Effects of COVID-19 pandemic on computational intelligence and cybersecurity: a survey

Mohamed Wiem Mkaouer, Tarek Gaber, Zaineb Chelly Dagdia

Applied Computing and Intelligence

https://www.aimspress.com/journal/aci

Applied Computing and Intelligence, 5(x): xxx–xxx
DOI:
Received: ** 2022
Revised: ** 2022
Accepted: ** 2022
Published: ** 2022

Survey

Effects of COVID-19 pandemic on computational intelligence and cybersecurity: a survey

Mohamed Wiem Mkaouer[1] *, **Tarek Gaber**[2], **and Zaineb Chelly Dagdia**[3,4]

[1] Rochester Institute of Technology, New York, United States
[2] School of Computing, Science and Engineering, University of Salford, United Kingdom
[3] Université Paris-Saclay, UVSQ, DAVID, France
[4] LARODEC, ISG, Université de Tunis, Tunis, Tunisia

* **Correspondence:** mwmvse@rit.edu

Abstract: In late December 2019, the World Health Organization (WHO) announced the outbreak of a new type of coronavirus, named the Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2), also known as COVID-19. The fatality of the virus has forced governments and countries to socially isolate their populations, causing a worldwide impact on the economy. Pandemic management has stressed health systems to work beyond their limits, adding more to the tragedy of losing millions of lives. As a natural response to such disasters, intelligent systems have been developed for various reasons related to virus detection, tracking, and control. The social lockdown created a record level of online platforms and applications being used to resume professional and educational activities in a virtual environment. This has triggered an unprecedented growth in cybercrime. This paper presents the effects of the pandemic on computational intelligence and cybersecurity.

Keywords: Coronavirus, COVID-19, computational intelligence, cybersecurity

1. Introduction

The coronavirus pandemic has been a once-in-a-lifetime phenomenon that has significantly burdened societies worldwide. The high transmissibility, life threatening, and novelty of the virus have led to a worldwide collective effort to combat the disease. Computational intelligence has been mobilised, along with health sciences, to combat the massive spread of COVID-19.

The integration of common intelligent computational models, including artificial neural networks, evolutionary computation, fuzzy systems, has been critical for the design and deployment of digital technologies that were devoted to fight the pandemic. Depending on the underlying technology, such as mobile computing, internet-of-things, big data, robotics, various dimensions of intelligent computing

systems have been heavily relied on. These technologies, once augmented with the suitable intelligent techniques, have greatly lessened the damage that could have been enacted if the virus had occurred in a less technologically advanced era. The use of these technologies has aided in a range of areas such as predicting the spread of disease, controlling the spread of the disease, diagnosing patients, and developing treatments.

However, the need for an urgent response has pushed the integration and deployment of these intelligent algorithms into operational systems quickly, and into a broad range of users, without adequately performing the traditional testing procedures. Therefore, these operating systems, once augmented with intellignet algorithms (i.e., AI-enabled systems), have created various challenges for their maintainers, in terms of handling various issues related to usability, accessibility, stability, compatibility, and especially privacy. Also, the shift to the working remotely has emerged several online platforms that were vastly adopted to mimic the in-person setting everywhere. These platforms, besides being drastically operating on a larger scale than anticipated, were also being used by all types of individuals regardless of gender, age, culture, language. For instance, contact-tracing apps were designed, augmented with intelligent algorithms, developed, and shipped to production in a short cycle in comparison with traditional apps. This urgency requirement has prevented various types of important tests, such as security and privacy, to be properly performed, leading them to be more prone to vulnerabilities, and exposing their users to various risks, especially as they are being used online.

The purpose of this paper is two-fold: 1) we aim to analyze the impact of emerging technology on cybersecurity; and 2) we review the response of intelligent computing systems in the fight against the virus. We first analyze how the fast release of these applications had revealed various gaps and vulnerabilities that caused an increase in cybercrime. We foresee the absence of proper frameworks that ensure the existence of proper regulations built-in the shipped solutions. Our analysis shall provide developers and practitioners with actionable insights that need to be taken into account when developing such emerging AI-enabled systems in the future. Second, we dive into the various intelligent algorithms that were adopted in practice by these systems, as part of ensuring several tasks varying from accurately detecting the virus, into monitoring patients, and predicting the geographical and temporal propagation of the pandemic.

This paper structure is as follows: Section 2 covers the impact of the pandemic on the security and privacy of users. Section 3 focuses on public health policy and Section 4 presents the medical healthcare asepct; both from a computational intelligence's applications presepective to fight the pandemic. The conlusion is given in Section 5.

2. Impact on cybersecurity

To respond to the impact of the pandemic, governments, healthcare providers, schools, universities and companies have used different information technology tools to mitigate the implications of lockdown constraints. Before the pandemic, mobile apps related to health (m-health apps) were usually effective tools for users to have control over their health, including calories consumption, vital signs, and activity. Such apps are found to be helpful in fighting COVID-19 [1]. Namely, contact-tracing apps, widely used in the last two years, were useful tools in containing COVID-19. The main idea of these apps is about collecting and processing personal information like user' current location, system settings, cell phone signals, voice and texts. With such information, users can get real-time

medical advice such as alerts about COVID-19 infection hot-spots to avoid them. Many governments have adopted m-health apps applying the same idea to combat the deadly COVID-19 outbreak. Those include China, Korea, UK, and USA [2]. Although, such apps were found useful in containing the pandemic, there were a big concern about the users' privacy. More than half of US adult respondents surveyed by Pew Research Center stated that they will not install COVID-19 related health apps while 30% revealed that they will remove a mobile app which would exploit their personal data [3].

On the other hand, many online video-conferencing apps, such as Zoom, Google Meet, and Microsoft Teams, have emerged and used by people to overcome the limitations of lockdowns. Although this technology helped keeping the family, friends, and employees connected and work, they increased privacy risks. Zoom, for example, has seen a tremendous reaction as security specialists, privacy groups, and lawmakers warn that Zoom's default configurations are not safe [4]. A recent consumer survey showed that apps like Google Meet, Microsoft Team, and Zoom capture more data than users realise [5]. Such data can be analysed by AI-based applications to reveal personal information (i.e., violating users' privacy).

Due to the weak security [6] of the apps above, among many others, and the increase in the use of digital communication tools through running the businesses online (or work-from-home patterns), COVID-19 pandemic has led to an increase in the risk of cyberattacks. Responding to the lockdown, most of critical national business, such as healthcare and governmental services, had to carry on working but online. Such services would have not been equipped with right cybersecurity defence making them a good target to cyberattacks [7].

Responding to this threat, two big cybersecurity centres – *National Cyber Security Centre (NCSC)* of the United Kingdom and the *Cybersecurity and Infrastructure Security Agency (CISA)* of the United States – have met on April 8, 2020 and published a joint advisory committee. Among the aims of this committee are to describe how cyber-criminals and Advanced Persistent Threat (APT) groups were exploiting the current COVID-19 pandemic, and to provide how to avoid computer security threats [8]. Various vulnerabilities were mentioned in this alert, including phishing, malware, and the infiltration of communication platforms such as Zoom and Microsoft Teams. An encompassing appraisal of the full spectrum of attacks associated with the pandemic, on the other hand, is likely lacking in this report. Like other businesses at that time, the current state-of-the-art was extremely fragmented, with attacks reported by governments, the media, security organisations, and incident response teams all contributing to the overall picture. Therefore, organisations face a significant challenge in developing adequate protection and reaction measures in light of the changing environment in which they must operate.

