IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INTERNET-OF-THINGS ATTACKS AND DEFENSES: RECENT ADVANCES AND CHALLENGES

Received June 13, 2020, accepted June 27, 2020, date of publication June 30, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3006172

Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies

SAQIB HAKAK[1], (Member, IEEE), WAZIR ZADA KHAN[2], (Senior Member, IEEE), MUHAMMAD IMRAN[3], (Member, IEEE), KIM-KWANG RAYMOND CHOO[4], (Senior Member, IEEE), AND MUHAMMAD SHOAIB[5]

[1]Faculty of Computer Science, University of Northern British Columbia, Prince George, BC V2N 4Z9, Canada
[2]Faculty of CS & IS, Jazan University, Jazan 45142, Saudi Arabia
[3]College of Applied Computer Science, King Saud University, Riyadh 11451, Saudi Arabia
[4]Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249, USA
[5]College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia

Corresponding author: Muhammad Imran (cimran@ksu.edu.sa)

This work was supported in part by the University of Northern British Columbia under Grant FUND 15021 ORG 4460, and in part by the Deanship of Scientific Research (DSR) at King Saud University through research group project under Grant RG-1439-036.

ABSTRACT Cybercriminals are constantly on the lookout for new attack vectors, and the recent COVID-19 pandemic is no exception. For example, social distancing measures have resulted in travel bans, lockdowns, and stay-at-home orders, consequently increasing the reliance on information and communications technologies, such as Zoom. Cybercriminals have also attempted to exploit the pandemic to facilitate a broad range of malicious activities, such as attempting to take over videoconferencing platforms used in online meetings/educational activities, information theft, and other fraudulent activities. This study briefly reviews some of the malicious cyber activities associated with COVID-19 and the potential mitigation solutions. We also propose an attack taxonomy, which (optimistically) will help guide future risk management and mitigation responses.

INDEX TERMS COVID-19, cyberattacks, security and privacy, taxonomy, mitigation, potential solutions.

I. INTRODUCTION

COVID-19, which is also referred to as novel coronavirus, 2019-nCoV, or SARS-CoV-2, is among the worst pandemics in recent times and has resulted in numerous countries introducing travel bans, social distancing, lockdowns, and stay-at-home orders [1]. These measures have a broad range of consequences, including those shown in Figure 1. For example, one of the trends is increased remote working and education arrangements, such as using videoconferencing software (e.g., Zoom, Microsoft Teams, and Skype Business) for work and educational purposes.[1]

Corresponding security and privacy risks have also been observed. For example, Singapore's Minister for Home Affairs indicated that between January and April 2020, "a total of 394 scams related to Covid-19 were reported and victims were cheated of at least SGD 1.4 million".[2] The Australian Competition and Consumer Commission's Scamwatch also reportedly received over 2,700 COVID-19-related scam reports, with an estimated loss of over AUD 16,390,650 as of April 2020.[3] The US Federal Trade Commission estimated that USD 12 million dollars were lost from COVID-19-related fraudulent activities between January and April 14, 2020, with a total of 18,235 reports related to COVID-19 and up to USD 13.44 million dollars were lost to fraud.[4] The affected victims

The associate editor coordinating the review of this manuscript and approving it for publication was Shaohua Wan.

[1]https://www.marketwatch.com/story/zoom-microsoft-cloud-usage-are-rocketing-during-coronavirus-pandemic-new-data-show-2020-03-30, last accessed June 4, 2020.

[2]https://www.todayonline.com/singapore/close-400-covid-19-related-scams-reported-s14-million-cheated-january-april, last accessed June 4, 2020.

[3]https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams, last accessed June 4, 2020.

[4]https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers, last accessed June 4, 2020.

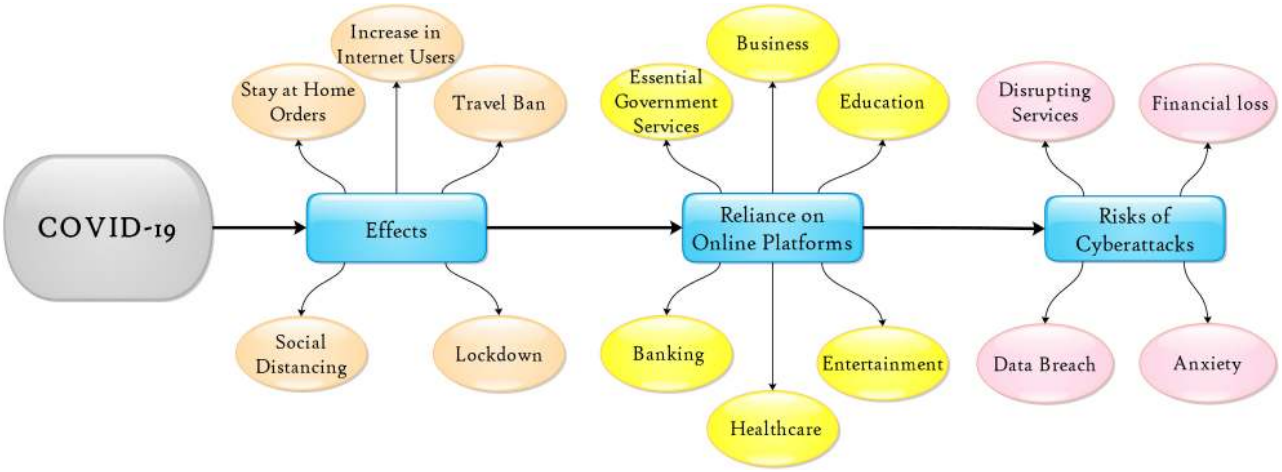


FIGURE 1. Effects of COVID-19 Pandemic.

TABLE 1. Examples of COVID-19-related cyber incidents.

Sources	Summary
www.forbes.com	Hammersmith Medicines Research, a London-based coronavirus vaccine testing facility, was reportedly affected by ransomware. Given that the facility did not pay the ransom amount, personal records of thousands of patients' information were published online.
www.msn.com	Distributed denial of service (DDoS) attacks were launched against the US Health and Human Services departmental servers.
www.reuters.com	The World Health Organization (WHO) was reportedly targeted by an advanced persistent threat (APT) actor called DarkHotel, who attempted to steal the passwords of WHO members.
www.reuters.com	E-mail accounts of several employees of Monte dei Paschi, an Italian state-owned bank, was reportedly hacked to gain access to sensitive information.
www.independent.co.uk	Johns Hopkins University created a map to track global COVID-19 cases, but it was reportedly abused by cyber criminals to infect users and steal their passwords as soon as a user clicks on the map.
www.cnet.com	A spyware campaign was reportedly launched through fake applications, such as corona live 1.1, to carry out surveillance activities.

range from organizations (e.g., educational and commercial entities), governments, to individuals, such as those listed in Table 1. Reports also indicated that urgent surgeries had to be postponed [2]–[4]. However, an extremely challenging endeavor is quantifying the losses (e.g., financial and social) caused by cyberattacks associated with this pandemic, or even fully comprehending the entire threat landscape.

