Telehealth interventions during COVID-19 pandemic: a scoping review of applications, challenges, privacy and security issues

Muhammad Tukur [iD] ,[1,2] Ghassan Saad,[1] Fahad M AlShagathrh,[1] Mowafa Househ,[1] Marco Agus[1]

¹ICT, Hamad Bin Khalifa University College of Science and Engineering, Doha, Qatar
²Computer Science, Gombe State University, Gombe, Nigeria

Correspondence to
Dr Marco Agus;
magus@hbku.edu.qa

Muhammad Tukur;
mutu15902@hbku.edu.qa

ABSTRACT

Background The COVID-19, caused by the SARS-CoV-2 virus, proliferated worldwide, leading to a pandemic. Many governmental and non-governmental organisations and research institutes are contributing to the COVID-19 fight to control the pandemic.

Motivation Numerous telehealth applications have been proposed and adopted during the pandemic to combat the spread of the disease. To this end, powerful tools such as artificial intelligence (AI)/robotic technologies, tracking, monitoring, consultation apps and other telehealth interventions have been extensively used. However, there are several issues and challenges that are currently facing this technology.

Objective The purpose of this scoping review is to analyse the primary goal of these techniques; document their contribution to tackling COVID-19; identify and categorise their main challenges and future direction in fighting against the COVID-19 or future pandemic outbreaks.

Methods Four digital libraries (ACM, IEEE, Scopus and Google Scholar) were searched to identify relevant sources. Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR) was used as a guideline procedure to develop a comprehensive scoping review. General telehealth features were extracted from the studies reviewed and analysed in the context of the intervention type, technology used, contributions, challenges, issues and limitations.

Results A collection of 27 studies were analysed. The reported telehealth interventions were classified into two main categories: AI-based and non-AI-based interventions; their main contributions to tackling COVID-19 are in the aspects of disease detection and diagnosis, pathogenesis and virology, vaccine and drug development, transmission and epidemic predictions, online patient consultation, tracing, and observation; 28 telehealth intervention challenges/issues have been reported and categorised into technical (14), non-technical (10), and privacy, and policy issues (4). The most critical technical challenges are: network issues, system reliability issues, performance, accuracy and compatibility issues. Moreover, the most critical non-technical issues are: the skills required, hardware/software cost, inability to entirely replace physical treatment and people's uncertainty about using the technology. Stringent laws/regulations, ethical issues are some of the policy and privacy issues affecting the development of the telehealth interventions reported in the literature.

Conclusion This study provides medical and scientific scholars with a comprehensive overview of telehealth technologies' current and future applications in the fight against COVID-19 to motivate researchers to continue to maximise the benefits of these techniques in the fight against pandemics. Lastly, we recommend that the identified challenges, privacy, and security issues and solutions be considered when designing and developing future telehealth applications.

INTRODUCTION

COVID-19, caused by the SARS-CoV-2 virus, was first identified in China in December 2019 and later became a pandemic.[1 2] When this manuscript was finalised (12 June 2022), globally, the total number of infected cases had reached 540 318 million and over 6.331 million people had died.[3]

Telehealth refers to the delivery of healthcare particularly preventive and primary healthcare over a distance. Furthermore, it has been described as the use of medical information exchanged from one site to another via electronic communication to improve a patient's health.[4] It can also be defined as distributing health-related services and information through electronic information and telecommunication technologies. It enables long-distance patient and clinician care, contact, reminders, advice, education, intervention and remote admissions. During the spread of COVID-19, several technological interventions were introduced to help manage the pandemic (eg, utilisation of digital tools to combat the COVID-19 pandemic[5] such as internet of things (IoT), drones, artificial intelligence (AI), blockchain and 5G).[6]

When the COVID-19 pandemic pushed the healthcare system to its breaking point, telehealth appeared as a critical alternative for burdened physicians and organisations.[7] Telehealth was a valuable tool in the fight against the COVID-19 pandemic.[8 9] Functions such as remote patient monitoring,[10–12] communication and counselling,[13] psychotherapy,[14] telerehabilitation, consultation,[15] and telementoring[14] became extremely popular, useful features for delivering healthcare. As telehealth became characterised by technologies, users, environment, processes and organisations, telehealth became multi-layer healthcare system support. However, increased data privacy issues,[8 16] human error, social factors, psychosocial factors, technological issues and other external factors are bringing about the need for better control of telehealth applications.