From commerce and social connection to business and industry, the widespread adoption of digital technologies has shifted many aspects of society online, including crime. As of 2020, global cybercrime expenses are expected to rise 15% yearly over the next five years, to 10.5 trillion USD by 2025, from 3 trillion USD in 2015 [9]. As a result, the danger to innovation and investment is tenfold greater than the damage caused by natural disasters per year. Cybercrimes are estimated to be more profitable than all major illegal drugs combined making them more attractive for attackers. The cost estimated above include data damage and destruction, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to business, forensic investigation, restoration and deletion of the hacked data, and reputational harm [9].

2.1. Cybercrime and COVID-19

To emphasize the relation between cybercrime and COVID-19, it is important to define how a cybercrime can take place. For a cybercrime to occur, there must be three factors (fraud triangle): victim, motive, and opportunity [10]. A victim is the target of the crime/attack, the criminal's motive is the reasons of mounting an attack such as financial or political gain, and an opportunity to perform the crime is the chance for it to happen (e.g., it can be an essential vulnerability in the system or an unprotected device). Opportunistic untargeted attacks are fairly common, as well as sophisticated targeted attacks. Opportunistic attacks target victims depending on their vulnerability to attack. Adversaries pick-up victims with known weaknesses or use social engineering to create weaknesses. Any device meant to fool a victim into becoming an attack prey is considered a hook [11]. Such a hook could exploit human distraction, time restrictions, and terror to make the attacks work [12]. People are more easily mislead if they are distracted or worried. Temporal restrictions also increase victims' vulnerability to mistakes and scams. There are other occurrences that have a profound and devastating influence on the entire society, such as fatalities and disasters.

Opportunistic attackers will wait for the perfect conditions to begin an attack. Such conditions include natural disasters, continuing crises, and major public events. Tysiac, in [13], has given some examples on how cybercriminals take on victims of natural disasters. Also, from history, below are a few examples of opportunistic attacks mounted after natural disasters and public events. Natural disasters: New Orleans (USA) and its neighbourhoods were devastated by Hurricane Katrina in 2005. Shortly thereafter, residents began receiving scam emails asking for personal information in order to facilitate possible government assistance efforts, and thousands of fake websites were published claiming collecting humanitarian donations. Similar scams and attacks have been mounted in 2020 during Australia bushfires [14]. Public events: In 2018, during the FIFA World Cup, there were numerous attempts, using spam and phishing emails, to lure people to go by offering them free tickets and gifts [15]. Later, these were found to be phishing emails resulting fraud.

Given the wide range of cyberattacks mounted during natural disasters and public events as shown above, it should come as no surprise to experience similar cyberattacks during the COVID-19 epidemic. Even the scale and volume of the attacks could worse as COVID-19 affected all countries. It was evidenced that the outbreak has created widespread disruption around the world forcing people to adjust their day-to-day activities such as stopping social connection and sport exercises, and most importantly working from home depending on the Internet technologies [16]. Giving all these conditions which have taken place all in once, many people have been overwhelmed and got stressed and worried. Such emotional conditions would increase the vulnerability chance of individuals to be victims for attacks. Additionally, to keep running their business during the lockdown, companies were forced to create new, but maybe not well-studied, working mechanisms such as working from home. Such sudden decisions and changes could lead to changing the protection status of some company assets from high to low or weaken access control to those assets [17]. Exploiting such weakness by cybercriminals across the world have created what is known as *COVID-19 cybersecurity pandemic*.

2.2. Cybersecurity pandemic

Given the massive increase of cybersecurity attacks during the pandemic, as will be highlighted below, the period from late 2019 and 2020, could be known as *cybersecurity pandemic*. Since the out-

break of the pandemic began, numerous sources have reported a significant increase in the number of scams and cyberattacks. Cybercriminals have employed different strategies to mount attacks. For example, they exploited high-demand goods related to COVID-19 (e.g., PPE and testing kits and drugs), which have a high profitable rate or can lead to impersonation attack (i.e., one claims to a public official from WHO [18]).

As reported in [14], on 31 December 2019 and 14 April 2020, the World Economic Forum (WEF) claimed that the pandemic resulted in a 50.1% increase in cyberattacks and an accompanying 30,000 cyberattacks that were explicitly COVID-19-related. Also, according to CGI company [18], because of COVID-19, there has been a 30% rise in cyberattacks. Between January and April 2020, the Interpol discovered a massive increase of different attacks and threats including 907,000 messages of spam, 737 incidents of malware, and 48,000 malicious URLs, all associated to COVID-19. It was also found that there was 60% rise of ransomware payout during the second quarter of 2020 comparing to that of the first quarter [19].

Another attack, ransomware was in particularly soared in April 2020 where most countries were in lockdown. Notably, this attack was mounted by a variety of previously inactive threat organisations. The average ransomware pay-out reached 178,254 USD in the second quarter of 2020 which is up 60% from the first quarter [20]. Such rise in ransomware payments may imply that cybercriminals anticipate a greater possibility of payment as a result of the pandemic's exceptional circumstances. In line with these facts, Google reported that they blocked 18 million malware and phishing emails everyday during April 2020 [21].

2.3. Most common attacks

To assess the impact of the COVID-19 on cybercrimes and cyberattacks across the world, the Interpol analysed data collected during a four-months period (January to April 2020) [19]. The analysis of these data showed that there is a massive increase of three main attacks - all related to COVID-19: 737 incidents of malware, 48,000 malicious URLs, and 907,000 spam messages. Figure 1 shows a summary of the most important results from the Interpol study which was conducted from January to April 2020 to gain insight of the COVID-19 related cybercrime posture of the Interpol members. Aligned with the results of the above studies, it was found that phishing and spam emails were the most common cyberthreats. Below, we highlight the main attacks, and how they could be mounted by the hackers using COVID-19 related information [19].

2.3.1. Online scams and phishing

The traditional internet frauds and phishing techniques have been reworked by hackers. Cybercriminals exploit COVID-19 information communicated through emails to trick their victims into disclosing personal or financial information, or into opening a malicious link or file, which gives them access to their target's machine. For example, attackers could use any or all the following information to compose a phishing email related to the vaccine of the COVID-19: registration of vaccines, a summary of your vaccination history, locations where the vaccination can be administered, a vaccination can be reserved in several ways, and/or requirements for vaccinations. Using such details, on Google platform only, cybercriminals managed to send around 18 million malware and phishing emails associated with COVID-19 during April 2020 [18].

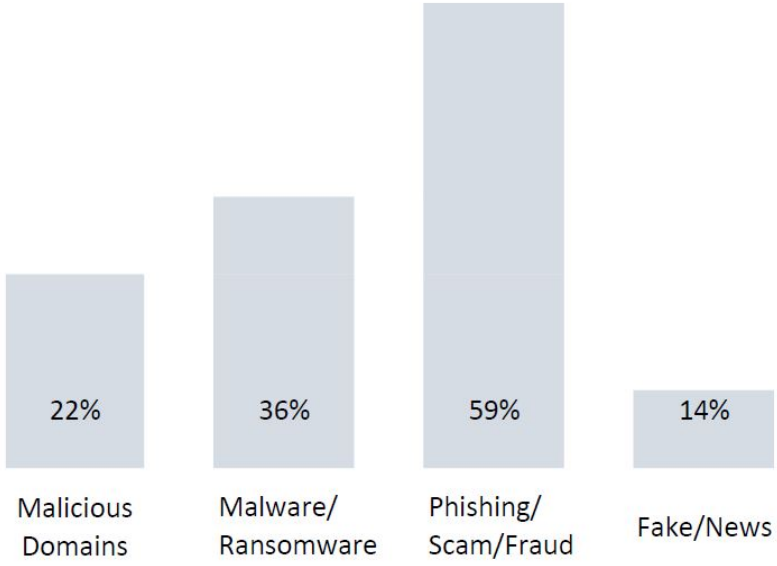

Figure 1. Most common attacks from January to April 2020 of Interpol countries [18]

2.3.2. Disruptive malware

This includes attacks such as ransomware and DDoS. These types of attacks are increasingly being used by cybercriminals targeting critical infrastructure. During COVID-19, healthcare facilities were a main target due to their importance at that time and for the high potential for high impact and capital profit. Several threat groups that have been relatively quiet for the previous few months stepped up their ransomware activities in the first two weeks of April 2020. As reported in [19], the majority of ransomware attackers are now able to workout how much of ransom they could ask for from their victims.