To the best of our knowledge, this study is the first attempt to provide an overview of cyberattacks prevalent during the COVID-19 pandemic. However, possible new attacks could have been perpetrated because the pandemic was still ongoing when this research was being conducted.

This study attempts to map some of these attacks based on categories (see Section III-A). We use these attack categories as bases to discuss potential mitigation strategies (see Section IV). The main contributions of this study are as follows:

- Identify various COVID-19-related cyber threats,
- Develop a new taxonomy of attacks and their effects on security goals, and
- Discuss the potential mitigation strategies to counter the identified threats.

The remainder of this paper is organized as follows. Section 2 briefly reviews the related literature. Section 3 discusses the COVID-19 related cyberattacks prior to the presentation of the taxonomy and potential mitigation strategies in the next section. Sections 4 and 5 present the discussion and conclusion, respectively.

II. LITERATURE REVIEW

Cybersecurity is the process of securing assets, networks, programs, and data from any unauthorized access or attack. The evolving nature of attacks makes cybersecurity one of the challenging research areas. To understand information flow within cybersecurity, an important aspect is gaining familiarity with a few key terms, namely, adversary or threat agent, threat, risk, attack, vulnerability, security policy, assets, and countermeasures. Brief descriptions of these terms are provided in Table 2 [5], while the relationship of these terms is presented in Figure 2. Several standard organizations, such as the International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST), are involved in mitigating the impact of cyberattacks. These organizations are responsible for developing cybersecurity frameworks, security protocols, and guidelines to minimize the impact of attacks. For example, a latest versatile cybersecurity framework proposed by NIST is version 1.1 [6], which is mainly designed for critical infrastructure. A risk

TABLE 2. Key Security Terms.

Terms	Definition
Adversary	Individuals or groups with the aim of carrying out inimical activities
Threat	Any event or situation with the potential of adversely affecting information system sources
Risk	Measure of probability loss resulting from an attack
Attack	Threat carried out by an adversary to collect, disrupt, or damage information system sources
Vulnerability	Any weakness spot within information system resources that can be exploited by an adversary
Security policy	Set of guidelines to maintain the security provisions of an information system resource
Assets	Entity to be protected from attacks and includes hardware, software, data, and networks
Countermeasures	Approaches to mitigate or prevent attacks to secure assets

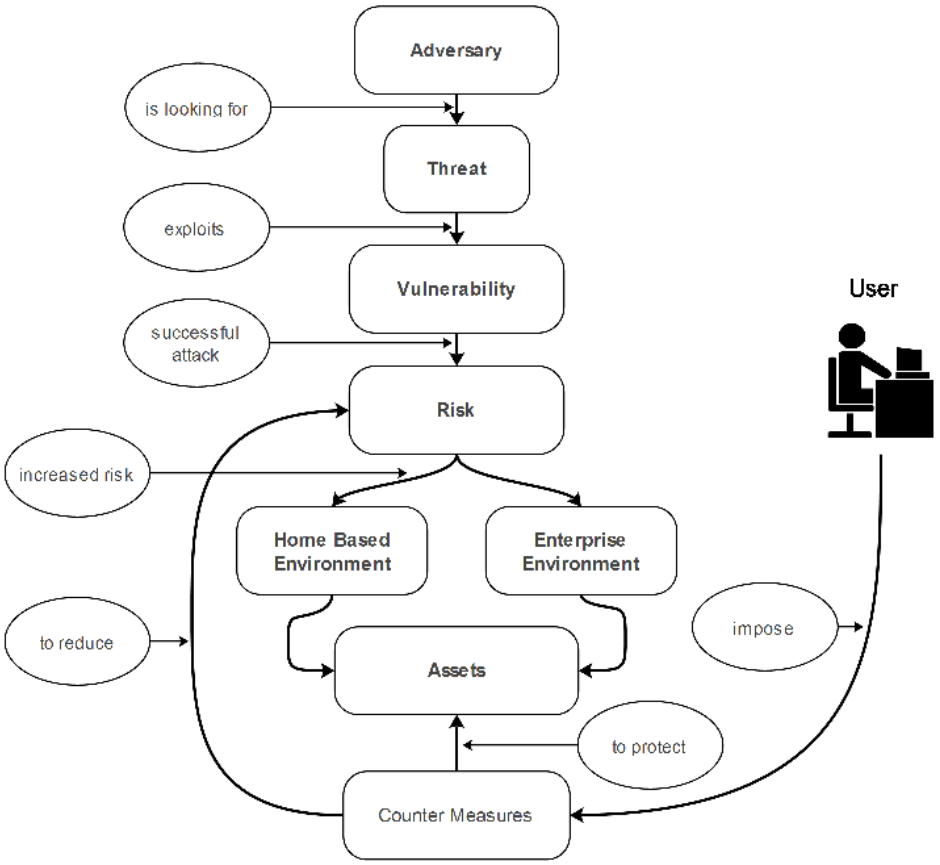


FIGURE 2. Relationship among threat, vulnerability, and risk.

management framework was proposed by ISO under standard ISO-31000 [7]. Although several other cybersecurity frameworks are suitable for small and large organizations, the suitability of these frameworks amid the COVID-19 pandemic has yet to be validated. Extensive research should be pursued in this domain, particularly on whether existing cybersecurity frameworks are sufficiently effective to minimize the risks associated with evolving work environments.

At present, only few studies have highlighted the effects of COVID-19 in terms of cybersecurity because the majority of the current studies have mostly focused on security, privacy and trust aspects in wireless sensor networks (WSNs) [8], Internet of Things (IoT) [9]–[13], software-defined IoT using edge computing ecosystems [14], smart cities [15], [16], and industrial IoT (IIoT) [17]. However, we were able to find few interesting articles that worked in this direction. Although the majority of the studies have highlighted the implications of tracking applications that violate privacy concerns [18], [19]. One such study has raised concerns in installing the related apps (e.g., TraceTogether, a mobile phone app released by the Singaporean government) [20]. This app works by exchanging tokens with nearby Bluetooth devices. When users are diagnosed with COVID-19, health officials ask users to share such an information via app, thereby possibly leading to different privacy attack, such as simple linkage attack [21].

To date, only a few approaches have been proposed to mitigate privacy concerns. Reference [22] claimed that healthcare data collection is at risk from being compromised by adversaries. To make data collection markedly secure, the authors have proposed a privacy-preservation application

TABLE 3. Existing COVID-19 related studies.

