143] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, “Blockchain Technology Applications in Healthcare: An Overview,” *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021.

[144] A. Altalbe and F. Kateb, “Assuring Enhanced Privacy Violation Detection Model for Social Networks,” *International Journal of Intelligent Computing and Cybernetics*, vol. 15, no. 1, pp. 75–91, 2022.

[145] M. Kumar, P. Mukherjee, K. Verma, S. Verma, D. B. Rawat, and D. B. Rawat, “Improved Deep Convolutional Neural Network Based Malicious Node Detection and Energy-Efficient Data Transmission in Wireless Sensor Networks,” *IEEE Transactions on Network Science and Engineering*, 2021.

[146] M. Mehmood, T. Javed, J. Nebhen et al., “A hybrid approach for network intrusion detection,” *CMC-Computers Materials & Continua*, vol. 70, no. 1, pp. 91–107, 2022.

[147] R. Abid, C. Iwendi, A. R. Javed et al., “An optimised homomorphic crtrsa algorithm for secure and efficient communication,” *Personal and Ubiquitous Computing*, pp. 1–14, 2021.

[148] A. A. Ikram, A. R. Javed, M. Rizwan, R. Abid, J. Crichigno, and G. Srivastava, “Mobile cloud computing framework for securing data,” in *2021 44th International Conference on Telecommunications and Signal Processing (TSP)*, pp. 309–315, Brno, Czech Republic, 2021.

[149] P. M. Valkenburg, A. Meier, and I. Beyens, “Social media use and its impact on adolescent mental health: An umbrella review of the evidence,” *Current opinion in psychology*, vol. 44, pp. 58–68, 2022.

[150] A. Amanat, M. Rizwan, A. R. Javed et al., “Deep learning for depression detection from textual data,” *Electronics*, vol. 11, no. 5, p. 676, 2022.

[151] M. Rizwan, A. Shabbir, A. R. Javed, M. Shabbir, T. Baker, and D. al-Jumeily Obe, “Brain Tumor and Glioma Grade Classification Using Gaussian Convolutional Neural Network,” *IEEE Access*, vol. 10, pp. 29731–29740, 2022.

[152] Z. Yue, R. Zhang, and J. Xiao, “Passive social media use and psychological wellbeing during the covid-19 pandemic: The role of social comparison and emotion regulation,” *Computers in Human Behavior*, vol. 127, article 107050, 2022.

[153] M. Nyamadi and P. Tsibolane, “Exploring the problematic consumption of digital platforms during the covid-19 pandemic among university students in africa,” in *Digital Innovations, Business and Society in Africa*, pp. 229–249, Springer, 2022.

[154] M. A. Shabbir, F. Mehak, Z. M. Khan et al., “Delving the Role of Nutritional Psychiatry to Mitigate the Covid-19 Pandemic Induced Stress, Anxiety and Depression,” *Trends in Food Science & Technology*, vol. 120, pp. 25–35, 2022.

[155] K. Sekścińska and D. Jaworska, “Who felt blue when facebook went down?-the role of self-esteem and fomo in explaining people’s mood in reaction to social media outage,” *Personality and Individual Differences*, vol. 188, article 111460, 2022.

[156] Y. Wang, X. Guo, M. Wang et al., “Transcranial direct current stimulation of bilateral dorsolateral prefrontal cortex eliminates creativity impairment induced by acute stress,” *International Journal of Psychophysiology*, vol. 171, pp. 1–11, 2022.

[157] L. O’Meara, C. Turner, D. C. Coitinho, and S. Oenema, “Consumer experiences of food environments during the covid-19 pandemic: Global insights from a rapid online survey of individuals from 119 countries,” *Global food security*, vol. 32, article 100594, 2022.

[158] H. Zhang, L. Xue, Y. Jiang, M. Song, D. Wei, and G. Liu, “Food delivery waste in wuhan, china: Patterns, drivers, and implications,” *Resources, Conservation and Recycling*, vol. 177, article 105960, 2022.

[159] I. K. Milaković and D. Miocevic, “Consumer’s transition to online clothing buying during the covid-19 pandemic: exploration through protection motivation theory and consumer well-being,” *Journal of Fashion Marketing and Management: An International Journal*, 2022.

[160] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, “Cyber security in iot-based cloud computing: A comprehensive survey,” *Electronics*, vol. 11, no. 1, p. 16, 2021.

[161] A. Mohiyuddin, A. R. Javed, C. Chakraborty, M. Rizwan, M. Shabbir, and J. Nebhen, “Secure cloud storage for medical iot data using adaptive neuro-fuzzy inference system,” *International Journal of Fuzzy Systems*, pp. 1–13, 2021.

[162] P. Kumar, G. P. Gupta, and R. Tripathi, “Design of anomaly-based intrusion detection system using fog computing for iot network,” *Automatic Control and Computer Sciences*, vol. 55, no. 2, pp. 137–147, 2021.

[163] P. Kumar, G. P. Gupta, and R. Tripathi, “Pefl: Deep Privacy-Encoding Based Federated Learning Framework for Smart Agriculture,” *IEEE Micro*, 2022.

[164] P. B. Narasingapuram, “A secure cloud authentication and access control system for cloud infrastructure,” *Information Technology in Industry*, vol. 9, no. 2, pp. 1296–1300, 2021.

[165] A. Sai Prasanna, J. Tejeswini, and N. Mohankumar, “Limes: Logic locking on interleaved memory for enhanced security,” in *Computer Networks, Big Data and IoT*, pp. 613–626, Springer, 2021.

[166] G. Li, H. Yang, J. Zhang, H. Liu, and A. Hu, “Fast and secure key generation with channel obfuscation in slowly varying environments,” 2021, https://arxiv.org/abs/2112.02273.

[167] U. Aziz, M. U. Gurmani, S. Awan, M. B. Sajid, S. Amjad, and N. Javaid, “A blockchain based secure authentication and routing mechanism for wireless sensor networks,” in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Cham, 2021.

[168] T. Alvarez and H.-C. Chen, “Meta-Analysis of social networking sites for the purpose of preventing privacy threats

in the digital age," *Journal of Applied Data Sciences*, vol. 2, no. 3, pp. 64–73, 2021.

[169] O.-K. D. Lee, S. Lee, W. Suh, and Y. Chang, "Alleviating the Impact of Sns Fatigue on User Discontinuance," *Industrial Management & Data Systems*, 2021.

[170] M. Dorasamy, M. Kaliannan, M. Jambulingam, I. Ramadhan, and A. Sivaji, "Parents' awareness on online predators: cyber grooming deterrence," *The Qualitative Report*, vol. 26, no. 11, pp. 3683–3723, 2021.

[171] R. Chen, D. J. Kim, and H. R. Rao, "A study of social networking site use from a three-pronged security and privacy threat assessment perspective," *Information & Management*, vol. 58, no. 5, article 103486, 2021.