2.3.3. Data harvesting malware

Data stealing malware is a web-based threat that deprives victims of their personal and proprietary information with the purpose of profiting the hacked data through direct usage or underground distribution. Cybercriminals are increasingly deploying data harvesting software, such as banking trojans information stealers, spyware, and remote access trojans, to collect information about their victims. The cybercriminals attack systems using materials related to the COVID-19 context for different purposes including divert money, construct botnets, compromise networks, steal data, among many others [19].

2.3.4. Malicious domains

Cybercriminals are taking advantage of the increasing demand for medical supplies and information about COVID-19 by registering domain names that include keywords, such as “coronavirus” or “COVID”. All sorts of harmful operations, such as C2 servers, malware distribution, and phishing, are supported by these bogus websites. Malicious registrations, such as malware and phishing, increased by 569% from February to March 2020, according to data provided to Interpol by a private sector partner, and high-risk registrations increased by 788% during the same period. Also Google reported that

they managed to block 126 million COVID-19 phishing scams in just one week [19].

2.3.5. Misinformation

The public is being flooded with fake news and misinformation at an alarming rate. Conspiracy theories, incomplete threat assessments, and unverified information have all intensified public fear and, in some situations, made it easier for cyberattacks to be carried out. Almost a third of the countries that took part in the global survey [19] on cybercrime reported that incorrect material about COVID-19 was being circulated. One country reported 290 postings in a month, most of which contained hidden spyware [19]. Also, in this survey, it has been reported that false medical information is being sold illegally. Scams involving 'too good to be true' offers like free meals, unique bonuses, or substantial discounts at supermarkets were another source of incorrect information spread via mobile text messages.

Following the COVID-19 pandemic, statista.com [22] conducted a survey among IT experts all over the world, and investigated whether the pandemic has left an impact on the landscape of the cyberattacks. The recent survey was done in August 18, 2021 and its main findings, as depicted in Figure 2, show an increase in cyberattacks since the COVID-19 outbreak, with the majority of the rise occurring in the area of data exfiltration and leakage. Phishing emails are also becoming more common, with half of the respondents reporting that they had received one recently.

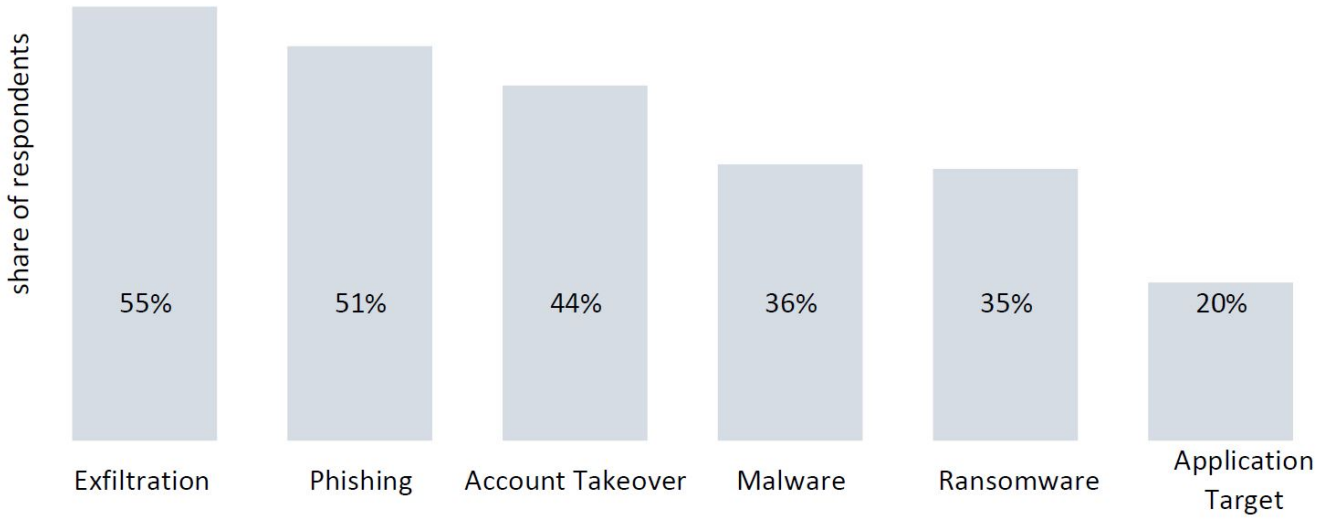

Figure 2. Landscape of the cyberattacks after COVID-19 [22]

People all around the world are becoming increasingly reliant on the internet, which is opening up new economic prospects. However, many firms and individuals are not keeping their cyber defences up to date which may lead to privacy and security problems. The lesson learnt from surge in cyberattacks during COVID-19 would reinforce the necessity for greater public-private sector cooperation if we are to effectively combat the privacy and security threat posed by COVID-19 to our cyber space. Cybercrime is only going to get worse in the near future. Cybercriminals will continue to ramp up their activity and create more advanced and sophisticated methods of operation as a result of vulnerabilities associated with working from home and the potential financial gain that this brings. To take advantage of the public's anxiety over the outbreak, criminals will likely continue to use coronavirus as a theme

in their phishing and online frauds. The economic crisis and changes in the business sector will certainly lead to an increase in Business Email Compromise schemes, creating new chances for criminal activity.

One of the main lessons learned of the COVID-19 cybersecurity threats is that the threats is global, so it needs a global effort to compact such threats for future similar events. This was started, as previously mentioned, by two big cybersecurity centres – *National Cyber Security Centre (NCSC)* of the United Kingdom and the *Cybersecurity and Infrastructure Security Agency (CISA)* of the United States – when they formed a joint advisory committee on April 8, 2020 as a response to COVID-19 related attacks. In the future, it is possible to see regulatory bodies for approving and controlling cybersecurity software as there would be a raise of the security expectations. Also, the *Security-by-Design* would be the main stream for developing secure software.

2.4. National cybersecurity strategies and COVID-19

Apart from the negative security and privacy impact caused by COVID-19 pandemic, it showed positive impact through digitization which enabled the continuous running of the business during lockdown. The digitization is a significant enabler of the progress in many, if not all, sectors including economy, social, healthcare and education. Recently, it was reported in [23] that digitization is essential for accomplishing the 17 Sustainable Development Goals (SDGs) developed by the United Nations and which constitute a vital appeal to action by all nations either developed or developing ones.

The digitization of the activities of economy, social, healthcare sectors cannot achieve intended outcomes without safe and secure digital infrastructures. On the other hand, there is a rapid growth of cybersecurity threats that can affect a country's digitization process. So, there is a need for a National Cybersecurity Strategies (NCSs) for each country. Responding to this, according to Global Cybersecurity Index 2020 [24], many countries are developing NCSs. In the past two years, the number of nations that have adopted NCSs has increased by 40%. Nevertheless, despite recent improvements, 60% of least developed countries (LDCs) still lack strategies, and the majority of developing nations that have created NCSs failed to implement them due to a lack of financial and human resources.