	Cyberattacks	Security and Privacy Concerns	Role of Emerging Technologies for Tracking and Monitoring	Prediction and Diagnosis
Z. Allam *et al.* [2]	✗	✗	✓	✗
H. Cho *et al.* [20]	✗	✓	✗	✗
A. De Carly *et al.* [22]	✗	✓	✗	✗
P. Gupta *et al.* [23]	✗	✓	✗	✗
Z. Yang *et al.* [24]	✗	✗	✗	✓
B. Pirouz *et al.* [25]	✗	✗	✗	✓
A. Kumar *et al.* [26]	✗	✗	✓	✗
L. Wynants *et al.* [27]	✗	✗	✗	✓
X. Meng *et al.* [28]	✗	✗	✓	✗
M. Javaid *et al.* [29]	✗	✗	✓	✗
C. J. Wang *et al.* [30]	✗	✗	✓	✓
V. Chamola *et al.* [31]	✗	✗	✓	✗
This Study	✓	✓	✗	✗

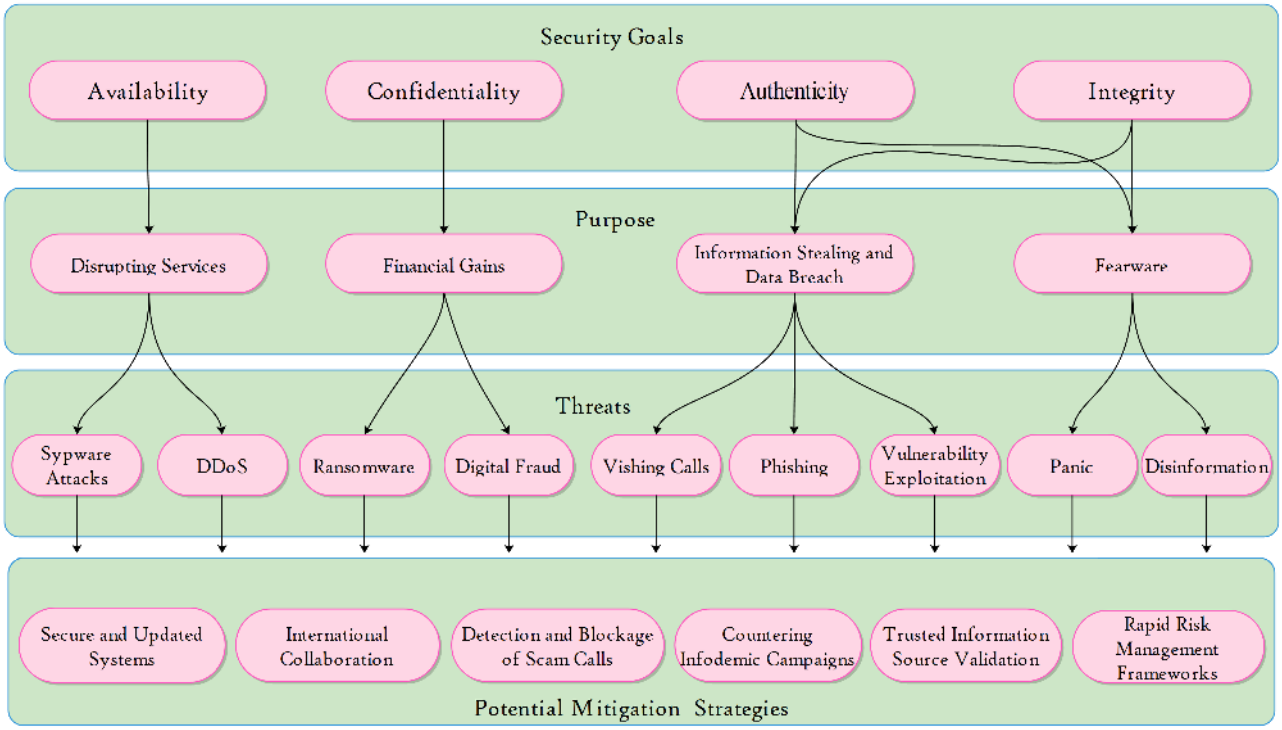


FIGURE 3. Taxonomy of the COVID-19-themed Cyber incidents.

called Wetrace, which uses Bluetooth low energy for the message to reach its destination. Reference [23] proposed QUEST, a WiFi-based privacy-preservation technology to track individuals and their interactions. The aforementioned study discussed that existing tracking approaches, such as Bluetooth beacons and smartphone apps, violate individual privacy rights and needs proper privacy-preservation-based approach.

The other studies that highlighted the cybersecurity issues that arised owing to this pandemic include the work of [32], which feature the sectors severely affected by the pandemic and the need for proper security measures to prevent cyberattacks. Similarly, the work of [33] highlighted the cybercrime and cybersecurity challenges that arised from the work-from-home directives from various governments and other organizations. The authors cited the Global Endpoint Security Trend Report and highlighted that approximately 42 percent endpoints worldwide are not secure owing to working from home scenarios, as employees have minimal cybersecurity resources at their disposal. Table 3 presents the other aspects of research to address COVID-19 using information and communication technologies, in which differences between those studies and our research is also highlighted.

III. COVID-19 CYBER INCIDENTS AND CONSEQUENCES

In this section, we will present the taxonomy of COVID-19 related cyber incidents (see Figure 3), and discuss the associated consequences.

A. CYBER INCIDENTS

Recent statistics have shown that the number of COVID-19-themed cyberattacks has increased in the past weeks and months, as shown in Figure 4. Tables 1 and 4

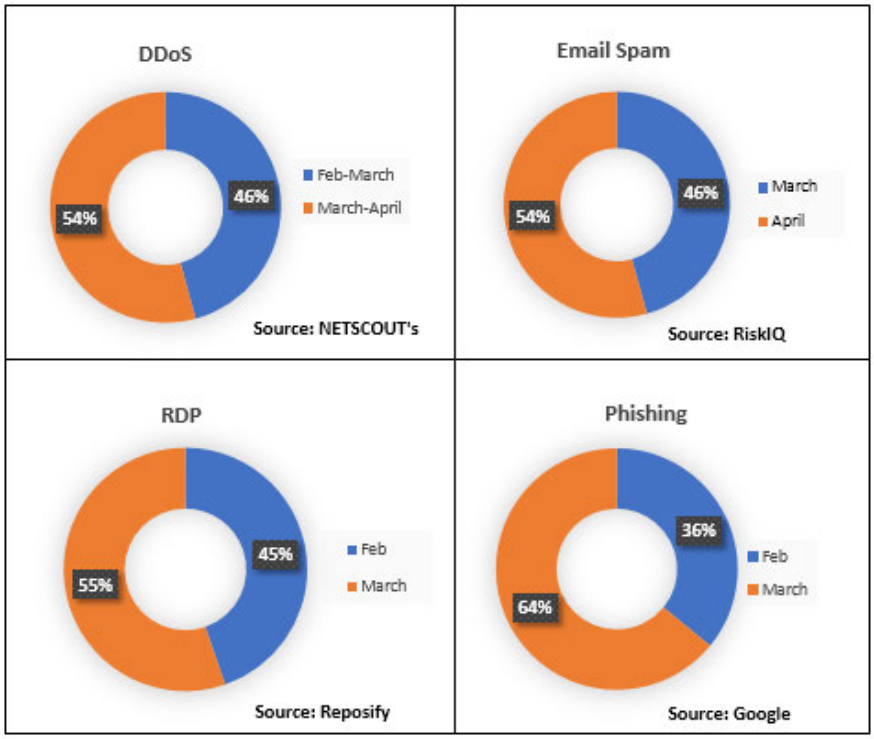


FIGURE 4. Surge of Cyberattacks amid COVID-19.