In this study, we have conducted a scoping review covering four different databases: ACM, IEEE, Scopus and Google Scholar; and identified 28 telehealth intervention challenges/issues. The challenges/issues were categorised into technical (14), non-technical (10), and privacy, and policy issues (4). The issues reported in this article comprise both technical and behavioural security concerns, issues such as attacks, vulnerabilities, weaknesses are examples of technical security issues found in the literature. While ethical issues such as 'a clinician may improperly exploit patient data to conduct genetic or biological investigations or dispense medications that violate approved regulations' are examples of behavioural security issues reported in our reviewed articles. Furthermore, the reported telehealth interventions were classified into two main categories: AI-based and non-AI-based interventions. The distinction between AI and non-AI telehealth is significant since it represents the degree of automation and intelligence engaged in healthcare service delivery. Traditional telehealth services that rely on basic videoconferencing, remote monitoring and other communication technologies to support interactions between patients and healthcare practitioners are referred to as non-AI telemedicine. In contrast, AI-enabled telehealth uses powerful machine learning algorithms, natural language processing and other AI techniques to evaluate patient data, develop insights and deliver individualised suggestions to patients and healthcare professionals.[17]

Moreover, AI-enabled telehealth has the potential to greatly improve healthcare delivery quality and efficiency. AI algorithms, for example, may assist clinicians in efficiently analysing massive quantities of patient data, identifying patterns and trends, and making correct diagnoses.[17 18] Its virtual assistants and chatbots may also give real-time assistance, support and education to patients, which can enhance patient engagement, self-management and adherence to treatment programmes. Nevertheless, it is also critical to acknowledge the possible dangers and obstacles connected with AI-enabled telehealth, such as data privacy concerns, algorithmic bias and the ethical implications of depending on machine-based decision-making in healthcare. As a result, it is vital to carefully weigh the benefits and downsides of both AI and non-AI telehealth systems, as well as to ensure that proper protections are in place to protect patients and preserve the highest standards of care. Thus, our study aimed to achieve the following research questions.

Research questions/objectives

The main objective of this survey is to identify and classify telehealth interventions that emerged during COVID-19 pandemic, document their challenges, and policy, privacy and security issues. This is to motivate researchers to continue to maximise the benefits of these techniques to fight COVID-19 and other diseases, and as well consider the issues/solutions reported when designing and developing future telehealth applications. Therefore, this study aimed to answer the following research questions to address this goal:

▶ What are the distinct types of telehealth interventions that appeared and became popular during the COVID-19 pandemic?
▶ What are telehealth intervention challenges when fighting the COVID-19 pandemic?
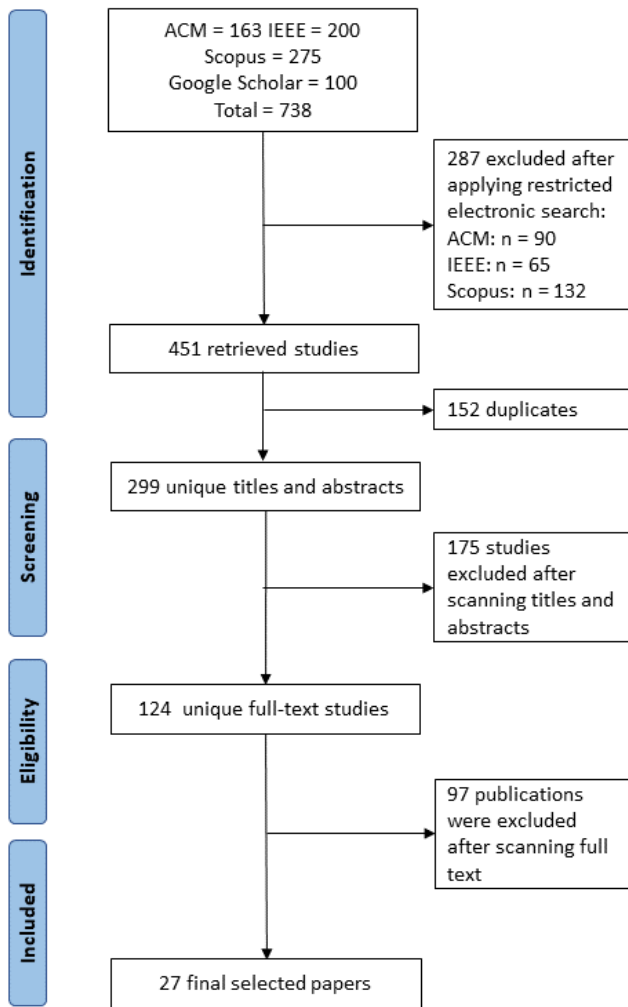▶ What are telehealth intervention policy, privacy and security issues specific to fighting the COVID-19 pandemic?