To help policymakers, such as governments, to address the above concerns, a guide for developing NCSs has been developed by many international partners including ITU, Microsoft, INTERPOL, and WorldBank [25]. Because of COVID-19, the guide included techniques and approaches on how to *strengthen infrastructures resilience and service availability to disasters and pandemics*. The guide presents a practical and adaptable framework to aid policymakers in developing, updating, implementing, monitoring, and assessing their strategies. Apart from the guidance and advice, the question is now how the least developed and developing countries can secure a budget to implement a national security strategy. If this cannot be achieved, such countries would not be able to use the advantages of the Internet to achieve advancement. Consequently, this would lead to the injection of more cybercriminals looking for financial gain.

2.5. Discussion of recent research

This section will cover a brief discussion of the recent literature of three important tools and mechanisms used to achieve security for the companies and organization during the pandemic.

Antivirus tools: When it comes to protecting one's computer, one of the most important steps a user may take is to install antivirus software. Iakovakis et al. [26] conducted a comparison among various antivirus tool to see which is effective to compat cyber-attacks and threats during COVID-19. They identified and used nine criteria: price, malicious URL blocking, strengths, weaknesses, phishing protection, on-demand malware scan, on-access malware scan, website rating, and behavior-based detection. The comparison and analysis showed two main points. Firstly, there are a handful antivirus software products – including Sophos, Avast, Avira, and Bitdefender Free Edition – which are available for absolutely no cost and still effective in detecting most of the viruses and blocking malicious URLs. Secondly, the most well-known antivirus tools such as McAfee, Symantec Norton, Kaspersky, Trend Micro, and Bitdefender have met all criteria but need to be updated. This study could be improved considering the privacy of the users. There are several questions which still need to be investigated and these include what type of data will be collected from users and where such date will be stored? Will the user have access to any information related to their privacy and will the collected data be shared with other third parties?

VPN: Research and Markets at Yahoo estimated that by 2026, it is anticipated that the *Global Virtual Private Network* (VPN) would reach 91.20 USD Billion [27]. The global VPN market is predicted to increase from 38.56 USD billion in 2021 to 45.89 USD billion in 2022, because of the impact of the pandemic which forced companies to use VPN products to secure working from home.

One of the recent research in this area is about scaling VPN during a major disaster such as pandemics [28]. As discussed above, the pandemic radically altered how we live and work. Companies were forced to let their employees to work from home. To protect proprietary information, monitor staff efficiency, and control shareholder profitability while satisfying customer demand, the telecommunications sector needed to scale up VPN. The main recommendation of the paper [28] is to increase the broadband and use seamless VPN tunnels to enable connecting remote users with their company network. Although scaling up the use of VPN to support the expected increase of remote working, the study overlooked deep security analysis including attacks such as man-in-the-middle attacks. These attacks are possible to be mounted since it is possible for an adversary to take control of a VPN session and decode the data being sent and received. Public people who do not work for companies and do not use security environments may be at an increased risk of having their private information disclosed.

Multi-factor authentication: Multi-Factor Authentication (MFA) mechanism was among the best practices recommended by security specialists and governments to compact security problems during the pandemic. A recent market report by marketsandmarkets.com [29] showed that it is anticipated that the size of the global market for multi-factor authentication would increase from 11.1 billion USD in 2021 to 23.5 billion USD by 2026. It showed that the main reason of this jump was the impact of the pandemic where there has been a huge increase in reliance on e-businesses including banking, financial services, healthcare, and retail sector. To better secure communications and transactions of businesses, multi-factor authentication was adopted where a system requires two or more credentials to login. MFA strengthens security because even if one credential is compromised, unauthorised users cannot meet the second authentication criterion and cannot access the targeted place, device, network, or database.

To further improve the efficiency and the security of the MFA mechanism to support remote work

depending on IoT and cloud technologies, Alsahlani et al. [30] have proposed a Lightweight MFA and authorization scheme which can be used for real-time data access in IoT and cloud-based applications. IoT and cloud-based technologies allow people to manage vital tasks remotely with minimal efforts, but also allow sharing and collecting sensitive information across insecure public channels which is risky. To overcome this problem, Alsahlani et al. [30] proposed a lightweight scheme which can provide MFA and also authorisation for IoT and cloud-based data access. This scheme could be used in many applications including the management of large-scale systems, e.g., healthcare industry. The main limitation of this scheme is privacy. The information obtained from the users is kept on a remote server and users do neither have access to any information linked to their privacy nor they know how it will be processed.

3. Public health policy

3.1. Planning

Since the onset of the pandemic, computational technology has played a critical role in planning emergency protocols for governments and organizations worldwide. The results have been crucial for developing proper public health policy frameworks to control the impact of the pandemic. One of the earliest uses of computational technology was at the pandemic's epicenter in Wuhan, China. Big data analysis and artificial intelligence were used to forecast the movement of potential Covid-infected individuals who dispersed from Wuhan after the outbreak. This forecast was constructed using machine learning models, trained on movement data collected from mobile phones, mobile payment applications, and social media. This forecasting model allowed China to put in place containment measures to frame the spread. Similarly, Taiwan integrated immigration records with its centralized, real-time national health insurance database. This integrated data allowed Taiwan authorities to cross-reference records and determine individuals who have traveled to Wuhan or been in contact with someone who has been to Wuhan. These individuals could then be quarantined and tested. These procedures have drastically decreased the early spread of the virus [31].

Predictive modeling was also designed to identify geographical areas that potentially need to be restricted. These models were challenged by the need to process and extract features from heterogeneous sources of information [32]. The management of personal protective equipment was also a critical challenge in the early months of the pandemic. One solution for this issue was developed by Swedish Health Services, a USA-based healthcare organization. The company developed a platform for healthcare workers to report real-time data on volumes of patients with COVID-19, personal protective equipment, staffing, ventilator usage, and other information. This platform leverages big data technologies, supported with high-performance computers, to provide an immediate service for proper monitoring of resources so that any shortfall could be quickly identified, and resource balancing for high-demand areas and those in need can be implemented.

Due to the unknown nature of the virus, there was limited amount of information about it and hence hindered the planning for virus containment. Iceland has one of the highest per-capita testing rates, and was among the first counties to put in place mobile apps to report symptoms. This symptom dataset was collected and used in conjunction with clinical and genome sequencing to reveal characteristics of the virus such as its pathology and transmissibility. The app was available in all platforms and phone devices to increase its coverage among the population. The data gathered by the app have significantly

increased the awareness of the virus, and was tailored to plan its control.

3.2. Monitoring

Another significant challenge that attracted many researchers was the development of strategies for monitoring the population and identifying COVID-19 cases. Furthermore, the identification of any case automatically triggers its contact tracing. In Taiwan, as shown in Figure 3, high-performance infrared thermal cameras were set up in airports to detect individuals who have fevers so that they can be prioritized for testing. The use of thermal temperature played a central role in many other countries. In Singapore, for example, temperatures were monitored at public building entrances to identify potential COVID-19 hotspot areas. A private company in the USA also used digital thermometers to collect real-time body temperature information. The data collected were then combined with resting heart rate data collected from smartwatch applications to develop a methodology to proactively identify COVID-19 emerging outbreaks. Likewise, an interactive map of potential COVID-19 cases was created in Germany from data collected from a smartwatch application. The application gathers pulse, temperature, and sleep pattern data then evaluates these for possible viral illness.