TABLE 4. Examples of COVID-19-themed Malware.

Malware	Summary	Sources
Maze	Ransomware	www.mcafee.com
Mummy Spider	Utilizes e-mail-thread hijacking techniques to trick victims to download malware samples, such as Emotet.	www.crowdstrike.com
AZORult	Information-stealing malware targeting coronavirus online map trackers.	www.scmagazine.com
Zloader	Users (tricked into) download(ing) Zloader will result in their system being infected with the Zeus malware.	www.zdnet.com
Remote Access Trojan (RAT)	Attempts to take over administrative control of victims' devices to carry out surveillance or other nefarious activities.	www.anomali.com.
AndroidOS-ProjectSpy.HRX and IOS-ProjectSpy.A	Steals messages from popular messaging platforms and information related to WiFi and SIM.	www.trendmicro.com

highlight the popular real-world cybersecurity and malware attacks, respectively, amid the COVID-19 pandemic. These attacks can be broadly categorized on the basis of the intentions of cyber criminals, such as to disrupt essential/entertainment services, obtain illicit financial gain, steal information, and seek to spread fear (see Sections III-A1 to III-A4).

1) DISRUPTING SERVICES

a: DDoS ATTACKS

Europol reported a steady increase in DDoS attacks during the pandemic. These attacks have substantial practical consequences because the number of Internet users also increases owing to social distancing, work-from-home environments, and online educational activities (e.g., video tutorials) [34], among others. An example of such a scenario was reported by the US Health and Human Services Department and occurred in March 2020 [35].

b: SPYWARE ATTACKS

Spyware is a type of malware used to clandestinely obtain covert information of other systems. This threat has been observed in the current COVID-19 pandemic. For example, COVID-19-related tracker-based apps were reportedly embedded in spyware-based programs to track the activity of users. A popular malicious app is Corona Live 1.1.

2) FINANCIAL GAINS

a: RANSOMWARE ATTACK

Malware, such as ransomware, are malicious programs designed to facilitate a broad range of nefarious activities [36], [37]. In particular, malware are designed to prevent access to people's personal data unless a ransom is paid (typically using some cryptocurrency, such as bitcoin). For example, CovidLock, an Android app, was developed to monitor heat map visuals and statistics on COVID-19. Users seeking to install this app have to grant the app certain

permissions on the users' device. As soon as the app is installed, it locks user contacts, pictures, videos, and access to social media accounts. To regain access, users have to pay the ransom using bitcoins. If the ransom is not paid, then users' information may be published and all data erased from the devices' memory [38].

b: DIGITAL FRAUD

Apart from COVID-19-themed malware designed to facilitate illicit financial gains, we also observed an increase in the number of COVID-19-themed gray marketing activities. Examples include attempts to sell personal protective equipment (PPE) or other COVID-19-related products at astronomical prices, or sell counterfeit and unapproved equipment and products. Approximately 2,000 online links were discovered by Interpol and other intelligence agencies between March 3 and 10, 2020 [39]. These links offered to sell COVID-19-related products at considerably high prices. Approximately 13 million Euros worth of pharmaceuticals and 37,000 counterfeit and unauthorized medical devices were reportedly seized during this short period.

3) INFORMATION THEFT AND DATA BREACH

a: VISHING CALLS

Telecomputing (e.g., telehealth) is becoming a norm in the current COVID-19 pandemic, in which organizations offer flexible work arrangements to their employees. Given that these employees rely heavily on phone and Internet communications to carry out their business operations, including healthcare advisories, such a communication channel can also be, and have been, exploited by cyber criminals. For example, cyber criminals have been reported to hijack or impersonate business and personal communications via voice phishing (i.e., vishing), robocall scams, and other technical support scams. Cyber criminals have also been reported to abuse voice over IP (VoIP) services to scam individuals into paying for non-existent services or hand over their personal information (e.g., bank account details, social security numbers) [40].

b: VULNERABILITY EXPLOITATION

The existing social distancing requirements have resulted in the closure of such organizations as universities, government agencies, and other non-essential services. This closure has resulted in the significant use of online systems and platforms, such as online learning management systems (LMS) and video conferencing applications and tools (e.g., Zoom). Several incidents, some of which are highly publicized, have been reported, in which cyber criminals identify and exploit vulnerabilities in the aforementioned systems and platforms. One popular but vulnerable platform was reportedly hacked owing to weak security and password mechanism. Consequently, the attackers were able to hijack video conference sessions or gain access to conferencing contents.

c: PHISHING

Phishing is also a common attack threat observed during the COVID-19 pandemic. RiskIQ [41] reported that over a three-day period (i.e., April 11 to 13, 2020) over 309,000 spam e-mails containing either ''corona'' or ''covid'' were discovered. In these e-mails [42], the attackers impersonated the World Health Organization (WHO) or some medical professionals by using such prefixes as ''Dr'' and ''Professor.'' These e-mails often contain such subject lines as ''COVID-19 updates,'' ''COVID-19 tracker of your city,'' and similar tags designed to lure victims in clicking on the attachment with extensions that include ''.rtf'' [43].

4) FEARWARE

a: DISINFORMATION

Several infodemic campaigns have also been observed on popular social media platforms, such as Facebook, WhatsApp, and LinkedIn, where fake or misleading information were posted. Examples include claims of ayurvedic medicine being effective against COVID-19 or drinking tea or cow urine can prevent COVID-19 transmission [44]. Although no scientific evidence validate these claims, they created confusion among the public and, in some cases, led to fatalities or injuries. Numerous articles and videos have also been shared through social media platforms that teach how to make home-made hand sanitizers and other related products. There have also been claims on popular social media websites that COVID-19 is not real, and citizens should disregard social distancing requirements. Moreover, COVID-19-themed articles advocating violence against certain ethnicity groups have been reportedly circulating online. Such activities can have fatal consequences.

B. EFFECTS ON SECURITY GOALS

All the previously discussed threats serve the same purpose, which is to disrupt security goals and exploit potential vulnerabilities in various sectors, such as health care, entertainment, education, business, banking, and essential government services. The brief descriptions of these security goals and effects are as follows.

1) CONFIDENTIALITY

Confidentiality ensures that information is accessible only to authorized people and is commonly achieved through encryption, in which information is hidden to the outside world but accessible to participating users. For financial benefits, hackers utilize various type of techniques, such as ransomware, to gain unauthorized access to user devices and encrypt and lock personal files on their mobiles and PCs. These incidents result in considerable financial losses to individuals and organizations [45].

2) INTEGRITY

The main goal of integrity is to safeguard data from any intentional or accidental changes by authorized/unauthorized users [45]. This aspect ensures that information is in its original form and maintains the data consistency of internal and external programs. During the COVID-19 pandemic, a few attacks have focused on the integrity of systems, in which

unauthorized health professionals pretend to be authorized professionals and use different approaches (e.g., e-mail spam, phishing calls) to lure users for their malicious financial benefits.