Research contributions

The contributions of this study can be summarised as follows:

▶ Identification, classification and analyses of the various kinds of telehealth interventions that appeared or were adopted during COVID-19;
▶ Identification, categorisation and analyses of the challenges of telehealth interventions that appeared or were adopted during COVID-19.
▶ Identification of policy, privacy and security issues about telehealth interventions aiding in fighting the COVID-19 pandemic.
▶ Identification of remedies available for tackling reported telehealth intervention policy, privacy and security issues when fighting the COVID-19 pandemic.

Previous studies have attempted to survey the telehealth interventions that emerged during the COVID-19 pandemic and the challenges associated with them.[17 19–22] These studies can be classified according to their study design and the main issues reported. Some studies conducted a systematic mapping study and focused solely on telehealth security issues,[23] while others have conducted systematic reviews on the use of telehealth during COVID-19, emphasising the features, benefits and effects of the reviewed systems.[19–22] However, some of these studies have only covered a few articles or general challenges without specifically addressing privacy, policy, and security issues and solutions.[19–21] Additionally, some studies have had limited search comprehensiveness by covering only a few databases,[21] or a specific type of telehealth intervention, such as AI-based systems[17]—a scoping

Figure 1 PRISMA chart for included studies. PRISMA: preferred reporting items for systematic reviews and meta-analyses.

Table 1 Publication venue of the selected papers

#	Venue	Type	# of publications
1	*IEEE*	Journal	8
2	*IEEE*	Conference	3
3	*IEEE*	Symposium	1
4	*ACM*	Journal	2
5	*ACM*	Conference	4
6	*ACM*	Workshop	1
7	*JMIR*	Journal	2
8	*BMJ*	Journal	1
9	*JAMA*	Journal	1
10	*New England Journal of Medicine Jama*	Journal	1
11	*Medknow Publications*	Journal	2
12	*SciELO Brasil*	Journal	1
	Total		27

December 2021 and 15 December 2021. Table 1 lists the publication venues of the final included articles. The detailed procedure of the method followed is provided as online supplemental material (Methodology).

RESULTS
Types of telehealth applications
Several studies presented telehealth interventions and their applications. These studies can be classified into two main categories according to their mode of application: The first category is AI-based; this category includes AI-based systems incorporating IoT and mechanical aspects and reported applications using machine learning or deep learning neural networks. The second category includes applications that do not employ any AI neural networks and are therefore categorised as non-AI based.

The following subsections present a general overview of some AI-based and non-AI-based telehealth interventions from our included studies.

AI-based techniques in fighting against COVID-19
This section presents a general review of some of our selected articles that discuss AI-based telehealth interventions during COVID-19. As Topol[25] describes it, the ultimate prospect for AI in medical technology is to restore the 'valuable bond between patients and physicians—the human touch,' in addition to lowering mistakes and enabling medical staff to spend more quality time.

As a result of the obstacles posed by COVID-19 and the associated lockdowns, many organisations and individuals have adapted robots to help them handle the pandemic's hurdles.[1] While compared with human methods, robotic and autonomous techniques have benefits such as inherent virus immunity and the impossibility of

review. In contrast, our study covered both AI-based and non-AI-based systems, and to the best of our knowledge, none of the existing studies have combined all of the above four contributions. Hence, this study can be considered the first comprehensive study to identify, classify, discuss and analyse the telehealth interventions, their associated challenges and issues, as well as discussing societal considerations (privacy, policy, security) with respect to various system types, technical and behavioural issues. Our study also highlights how the challenges/issues imposed by the pandemic boosted research and technology towards the improvement and diffusion of telehealth solutions.

METHODS
PRISMA Extension for Scoping Reviews (PRISMA-ScR)[24] was used as a guideline procedure to develop this comprehensive scoping review. As illustrated in figure 1, the search procedure for this scoping review was extensive. The search execution was performed between 13

disease-causing germs passing from human to robot to human. However, the robotics sector still faces many technical challenges. Shen et al[1] evaluated over 200 studies discussing robotic systems that emerged or were repurposed during the COVID-19 outbreak to provide insights to academia and businesses. The authors explored the benefits and challenges of using an automated system to combat the COVID-19 pandemic. They discovered that robotic systems are generally effective solutions for most of the issues caused by COVID-19 during surgery, screening, diagnosis, disinfection, telehealth, care, manufacturing, logistics and interpersonal matters unique to pandemic lockdowns.