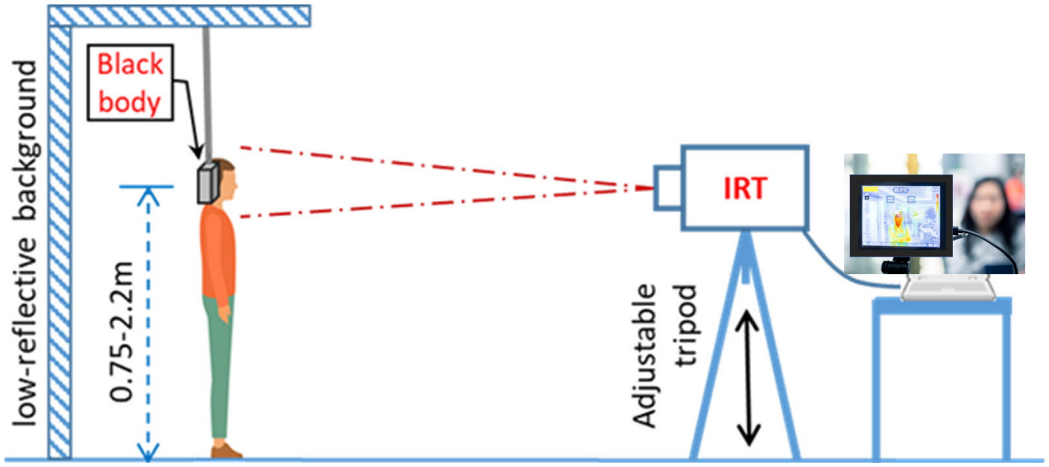

Figure 3. Thermal imaging systems

Thermal cameras suffered from many challenges such as their ineffectiveness when simultaneously capturing temperatures of multiple individuals when they are interleaved in front of the camera (e.g., pedestrians crossing from both sides of the road). Therefore, they need a special setup to allow an alignment of the individuals under test, to avoid mass temperature screening. Besides, these systems can only capture surface skin temperature, which is typically lower than the oral measured temperature. So, they may miss few positive cases, besides requiring corrections to reduce the gap between skin and oral measured temperatures.

Another essential use of monitoring technologies was in the area of contact tracing (Figure 4). Traditionally, upon the detection of positive cases, they are interviewed by public health officials to reveal their proximities, and potential exposures. Then, they reach out to exposed individuals and request their test and self-quarantine. While this process was found to be effective with previous epidemics, COVID-19 has revealed its limitations since it is labor-intensive and time-consuming. Also, the rapid spread of the virus has created a shortage in the public health staff, hindering the timely

tracing of infected individuals. Therefore, intelligent computing systems were needed to mitigate these challenges.

One of the most comprehensive forms of COVID-19 contact tracing was seen in South Korea, where the whole process was fully automated: security camera footage, facial recognition technology, bank card records, and GPS location data from vehicles and mobile phones, are all used to monitor individuals. In the event of a positive case, the monitoring data are used to ascertain the possible exposed contacts and emergency text alerts sent to them and others in the general region. Another application of contact tracing was in Singapore. The mobile phone application exchanges short-distance Bluetooth signals when individuals are close. Exposed contacts could then be identified based on the information collected by the application.

Figure 4. Contact tracing through wearable devices

Yet, contact tracing applications still have their own drawbacks. Not all apps were compatible with old mobile devices, because they did require various permissions, and advanced features that average devices did not have. That is why, the app was effective with only a small fraction of the users. For example, after the first month of its launch, the Singapore app was adopted by only 20% of the targeted individuals. As the lockdown started to be alleviated, the app adoption has reached 40% by summer 2021.

3.3. Mitigation

In the fight against COVID-19, one of the main mitigation tools has been the use of quarantine and isolation measures to isolate confirmed and potential cases from the general population. In China, quarantined individuals must fill out an app-based symptom survey and record their temperature. This information is then used to monitor an individual's movement and track the severity of their symptoms. The system then provides color codes associated with the exposure level of the individuals. Similarly, in Taiwan, home quarantine is supported by geofencing and GPS applications running on government-issued mobile phones. When an individual breaches quarantine, a message is sent to the mobile phone, and a fine is imposed. South Korea and Iceland use a similar approach for home quarantine. However, the monitoring application runs on the individual's personal phone. In Canada, blockchain technology was used to create an app called Civitas, which associates people's official IDs with blockchain records to verify whether a person has permission to leave his/her home.

Similar to contact tracing, any mobile-based software solution faces the challenge of being easily left behind by users when they are moving. In some countries, wearable devices, such as smart watches, have been explored as an alternative to mobile phone tracking. In Hong Kong, cloud-based technology

is used to support wearable risk bans that are assigned to individuals in home-quarantine. In the event of breaching a mandatory quarantine order, authorities are alerted. In Australia, quarantine violations could be punished by requiring individuals to wear tracking devices, after which any further breaches would incur a fine.

Figure 5. Drones used for COVID-19 impact management

Human resource demands to enforce COVID-19 measures such as quarantine and mask mandates have strained many countries worldwide. This strain has led some countries to turn to drones and other robotic solutions to supplement frontline workers. Figure 5 illustrates the range of functionalities that have been developed using drone technologies. Using AI-based drones and surveillance cameras, China supports its quarantine measure to limit gathering sizes and identify individuals not wearing masks. India company, Cyient, provided unmanned aerial drones to law enforcement in Telangana. The drones are used for maintaining COVID-19 lockdown restrictions for a wide area with less staffing. Violations spotted by the drone can be promptly forwarded to law enforcement for handling. Another advantageous use of drones is for public announcements. This practical use of drones was demonstrated in European countries such as Spain, where Madrid police used loudspeaker equipped drones to inform the public about the guidelines for the imposed state of emergency.

Drone and other robotic devices have also been used to sanitize contaminated areas to reduce human exposure. Examples of disinfecting drones have been seen in India, China, and some European countries. For instance, the Spanish military has used modified DJI-made drones, previously intended for agricultural use, to spray disinfecting chemicals over public spaces. In the robotics sphere, a Danish robotics company, UVD Robots, has developed multiple disinfection robots to be delivered to hospitals worldwide. Another example is an autonomous disinfection robot to help limit the number of hospital-acquired infections created by US-based Xenex Disinfection Services. The company was established by two John Hopkins educated epidemiologists.

4. Medical healthcare

4.1. Diagnosis

Given that COVID-19 was a new virus and had similarities to other diseases such as influenza and pneumonia, its detection was not easily done in the early stages of the pandemic. However, artificial intelligence research has sought to remedy the diagnosis process. Roy et al. [33] used artificial neural networks to analyze lung ultrasonography (LUS) images to detect the presence and severity of the virus at the frame-level, video level, and pixel-level. The approach was developed using fully annotated

dataset of LUS images collected from several Italian hospitals, with labels indicating the degree of disease severity at a frame-level, video level, and pixel-level (segmentation masks).

In radiology, extensive research has been done to diagnose the virus using a variety of techniques. Wang et al. [34] created COVIDNet, which is based on a convolutional neural network (CNN) trained on 13,800 images collected from 13,725 patients. COVIDNet leverages its model to detect infected patients. Similarly, Panwar et al. [35] developed a deep learning-based detection model for a quick virus identification within 5 seconds using X-ray images. Wang et al. [36] developed a fully automated process for the virus diagnosis and prognosis using deep learning technology using X-ray and CT scan images.