3) AVAILABILITY

Availability ensures that data and resources are readily available to authorized users, particularly during emergencies [45]. The COVID-19 pandemic has witnessed several attacks that target several sectors (e.g., health care, which was the worst hit) using DDoS and malware attack strategies to disrupt the availability of critical services. The ultimate consequence of compromising this security goal results in rescheduling urgent healthcare surgeries and appointments and delay in chemotherapy, among others.

4) AUTHENTICITY

Authenticity [5] is the latest addition to the CIA triad, in which the ultimate goal is to verify that the received message or any data exchange is from that original source only. This objective is often achieved through authentication via static and dynamic authentication methods. Several malware were created during the pandemic to facilitate the stealing of user credentials and information, such as social security numbers [46], [47]. Concerns have also been raised related to privacy and surveillance, such as the use of COVID-19 tracking apps [48].

Figure 3 presents the motivation of attacks, approaches in conducting attacks, and potential mitigation strategies and security goals. The description of mitigation strategies is discussed in the following section.

IV. POTENTIAL MITIGATION SOLUTIONS

This section provides guidelines for individuals working from home to minimize attacks. We also discuss the potential mitigation approaches to counter future pandemic-themed cyberattacks (see also Figure 5 and Tables 5 and 6).

A. TRUSTED INFORMATION SOURCE VALIDATION

One of the potential approaches to mitigate ransomware attacks is to vet third-party apps and educate users, thereby enabling them to identify trusted or reputable sources (e.g., government organizations or reputable research and healthcare institutions). App ratings can also be another indication whether apps are trustworthy. However, this approach will not work for new apps, particularly in pandemic-type situations.

B. DETECTION AND BLOCKAGE OF SCAM CALLS

VoIP service providers can play an effective role in mitigating scam call threats, such as assisting to raise user awareness and actively identify and block potentially fraudulent or scam callers (e.g., based on red flag indicators, such as robot calls). Although not all users are cyber aware, free educational campaigns, such as not sharing personal information through voice calls and disregarding online offers that are too good to be true (e.g., free medical tests and vaccinations), could be intensified during pandemics.

FIGURE 5. Potential solutions to mitigate cyberattacks during pandemics.

The other possible mitigation strategy involves the design and development of anti-spam detectors based on artificial intelligence (AI). Using the data from previous pandemics, an AI-based bot can be developed to answer calls (instead of users) and verify whether an incoming call is a spam or not.

C. INTERNATIONAL COLLABORATION

Evidently, we need collective effort from different countries and governments during pandemics, such as the current COVID-19 emergency. To combat pandemic-themed cyber threats, effort and countermeasures are required from the international community, including the establishment of an international task force to facilitate the sharing of current cyber threat intelligence (e.g., threat vectors and techniques).

The importance of financial support cannot be understated in international collaboration activities (e.g., cyber hygiene education). However, many other competing priorities are present during pandemics. Hence, the support of the community and international organizations should be sought to fund mitigation initiatives. For example, financial support from such organizations as the International Monetary Fund (IMF) can be used to develop tools and skills to mitigate cyber threats.

D. COUNTERING INFODEMIC CAMPAIGNS

To counter infodemic campaigns, we need the support and involvement of a broad range of stakeholders, such as social media platforms. However, determining whether posted contents are fake can be challenging, particularly when relating to ongoing pandemics. Hence, computer and social scientists

TABLE 5. Potential solutions and guidelines.

Solutions	Causes	Guidelines
Trusted Information Source Validation	(a) Downloading new low-rated pandemic-related applications, (b) trusting unauthenticated news sources	(a) Evaluate application ratings and reviews, (b) user education for identifying pandemic-related information from trusted and reputable sources, (c) mitigation of ransomware attacks through sophisticated third-party apps
Detection and Blockage of Scam Calls	(a) No single reliable solution available for the detection and mitigation of scam calls, (b) provide personal details through phone and other VoIP-related services	(a) User awareness for identifying and blockage of fraudulent or scam callers, (b) free educational campaigns for not providing any personal and financial information, such as social security number and bank details, through voice calls, (c) avoid or disregard free offers for pandemic testing and vaccination
International Collaboration	(a) Lack of international collaboration to combat pandemic-themed cyberattacks	(a) Establishment of an international task force to facilitate the sharing of current cyber threat intelligence (e.g., threat vectors and techniques), (b) international cyber hygiene educational and training programs, (c) financial support from such organizations as the International Monetary Fund (IMF) can be used to develop tools and skills to mitigate these cyber threats
Countering Infodemic Campaigns	(a) Fake information spreading through social media for panic and financial gains	Identification and classification of fake or misleading news through human-in-loop machine learning techniques.
Secure and Updated Systems	Increase of system usage at home owing to social distancing	(a) Patching of operating systems and applications, (b) free of charge reliable security products (e.g., anti-malware and anti-viruses) during pandemics

TABLE 6. Security guidelines for users working from home.

Tips	Reasons
Increase your awareness related to cyberattacks	Extensive information is available to equip individuals, whether new or technical computer users, with the necessary and basic cybersecurity knowledge. Such information as creating strong passwords, identifying vulnerable malware links, and using social media wisely, can help users mitigate numerous cyberattacks. A few of the related popular guidelines are available on [1], [2], [3].
Update installed anti-virus and anti-malware products through original vendors	Given that attacks evolve over time, anti-malware products should be updated to quarantine/counter the effects of new attacks. Different strategies to update anti-virus products are provided by [4].
Be cautious to e-mails from unfamiliar sources and the following categories: promotional/special offers, surveys or announcements of any kind, charity-based, bank-related and employers.	These malicious e-mails crafted by scammers encourage users to provide personal information by clicking on links and downloading attachments, and lure users through lucrative offers, such as free entertainment subscriptions, lottery tickets, and cash rewards. The intention is either to damage the system or steal money.
Consistently back-up data	In worst-case scenario of data being compromised, corrupted, or stolen, backing up your data to external devices, such as USBs and hard disks, is recommended.
Do not provide bank/personal details via phone/email for any of the system maintenance services	In the majority of cases, new computer users are tricked by scammers through telephone calls or e-mails. They pretend to update the host system remotely with the intention of hacking it and stealing bank account details.
Be vigilant while clicking online meeting platform links, such as Zoom, Google Meets, and Microsoft Teams	Attackers can impersonate such links as well. A recent example in which a victim pretending it to be from Microsoft teams clicked the following link [5] and ended up downloading malware. There are also fake Google Meets domains, such as "Googelmeetscom." Further guidelines to mitigate this attack is provided by [6].
Use virtual private network (VPN)	VPN provides a private tunnel for users, in which information is encrypted and cannot be accessed by hackers. Hence, organizations can secure the home networks of employees using VPN.
Consistently shutdown laptop or home computer	Some software updates, such as firewall settings and Windows-patch updates, require system restart to be effective. Moreover, system shutdown flashes temporary and unimportant data and stops memory leaks.
Change passwords frequently	A good practice for employees is to frequently change their passwords while accessing online services from their homes. This practice can substantially reduce the impact of passive attacks.
Avoid public WiFi spots	Never use public WiFi spots to access information of your organization or any banking related transactions owing to unencrypted network traffic and legitimacy of these spots.
Strictly follow bring-your-own-device (BYOD) policy	Organizations that allow employers to use their own devices for work provide BYOD policies. These policies include certain security guidelines that aid employees secure their respective devices. Further general guidelines on protecting information while working from home can be found at [7].

[1] https://www.comtact.co.uk/blog/6-steps-of-a-successful-cyber-security-user-awareness-programme
[2] https://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf
[3] https://www.enisa.europa.eu/publications/archive/copy_new-users-guide/at_download/fullReport
[4] https://www.us-cert.gov/sites/default/files/recommended_practices/Recommended Practice Updating Antivirus in an Industrial Control System_S508C.pdf
[5] http://loginṁicrosoftonline.com-common-oauth2-eezylnrbṁedyacaṁcom/common/oauth2/
[6] https://www.us-cert.gov/ncas/current-activity/2020/04/02/fbi-releases-guidance-defending-against-vtc-hijacking-and-zoom
[7] https://www.oipc.bc.ca/guidance-documents/1447

and healthcare professionals have roles in collaborating and designing approaches (e.g., based on human-in-the-loop machine learning techniques) to considerably identify and classify fake or misleading news.

E. SECURE AND UPDATED SYSTEMS

Given the increased use of systems at homes due to social distancing measures, effort should be exerted to ensure that home systems are patched and secure. For example, patching operating systems and applications is one of the key cyber mitigation strategies recommended by the Australian Signals Directorate's Australian Cyber Security Centre [49].

Security organizations can also play a role, such as by not charging subscriptions for their security products (e.g., anti-malware software) during pandemics.

F. RAPID RISK MANAGEMENT FRAMEWORKS

Risk management framework is an effective method to access, mitigate, and evaluate risks associated with the threat. Several risk management frameworks are available such as for scada systems [50], online services [51], and cyber physical systems [52]–[54]. Accordingly, a pandemic such as COVID-19 warrants new and rapid framework that can be implemented immediately. Such a framework should be robust, scalable, time-efficient, and accurate which can be easily followed by technical/non-technical computer experts within dynamic environments whether home- or office-based environment.

V. DISCUSSION

The most pronounced impact of COVID-19 is the shift of the cyber security landscape from an enterprise to a home environment. The fortuitous shift has provided many new opportunities to hackers and cybercriminals, thereby resulting in an increased risk of vulnerability exploitation. During the COVID-19 pandemic, a new wave of cyberattacks was recorded. Working from home has increased the risk of cyberattacks owing to various reasons, which is highlighted in Figure 3. In the enterprise or corporate environment, the security of all assets (hardware and software) are properly managed by the IT support staff and access to systems, and the internet is governed under strict cybersecurity policies and SOPs. IT-related assets are patched and updated regularly. However, working from home using employees own devices with their unsafe networks increase the opportunities of cyber threats. Accordingly, working with these unprotected and unsecured communication channels from home provides an entry point to hackers and cybercriminals.

User awareness is critical to mitigate and reduce the risk of such cyberattacks in the future. We summarized the key user awareness guidelines in Tables 5 and 6 that are suitable for home-based environment and vice versa. The most important security guidelines are as follows. First, organizations that allow employees to use their own devices to work from home provide BYOD policies, which contain security guidelines that aid employees to secure their respective devices. Second, VPNs should be used while working from home to communicate between employee personal devices and enterprise systems. Lastly, the cybersecurity awareness of employees should be enhanced regularly through cybersecurity education and training programs. Gamification [55] may be explored to further motivate people to gain cybersecurity awareness. The need to include basic cybersecurity curriculum in medical education and for a dynamic cybersecurity risk management framework should be highlighted to cope with pandemics.

Emerging technologies (e.g., AI, machine learning, IoT, IIoT, Industry 4.0, blockchain, Fog, edge computing [56], and mobile and wireless technologies) have extremely important roles in addressing pandemics, such as COVID-19, specifically relate to tracking/monitoring COVID-19 patients, infected areas, pandemic spreading prediction, expediting the development process of new vaccines for COVID-19, and diagnosing COVID-19.

VI. CONCLUDING REMARKS

This study explored COVID-19 themed cyberattacks and categorized them into four categories: disrupting services, financial gains, information theft, and fearware, and further categorized into sub-categories (e.g., malware, ransomware, phishing). We used these categories to present potential mitigation solutions. The cyberattack taxonomy and potential mitigation strategies can also facilitate cyberattack prevention effort plannings in future pandemics. In the future, we intend to extend the proposed taxonomy and propose risk management model for these pandemics.

ACKNOWLEDGMENT

The authors thank the DSR and RSSU at King Saud University for their technical support.

REFERENCES

[1] C. Sohrabi, Z. Alsafi, N. O'Neill, M. Khan, A. Kerwan, A. Al-Jabir, C. Iosifidis, and R. Agha, "World health organization declares global emergency: A review of the 2019 novel coronavirus (COVID-19)," *Int. J. Surgery*, vol. 76, pp. 71–76, Apr. 2020.

[2] Z. Allam and D. S. Jones, "On the coronavirus (COVID-19) outbreak and the smart city network: Universal data sharing standards coupled with artificial intelligence (ai) to benefit urban health monitoring and management," in *Healthcare*, vol. 8, no. 1. Basel, Switzerland: Multidisciplinary Digital Publishing Institute, 2020, p. 46.

[3] R. Nunes-Vaz, "Visualising the doubling time of COVID-19 allows comparison of the success of containment measures," *Global Biosecur.*, vol. 1, no. 3, 2020, pp. 1–4.

[4] ZDNet. (2020). *Czech hospital Hit by Cyberattack While in the Midst of a COVID-19 Outbreak*. [Online]. Available: https://www.zdnet.com/article/czech-hospital-hit-by-cy-ber-attack-while-in-the-midst-of-a-covid-19-outbreak/

[5] W. Stallings and L. Brown, "Computer security concepts," *Comput. Secur., Princ. Pract.*, vol. 4, p. 13, Aug. 2016.

[6] M. P. Barrett, "Framework for improving critical infrastructure cybersecurity version 1.1: Nist cybersecurity framework," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST IR 8204, 2018.

[7] *Risk management—Guidelines*, Standard ISO 31000:2018, I. O. for Standardization Technical Committee, International Organization for Standardization, Washington, DC, USA, 2018. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso

[8] M. Numan, F. Subhan, W. Z. Khan, S. Hakak, S. Haider, G. T. Reddy, A. Jolfaei, and M. Alazab, "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65450–65461, 2020.

[9] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Gener. Comput. Syst.*, vol. 100, pp. 144–164, Nov. 2019.

[10] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, N. M. Akim, and M. Imran, "Deep learning and big data technologies for IoT security," *Comput. Commun.*, vol. 151, pp. 495–517, Feb. 2020.

[11] I. Yaqoob, E. Ahmed, M. H. U. Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the Internet of Things," *Comput. Netw.*, vol. 129, pp. 444–458, Dec. 2017.