To alleviate limited x-ray training data issues, Oh et al. [37] developed a neural network for COVID-19 diagnosis that is suitable for training with limited X-ray images by adopting DenseNet103 and ResNet-18. Vaid et al. [38] also tackled the issue of limited data by developing a transfer learning approach to build a deep learning model by transferring pre-trained CNNs. Sing et al. [39] tackled the issue of optimizing CNN models for detection of COVID-19 from CT-Scans by using a multi-objective differential evolution algorithm to optimize the model's hyperparameters.

Many similar diagnosis models were put into practical use in the public health system worldwide. For example, China implemented a cloud-based AI-enabled system to quickly diagnose pneumonia attributable to COIVD-19 to distinguish it from other lung diseases [40]. Additionally, machine learning solutions developed in China can predict severe condition development for COIVD-19 patients. Clinicians can then use this information to guide the treatment of the patient and resource deployment.

The pandemic has also accelerated the use of telemedicine services for handling patients with and without COVID-19. In Canada, telemedicine visits for patients increased from approximately 1000 visits per day in February 2020 to 14000 per day in May 2020. Telemedicine use has allowed for infected individuals with mild and moderate symptoms to be diagnosed and treated without further exposing the public. The use of telemedicine services is also illustrated by Hospitals such as George Washington University Hospital in the USA and the state governments of Andhra Pradesh and Assam in India. George Washington University Hospital offers video consultations and live Facebook webinars to provide remote medical expertise to several people. Similarly, the state governments of Andhra Pradesh and Assam have utilized telemedicine to offer health services to potential COVID-19 infected individuals.

4.2. Treatment

Since the COVID-19 pandemic started, AI and big data analytics have played an indispensable role in fast-tracking the development process for treating COVID-19 cases. These technologies have been employed to find ways to re-purpose existing drugs and expedite the development of new medicines. For example, the German company Innoplexus AG developed an AI-supported platform to study a combination of existing drugs such as Remdesivir (an experimental antiviral developed initially to treat Ebola), Chroloquine, Tocilizumab (an immunosuppressive drug), Pegasys (used to treat Hepatitis B & C), and Clarithromycin (an antibiotic) to establish the best option for COVID-19 treatment [41].

A British start-up named Exscientia, in collaboration with other entities, has also created an AI-based solution that determines the most effective combination of compounds to treat COVID-19. The results will then be used to develop a drug for public use if it is successful in a successful clinical trial. Other potential AI-based research for re-purposing drugs to treat COVID-19 was done with Baricitinib

and Afatinib (used to treat non-small cell lung cancer).

Figure 6 shows the spectrum of computational intelligence's applications in modern technologies to fight the pandemic.

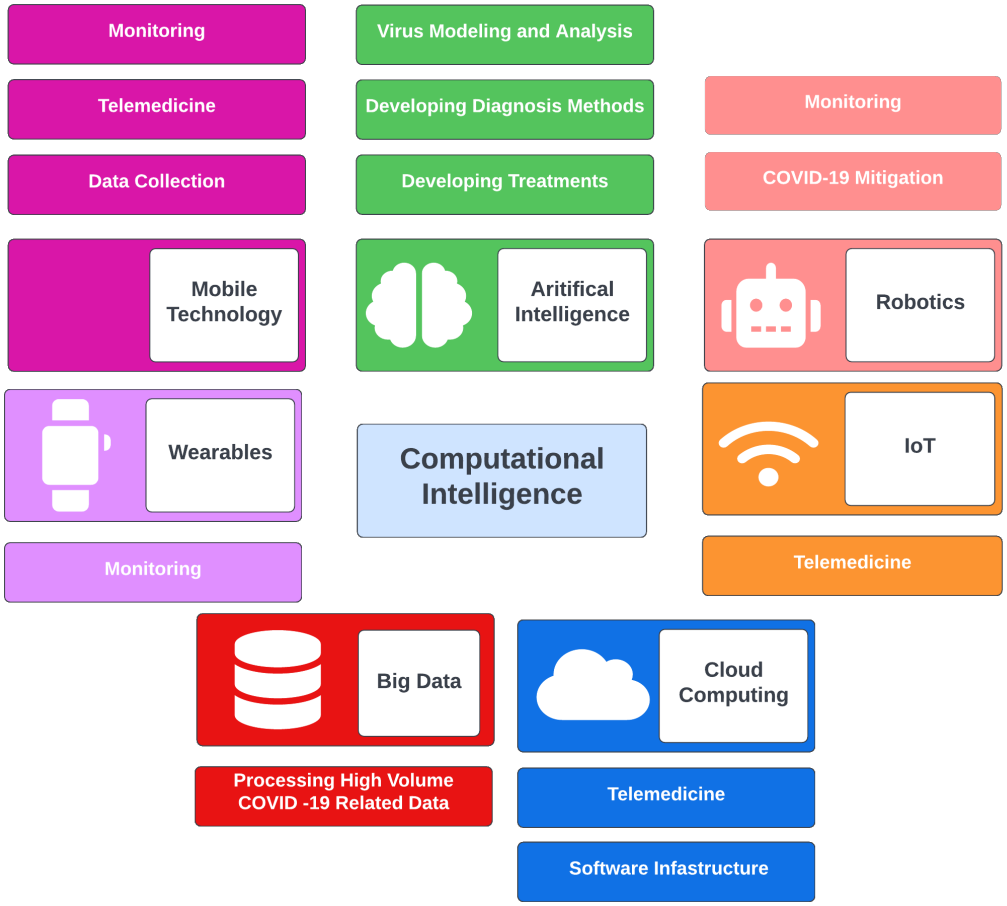

Figure 6. Applications of computational intelligence

4.3. Summary of intelligent computing systems usage

AI-based technologies and algorithms have become the backbone of the governmental and public health sectors, in combating the pandemic. Table 1 provides a summary of COVID-19 management categories, and their corresponding technologies. Various neural network-based models are being currently used in hospitals to optimize resource allocations, in vaccine development, and in the analysis of cell-phone data to trace those who have been in contact with or proximate to individuals diagnosed with the disease. While machine learning can help make pandemic response more efficient and expedite progress toward effective treatments, privacy, equity and related human rights concerns also abound.

Neural networks are built to learn data representation for various purposes including predictions and classifications. Representation learning allows the detection and recognition of features in particular data points and allows the identification of similar data points once the model is trained. Neural networks are powerful in replacing humans and performing various tasks without the need of humans'

support in extracting features. Therefore, neural networks were heavily relied on for detecting patterns that identify the virus, as soon as data is being collected. Neural networks were able to learn representations of virus propagation and the characteristic symptoms of the COVID-19 viral infection.

However, there were many challenges related to the adoption of such solutions. To develop deep neural networks, there is a need for a significant amount of data to properly learn the patterns of the virus. Due to its dynamic nature, it was extremely hard to collect sufficient amounts of data that would achieve a uniform performance across all variants that are coming from different geographical locations. That is why, as the virus was spreading across many countries, there was a collective effort of bringing together all sorts of data from various regions, to collectively build data sets and train models. One example of the very early data that were collected was X-ray images of tested positive patients chests. These images were fed into a particular type of artificial neural networks, called convolutional neural networks (CNNs). CNNs have provided promising results and emerged as one of the popular solutions. For instance, Wang et al. [34] proposed COVIDNet, CNN-based model for positive cases based on their chest X-ray images. The model was built using a set of images collected from 13,725 patients. The CNN architecture of the model uses a lightweight residual block, and a projection expansion technique, as part of enhancing the model accuracy while keeping its computational complexity low. Attention schemes were used by Han et al. [42] to train a deep 3D multiple instance learning model (AD3D-MIL) to identify the virus from 3D chest computed tomography images. The model makes binary classification of common pneumonia, along with interpreting the results by indicating the dominant features driving the binary decision.