[12] T. Khalid, A. N. Khan, M. Ali, A. Adeel, A. ur Rehman Khan, and J. Shuja, "A fog-based security framework for intelligent traffic light control system," *Multimedia Tools Appl.*, vol. 78, no. 17, pp. 24595–24615, Sep. 2019.

[13] M. F. Aziz, A. N. Khan, J. Shuja, I. A. Khan, F. G. Khan, and A. U. R. Khan, "A lightweight and compromise-resilient authentication scheme for IoTs," *Trans. Emerg. Telecommun. Technol.*, vol. 31, Nov. 2019, Art. no. e3813.

[14] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT services through software defined networking and edge computing: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, early access, May 26, 2020, doi: 10.1109/COMST.2020.2997475.

[15] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," *IEEE Netw.*, vol. 34, no. 1, pp. 8–14, Jan. 2020.

[16] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernández-Campusano, "A context-aware privacy-preserving method for IoT-based smart city using software defined networking," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101470.

[17] W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial Internet of Things: Recent advances, enabling technologies and open challenges," *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106522.

[18] W. Z. Khan, M. Y. Aalsalem, and M. K. Khan, "Communal acts of IoT consumers: A potential threat to security and privacy," *IEEE Trans. Consum. Electron.*, vol. 65, no. 1, pp. 64–72, Feb. 2019.

[19] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "Data and privacy: Getting consumers to trust products enabled by the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 35–38, Mar. 2019.

[20] H. Cho, D. Ippolito, and Y. W. Yu, "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs," 2020, *arXiv:2003.11511*. [Online]. Available: http://arxiv.org/abs/2003.11511

[21] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.

[22] A. De Carli, M. Franco, A. Gassmann, C. Killer, B. Rodrigues, E. Scheid, D. Schoenbaechler, and B. Stiller, "WeTrace—A privacy-preserving mobile COVID-19 tracing approach and application," 2020, *arXiv:2004.08812*. [Online]. Available: http://arxiv.org/abs/2004.08812

[23] P. Gupta, S. Mehrotra, N. Panwar, S. Sharma, N. Venkatasubramanian, and G. Wang, "Quest: Practical and oblivious mitigation strategies for COVID-19 using WiFi datasets," 2020, *arXiv:2005.02510*. [Online]. Available: http://arxiv.org/abs/2005.02510

[24] Z. Yang, Z. Zeng, K. Wang, S.-S. Wong, W. Liang, M. Zanin, P. Liu, X. Cao, Z. Gao, Z. Mai, and J. Liang, "Modified seir and ai prediction of the epidemics trend of COVID-19 in China under public health interventions," *J. Thoracic Disease*, vol. 12, no. 3, p. 165, 2020.

[25] B. Pirouz, S. S. Haghshenas, S. S. Haghshenas, and P. Piro, "Investigating a serious challenge in the sustainable development process: Analysis of confirmed cases of COVID-19 (new type of coronavirus) through a binary classification using artificial intelligence and regression analysis," *Sustainability*, vol. 12, no. 6, p. 2427, Mar. 2020.

[26] A. Kumar, P. K. Gupta, and A. Srivastava, "A review of modern technologies for tackling COVID-19 pandemic," *Diabetes Metabolic Syndrome, Clin. Res. Rev.*, vol. 14, no. 4, pp. 569–573, Jul. 2020.

[27] L. Wynants, B. Van Calster, M. M. Bonten, G. S. Collins, T. P. Debray, M. De Vos, M. C. Haller, G. Heinze, K. G. Moons, R. D. Riley, and E. Schuit, "Prediction models for diagnosis and prognosis of COVID-19 infection: Systematic review and critical appraisal," *Brit. Med. J.*, vol. 369, Apr. 2020, Art. no. m1328.

[28] X. Meng, Z. Dai, C. Hang, and Y. Wang, "Smartphone-enabled wireless otoscope-assisted online telemedicine during the COVID-19 outbreak," *Amer. J. Otolaryngol.*, vol. 41, no. 3, May 2020, Art. no. 102476.

[29] M. Javaid, A. Haleem, R. Vaishya, S. Bahl, R. Suman, and A. Vaish, "Industry 4.0 technologies and their applications in fighting COVID-19 pandemic," *Diabetes Metabolic Syndrome, Clin. Res. Rev.*, vol. 14, no. 4, pp. 419–422, Jul. 2020.

[30] C. J. Wang, C. Y. Ng, and R. H. Brook, "Response to COVID-19 in Taiwan: Big data analytics, new technology, and proactive testing," *J. Amer. Med. Assoc.*, vol. 323, no. 14, pp. 1341–1342, 2020.

[31] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact," *IEEE Access*, vol. 8, pp. 90225–90265, 2020.

[32] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten deadly cyber security threats amid COVID-19 pandemic," Taylor's Univ., Selangor, Malaysia, Tech. Rep. techrxiv.12278792.v1, 2020.

[33] T. Ahmad, "Corona virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity," School Law, GD Goenka Univ., Gurugram, India, Tech. Rep. ssrn.3568830, 2020.

[34] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2019, pp. 1–8.

[35] S. Stein and J. Jacobs. (2020). *Cyber-Attack Hits U.S. Health Agency Amid COVID-19 Outbreak*. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

[36] K.-K.-R. Choo, "The cyber threat landscape: Challenges and future research directions," *Comput. Secur.*, vol. 30, no. 8, pp. 719–731, Nov. 2011.

[37] K. Thakur and A.-S. K. Pathan, *Cybersecurity Fundamentals: A Real-World Perspective*. Boca Raton, FL, USA: CRC Press, 2020.

[38] L. Whitney. *CovidLock Ransomware Exploits Coronavirus With Malicious Android App*. Accessed: Apr. 29, 2020. [Online]. Available: https://www.techrepublic.com/article/covidlock-ransomware-exploits-coronavirus-with-malicious-android-app/

[39] Europol. *Staying Safe During COVID-19: What You Need to Know*. Accessed: Apr. 29, 2020. [Online]. Available: https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know

[40] K. Hobbs. *Socially Distancing From COVID-19 Robocall Scams*. Accessed: Apr. 29, 2020. [Online]. Available: https://www.consumer.ftc.gov/blog/2020/03/socially-distancing-covid-19-robocall-scams

[41] T. RiskIQ. *COVID-19 Cybercrime Daily Update*. Accessed: Apr. 29, 2020. [Online]. Available: https://www.riskiq.com

[42] W. Z. Khan, M. K. Khan, F. T. Bin Muhaya, M. Y. Aalsalem, and H.-C. Chao, "A comprehensive study of email spam botnet detection," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2271–2295, 4th Quart., 2015.

[43] CISA-Alert(AA20-099A). *COVID-19 Exploited by Malicious Cyber Actors*. Accessed: Apr. 29, 2020. [Online]. Available: https://www.us-cert.gov/ncas/alerts/aa20-099a

[44] S. Menon. (2020). *Coronavirus: Herbal Remedies in India and Other Claims Fact-Checked*. [Online]. Available: https://www.bbc.com/news/world-asia-india-51910099

[45] S. Hakak, A. Kamsin, O. Tayan, M. Y. I. Idris, and G. A. Gilkar, "Approaches for preserving content integrity of sensitive online arabic content: A survey and research challenges," *Inf. Process. Manage.*, vol. 56, no. 2, pp. 367–380, Mar. 2019.