As a summary, neural networks have been used to tackle the problem of symptoms characterization. This is primarily due to the explosion of medical images of positive cases. As more varients of the virus are appearing, more variants of the models themselves are being re-enforced. For instance, recurrent neural network models (RNNs) have surged as a reliable alternative for time series prediction. With the increase in the number of cured patients, datasets of treatment records are now available for training as time series. Moreover, the adoption of IoT technologies for smart care, is generating massive amounts of data that can be used to enhance the performance of current models and refine them to also detect current and future variants of the virus.

The blockchain technology can bring another layer of protection to data reliability. This can be useful as it can handle the heterogeneous nature of the data being collected from multiple sources, under various formats [43]. It also provides another layer of protection against data alteration. Because of the distributed nature of blockchain, it is more reliable when it comes to individual points of failure. Blockchain represents an opportunity to process the data in a decentralized fashion, while ensuring its reliability [44]. Generally speaking, emerging technologies, such as the blockchain, provide solutions of data privacy, lack of information, communications technology infrastructure, and monetary contrast. Governments need to establish needed infrastructures and its corresponding regulations to protect their citizens. The lessons learned from this pandemic will benefit us in all facets of healthcare, including the potential next crisis.

5. Conclusions

Computational intelligence has been heavily solicited as a response to the massive outbreak of COVID-19. Various researchers have been developing intelligent methods, discussed in this paper, that

Table 1. Summary of used technologies

	Description	**Digital Technology**	**Example Countries**
Planning	Projecting spread & impact of COVID-19 to guide healthcare policy	AI	China
		Big Data	Taiwan
		Mobile Technology	USA
			Iceland
Monitoring	Observing the population for potential COVID-19 cases	Mobile Technology	USA
		Digital thermometer	South Korea
		Big Data	Singapore
		Wearables	
		GPS	
		Bluetooth	
Mitigation	Measures for controlling the spread of COVID-19	AI	South Korea
		Mobile Technology	China
		Big Data	Australia
		Wearables	
		Cloud Computing	
		IoT	
		Drones	
Diagnosis	Developing methods detection of COVID-19 cases	AI	Canada
		Big Data	USA
		Cloud Computing	India
		Telemedicine	
Treatment	Developing medical treatments of COVID-19 cases	AI	UK
		Big Data	Germany

	Potential Advantages	Potential Disadvantages
Planning	Guides resource management & health-care polices	The pandemic has numerous variables that can throw off projections
Monitoring	Early detection of potential COVID-19 cases for testing	Privacy concerns
	Contact tracing & isolation	Limited ability to detect asymptomatic individuals
	Provides information on disease prevalence & pathology.	High cost to manage extensive monitoring system
		Failure to detect exposed individuals if the application is deactivated, mobile device is absent, or Wi-Fi/ cell connectivity is inadequate
Mitigation	Limits spread of the virus	Limited citizen freedom of movement
		Restricted access to food and essential services
		Privacy concerns
		Restricted access for the uninfected
		Failure to detect quarantined individuals if the application is deactivated, mobile device is absent, or Wi-Fi/ cell connectivity is inadequate
Diagnosis	Correctly diagnose individuals with COVID-19	Privacy breach
	Facilitate remote care	Extensive testing prior to approval for public use
		High cost
Treatment	Accelerate development of medical treatments	Extensive testing prior to approval for public use
	Repurpose existing medicines to fight COVID-19	High cost

can be incorporated into AI-enabled systems for combating the pandemic. Yet, the widespread usage of online resources (e.g., [45]) as means to pursue industrial and educational functions has brought its own challenges in terms of privacy and security. For instance, this paper has shown how such an online setting has significantly increased cybercrime.

Despite the large number of studies proposing various intelligent computing systems, their adoption in practice was challenged by various constraints that scientists and scholars typically do not address in their research papers. For instance, there is a strong assumption that the execution environment is capable of deploying these models and providing the necessary hardware and software requirements, which has been found to be nearly impractical, since many of these systems were lightweight mobile apps and wearable IoT devices. Furthermore, many of these models were not properly documented for software developers to acknowledge how exactly they should be deployed and used in real-world settings. Another interesting observation across the discussed papers, is that the models evaluation was theoretical, and relies on traditional validation metrics, such as precision, recall, and AUC. While there is no discussion on how these highly performing models would cost the manufacturers and software developers. For example, many of the trained deep learning models are found to be expensive in terms of energy consumption. Thus, shipping them into mobile and wearable devices would be challenging.

Another interesting insight reveals how these models were trained on specific datasets which may become quickly obsolete as new variants of the virus keep appearing. So there is a need for planning to reinforce the learning of these models, but many of their corresponding papers do not tackle this problem, leaving the assumption that these models are parameterized in an ad-hoc fashion. In such a scenario, not only the model can become quickly deprecated, its update would be unreasonable for software maintainers, with no prior knowledge. The lack of expertise on how models should be pipelined in the software update lifecycle would eventually cause a waste of development and maintenance effort, and therefore needs to be addressed by future studies.

Acknowledgments

This study has received a public grant through the national program “Programme d’Investissements d’Avenir (PIA)” under the reference ANR-18-RHUS-0004. This work is part of the Federation Hospitalo-Universitaire (FHU) Saclay and Paris Seine Nord Endeavour to PerSonalize Interventions for Sepsis (SEPSIS). This work is also supported by ANR PIA funding: ANR-20-IDEES-0002.

References

1. Robert SH Istepanian and Turki AlAnzi. Mobile health (m-health): Evidence-based progress or scientific retrogression. In *Biomedical Information Technology*, pages 717–733. Elsevier, 2020.
2. Cong Duc Tran and Tin Trung Nguyen. Health vs. privacy? the risk-risk tradeoff in using covid-19 contact-tracing apps. *Technology in Society*, 67:101755, 2021.
3. JL Boyles, A Smith, and M Madden. Apps and privacy: More than half of app users have uninstalled or decided to not install an app due to concerns about their personal information, 2015.
4. Navid Ali Khan, Sarfraz Nawaz Brohi, and Noor Zaman. Ten deadly cyber security threats amid covid-19 pandemic. 2020.

5. Consumer Reports. It's not just zoom. google meet, microsoft teams, and webex have privacy issues, too., 2020. Last accessed 06 April 2022.
6. Aaron R Brough and Kelly D Martin. Consumer privacy during (and after) the covid-19 pandemic. *Journal of Public Policy & Marketing*, 40(1):108–110, 2021.
7. WIRED. Hackers are targeting hospitals crippled by coronavirus, 2020. Last accessed 29 March 2022.
8. NCSC. Advisory: Covid-19 exploited by malicious cyber actors, 2020. Last accessed 29 March 2022.
9. Cybersecurity Ventures. Cybercrime to cost the world $10.5 trillion annually by 2025, 2020. Last accessed 29 March 2022.
10. Debra Littlejohn Shinder and Michael Cross. *Scene of the Cybercrime*. Elsevier, 2008.
11. Harjinder Singh Lallie, Lynsay A Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105:102248, 2021.
12. Jason RC Nurse. Cybercrime and you: How criminals attack and the human factors that they seek to exploit. *arXiv preprint arXiv:1811.06624*, 2018.
13. Ken Tysiac. How cybercriminals prey on victims of natural disasters, 2018. Last accessed 29 March 2022.
14. Emma Elsworthy. Hundreds of bushfire donation scams circulating., 2020. Last accessed 29 March 2022.
15. Tomáš Foltýn. You have not won! a look at fake fifa world cup-themed lotteries and giveaways, 2018. Last accessed 29 March 2022.
16. NHS. 9 tips to help if you are worried about covid-19, 2020. Last accessed 29 March 2022.
17. Paloma de las Cuevas, Pablo García-Sánchez, Zaineb Chelly Dagdia, María-Isabel García-Arenas, and Juan Julián Merelo Guervós. Automatic rule extraction from access rules using genetic programming. In *International Conference on the Applications of Evolutionary Computation (Part of EvoStar)*, pages 54–69. Springer, 2020.
18. CGI. Helping defend against a 30,000% increase in phishing attacks related to covid-19 scams, 2020. Last accessed 29 March 2022.
19. INTERPOL. Interpol report shows alarming rate of cyberattacks during covid-19, 2020. Last accessed 29 March 2022.
20. Jessica Davis. Covid-19 impact on ransomware, threats, healthcare cybersecurity, 2020. Last accessed 29 March 2022.
21. Jessica Davis. Google blocking 18m coronavirus scam emails every day, 2020. Last accessed 29 March 2022.
22. Statista.com. Where do it professionals see an increase in cyber attacks and attack attempts following the covid-19 pandemic?, 2021. Last accessed 30 March 2022.

23. Marco Obiso Isabel Neto and Marjo Baayen. How tailored national cybersecurity strategies enable safe, inclusive and sustainable digital development, 2022. Last accessed 12 June 2022.

24. Global Cybersecurity Index. Global cybersecurity index 2020, 2020. Last accessed 12 June 2022.

25. NCS Guide 2021. 2nd edition of the guide to developing a national cybersecurity strategy, 2021. Last accessed 12 June 2022.

26. George Iakovakis, Constantinos-Giovanni Xarhoulacos, Konstantinos Giovas, and Dimitris Gritzalis. Analysis and classification of mitigation tools against cyberattacks in covid-19 era. *Security and Communication Networks*, 2021, 2021.

27. Yahoo.com. Global virtual private network (vpn) markets report 2022, 2022. Last accessed 14 June 2022.

28. Jack Joe. Safely scaling virtual private network for a major telecom company during a pandemic. *Available at SSRN*, 2022.

29. marketsandmarkets.com. Multi-factor authentication market (2022 - 2026), 2022. Last accessed 14 June 2022.

30. Yaser Fahad Ahmed Alsahlani and Alexandru Popa. Lmaas-iot: Lightweight multi-factor authentication and authorization scheme for real-time data access in iot cloud-based environment. *Journal of Network and Computer Applications*, 192:103177, 2021.

31. Deedra Vargo, Lin Zhu, Briana Benwell, and Zheng Yan. Digital technology use during covid-19 pandemic: A rapid review. *Human Behavior and Emerging Technologies*, 3(1):13–24, 2021.

32. Joseph T Wu, Kathy Leung, and Gabriel M Leung. Nowcasting and forecasting the potential domestic and international spread of the 2019-ncov outbreak originating in wuhan, china: a modelling study. *The Lancet*, 395(10225):689–697, 2020.

33. Subhankar Roy, Willi Menapace, Sebastiaan Oei, Ben Luijten, Enrico Fini, Cristiano Saltori, Iris Huijben, Nishith Chennakeshava, Federico Mento, Alessandro Sentelli, et al. Deep learning for classification and localization of covid-19 markers in point-of-care lung ultrasound. *IEEE transactions on medical imaging*, 39(8):2676–2687, 2020.

34. Linda Wang, Zhong Qiu Lin, and Alexander Wong. Covid-net: A tailored deep convolutional neural network design for detection of covid-19 cases from chest x-ray images. *Scientific Reports*, 10(1):1–12, 2020.

35. Harsh Panwar, PK Gupta, Mohammad Khubeb Siddiqui, Ruben Morales-Menendez, and Vaishnavi Singh. Application of deep learning for fast detection of covid-19 in x-rays using ncovnet. *Chaos, Solitons & Fractals*, 138:109944, 2020.

36. Shuo Wang, Yunfei Zha, Weimin Li, Qingxia Wu, Xiaohu Li, Meng Niu, Meiyun Wang, Xiaoming Qiu, Hongjun Li, He Yu, et al. A fully automatic deep learning system for covid-19 diagnostic and prognostic analysis. *European Respiratory Journal*, 56(2), 2020.

37. Yujin Oh, Sangjoon Park, and Jong Chul Ye. Deep learning covid-19 features on cxr using limited training data sets. *IEEE transactions on medical imaging*, 39(8):2688–2700, 2020.

38. Shashank Vaid, Reza Kalantar, and Mohit Bhandari. Deep learning covid-19 detection bias: accuracy through artificial intelligence. *International Orthopaedics*, 44(8):1539–1542, 2020.

39. Dilbag Singh, Vijay Kumar, Manjit Kaur, et al. Classification of covid-19 patients from chest ct images using multi-objective differential evolution–based convolutional neural networks. *European Journal of Clinical Microbiology & Infectious Diseases*, 39(7):1379–1389, 2020.

40. Li Bai, Dawei Yang, Xun Wang, Lin Tong, Xiaodan Zhu, Nanshan Zhong, Chunxue Bai, Charles A. Powell, Rongchang Chen, Jian Zhou, Yuanlin Song, Xin Zhou, Huili Zhu, Baohui Han, Qiang Li, Guochao Shi, Shengqing Li, Changhui Wang, Zhongmin Qiu, Yong Zhang, Yu Xu, Jie Liu, Ding Zhang, Chaomin Wu, Jing Li, Jinming Yu, Jiwei Wang, Chunling Dong, Yaoli Wang, Qi Wang, Lichuan Zhang, Min Zhang, Xia Ma, Lin Zhao, Wencheng Yu, Tao Xu, Yang Jin, Xiongbiao Wang, Yuehong Wang, Yan Jiang, Hong Chen, Kui Xiao, Xiaoju Zhang, Zhenju Song, Ziqiang Zhang, Xueling Wu, Jiayuan Sun, Yao Shen, Maosong Ye, Chunlin Tu, Jinjun Jiang, Hai Yu, and Fei Tan. Chinese experts' consensus on the internet of things-aided diagnosis and treatment of coronavirus disease 2019 (covid-19). *Clinical eHealth*, 3:7–15, 2020.

41. Vinay Chamola, Vikas Hassija, Vatsal Gupta, and Mohsen 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*, 8:90225–90265, 2020.

42. Zhongyi Han, Benzheng Wei, Yanfei Hong, Tianyang Li, Jinyu Cong, Xue Zhu, Haifeng Wei, and Wei Zhang. Accurate screening of covid-19 using attention-based deep 3d multiple instance learning. *IEEE transactions on medical imaging*, 39(8):2584–2594, 2020.

43. Dinh C Nguyen, Pubudu N Pathirana, Ming Ding, and Aruna Seneviratne. Blockchain for 5g and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*, 166:102693, 2020.

44. Sin Kuang Lo, Xiwei Xu, Mark Staples, and Lina Yao. Reliability analysis for blockchain oracles. *Computers & Electrical Engineering*, 83:106582, 2020.

45. Zaineb Chelly Dagdia and Ana Cristina Simões E Silva. Effects of covid-19 pandemic on education and society. *STEM Education*, 2, 2022.

AIMS Press