[46] R. Naidoo, "A multi-level influence model of COVID-19 themed cybercrime," *Eur. J. Inf. Syst.*, vol. 29, pp. 1–16, May 2020.

[47] W. Yaokumah, F. Katsriku, J.-D. Abdulai, and K. O. Asante-Offei, "Taxonomy of cyber threats to application security and applicable defenses," in *Modern Theories and Practices for Cyber Ethics and Security Compliance*. Pittsburgh, PA, USA: IGI Global, 2020, pp. 18–43.

[48] T. Sharma and M. Bashir, "Use of apps in the COVID-19 response and the loss of privacy protection," *Nature Med.*, vol. 26, pp. 1–2, May 2020.

[49] AC SecurityCentre. (2017). *Strategies to Mitigate Cyber Security Incidents*. [Online]. Available: https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents

[50] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2016.

[51] J. Meszaros and A. Buchalcevova, "Introducing OSSF: A framework for online service cybersecurity risk management," *Comput. Secur.*, vol. 65, pp. 300–313, Mar. 2017.

[52] H. Kure, S. Islam, and M. Razzaque, "An integrated cyber security risk management approach for a cyber-physical system," *Appl. Sci.*, vol. 8, no. 6, p. 898, May 2018.

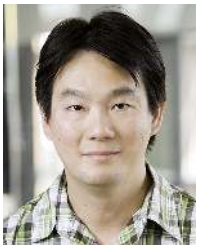
[53] H. Mokalled, C. Pragliola, D. Debertol, E. Meda, and R. Zunino, "A comprehensive framework for the security risk management of cyber-physical systems," in *Resilience of Cyber-Physical Systems From Risk Modelling to Threat Counteraction*. Cham, Switzerland: Springer, 2019, pp. 49–68.

[54] G. Falco, A. Noriega, and L. Susskind, "Cyber negotiation: A cyber risk management approach to defend urban critical infrastructure from cyberattacks," *J. Cyber Policy*, vol. 4, no. 1, pp. 90–116, Jan. 2019.
[55] S. Hakak, N. F. M. Noor, M. N. Ayub, H. Affal, N. Hussin, E. Ahmed, and M. Imran, "Cloud-assisted gamification for education and learning—Recent advances and challenges," *Comput. Electr. Eng.*, vol. 74, pp. 22–34, Mar. 2019.
[56] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Gener. Comput. Syst.*, vol. 97, pp. 219–235, Aug. 2019.

SAQIB HAKAK (Member, IEEE) received the bachelor's degree in computer science engineering from the University of Kashmir, India, in 2010, the master's degree in computer and information engineering from IIUM, Malaysia, and the Ph.D. degree from the Faculty of computer Science and Information Technology, University of Malaya, Malaysia. He is currently working as an Assistant Professor with the University of Northern British Columbia, Canada. Prior to this designation, he worked as a Postdoctoral Research Fellow at the prestigious Canadian Institute for Cyber-Security. His research areas include information natural language processing, cyber security, artificial intelligence, and wireless networks.

WAZIR ZADA KHAN (Senior Member, IEEE) received the bachelor's and master's degrees in computer science from COMSATS University Islamabad–Wah, in 2004 and 2007, respectively, and the Ph.D. degree from the Electrical and Electronic Engineering Department, Universiti Teknologi PETRONAS, Malaysia, in 2015. He is currently working with the Farasan Networking Research Laboratory, Faculty of CS & IT, Jazan University, Saudi Arabia. He is also serving as a Researcher at the Global Foundation for Cyber Studies and Research, which is an independent, non-profit, and non-partisan cybersecurity think-tank based in Washington D.C. He has published over 75 research articles in the journals and conferences of international repute. He is the serving as a reviewer for many reputed journals and also a member of the technical program committee for many international conferences. He has more than ten years of teaching/professional experience in Pakistan and Saudi Arabia. His current research interests include wireless sensor networks, security and privacy, blockchain, the IoT, IIoT, and reinforcement learning.

MUHAMMAD IMRAN (Member, IEEE) received the Ph.D. degree in information technology from University Teknologi PETRONAS, Malaysia, in 2011. He is currently an Associate Professor with the College of Applied Computer Science, King Saud University, Saudi Arabia. His research interests include the Internet of Things, mobile and wireless networks, big data analytics, cloud computing, and information security. His research is financially supported by several grants. He has completed a number of international collaborative research projects with reputable universities. He has published more than 200 research articles in peer-reviewed, well-recognized international conferences and journals. Many of his research articles are among the highly cited and most downloaded. He has been involved approximately in 100 peer-reviewed international conferences and workshops in various capacities, such as the Chair, the Co-Chair, and the Technical Program Committee member. He has served as an Editor in Chief for European Alliance for Innovation (EAI) *Transactions on Pervasive Health and Technology*. He has served/serving as a Guest Editor for about two dozen special issues in journals, such as the IEEE Communications Magazine, the IEEE Wireless Communications Magazine, *Future Generation Computer Systems*, IEEE Access, and *Computer Networks*. He has been consecutively awarded with Outstanding Associate Editor of IEEE Access in 2018 and 2019 besides many others. He is serving as an Associate Editor for top ranked international journals, such as the IEEE Communications Magazine, the IEEE Network, *Future Generation Computer Systems*, and IEEE Access.



KIM-KWANG RAYMOND CHOO (Senior Member, IEEE) holds the Cloud Technology Endowed Professorship with the Department of Information Systems and Cyber Security, The University of Texas at San Antonio. He is also a Fellow of the Australian Computer Society. He was a recipient of various awards, including the 2019 IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the Outstanding Associate Editor of 2018 for IEEE Access, the British Computer Society's 2019 Wilkes Award Runner-up, the 2019 *EURASIP Journal on Wireless Communications and Networking* (JWCN) Best Paper Award, the Korea Information Processing Society's Journal of Information Processing Systems (JIPS) Survey Paper Award (Gold) 2019, the IEEE Blockchain 2019 Outstanding Paper Award, the International Conference on Information Security and Cryptology (Inscrypt 2019) Best Student Paper Award, the IEEE TrustCom 2018 Best Paper Award, the ESORICS 2015 Best Research Paper Award, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award, in 2008.

MUHAMMAD SHOAIB received the B.Eng. and M.Eng. degrees from the NED University of Engineering and Technology, Karachi, in 1995 and 2005, respectively, and the Ph.D. degree in communication and information system from the Beijing University of Posts and Telecommunications, China, in 2010. He worked as a Senior Manager (IP Operations, South) in Pakistan Telecommunication Company Limited, Pakistan. He also worked as a Maintenance Engineer with R. M. International. He is currently working as an Assistant Professor with the Information Systems Department, College of Computer and Information Sciences, King Saud University. His areas of research include video compression techniques, multilayer video coding, commercial data center facilities and IP packet based networks, and infrastructure and security.