Ganesh et al[26] propose an IoT-based Smart Automated Health Machine, a user-friendly health machine with an interactive GUI for medical needs. It is a virtual health self-screening/check-up/test system that is meant to be an initial point of contact for patient screening to track heart rate, ECG, blood pressure, oxygen saturation and visual acuity. In addition, the system offers essential information and keeps track of various medical concerns and the necessities that need to be adopted. The efforts are part of the United Nations' SDG-3 target.

Chen et al[2] analysed the AI's primary scope and contributions in battling COVID-19 from illness detection and diagnostics, pathogenesis and virology, medication and vaccine development, and outbreak and dissemination prediction. The authors also summarise the available data and resources for AI-based COVID-19 studies. Finally, the main obstacles in combating COVID-19 and potential AI directions were highlighted. Chen et al[2] discovered that AI still has tremendous potential in this field. The article presents medical and AI scholars with an extensive view of the existing and future applications of AI technologies in the fight against COVID-19 to encourage scholars to continue maximising the benefits of AI and big data in the battle against COVID-19 and future pandemics. Ding et al[9] also surveyed various enabling systems and technologies with different application scenarios for tackling the COVID-19 pandemic. Their research focused on three scenarios: wearable devices for observing at-risk and quarantined individuals, assessing nurses and administrative health personnel, and expediting hospital admissions triage; inconspicuous sensing technologies for identifying disease and monitoring patients with relatively modest symptoms whose clinical state could abruptly develop; and telemedicine techniques for remote diagnosis and monitoring of COVID-19 and other relevant illnesses.

Another technique, the internet of medical things (IoMT)-based intelligent healthcare monitoring system, was presented by Dilibal.[11] The primary purpose of this technique is to remotely communicate in digital reality with optimum network throughput and latencies for quick decision-making process management during clinical assessments. Furthermore, the author claims that filtering and compressing raw medical information from real-time video footage is possible with the presented edge enabled IoMT computer architecture system.

Talukder and Haas[27] proposed a sophisticated smartphone-based care system that captures health information using progressive web applications (PWAs), incorporates the data with various health knowledge sources, and employs AI to assist diagnostic evaluation and patient stratification. In addition, the system may make recommendations for actions and treatments and be built with cybersecurity features to tackle data privacy and security issues. The application is built on next-generation internet technologies such as PWA, Web Speech API, Web-Bluetooth, Web-USB and WebRTC and works well with the intelligent hospital concept. However, implementing this system requires buying sophisticated hardware that might be costly to users.

The COVID-19 pandemic has caused an extreme scarcity of personal protective equipment, increasing the risk of infection among medical practitioners.[28] As a result, numerous studies have been conducted to develop enabling systems and techniques that limit disease risk among medical practitioners and other frontline workers. For example, Karanam et al[28] designed and developed a contactless patient positioning system using three-dimensional (3D) pose technology that addressed these issues. The authors showed how the device allowed remote scanning of a patient without physical closeness by presenting numerous parts of the system, including automatic calibration, positioning and multiview synthesis methods. While the presented technology allows medical scans to be contactless and more effective, it does not prevent healthcare practitioners from doing patient scans in person if desired in a non-pandemic situation.

Non-AI-based techniques in fighting against COVID-19

This section presents a general review of some of our selected articles that discuss non-AI-based telehealth interventions during the COVID-19 pandemic.

Li et al[14] proposed a remote telehealth monitoring technique for COVID-19-infected people in self-isolation that uses a multimodal fusion technique as a practical choice for monitoring self-isolated patients. The authors employed a radar sensor to observe basic activities and respiration and a smart wristband to get details on the patient's blood oxygen saturation and heartbeat. The authors conducted an experimental study with 10 volunteers with an average age of 28. They discovered that the technique is practical and realistic for tracking individuals in self-isolated situations. However, the method requires the purchase of some expensive hardware which might make the technology cost inhibitive to users.

Raj and Srikanth[29] initiated a study and field trial project to assess and evaluate the usefulness and efficacy of an 'assisted telemedicine' approach in tackling the accessibility gaps in the remote primary healthcare environment. Using a collaborative design paradigm, the effort also included creating a blueprint for an Assisted Telehealth app to meet medical consultation needs during and after the COVID-19 pandemic. For the 'assisted telemedicine' concept, a customised application was constructed,

and functionalities were gradually expanded based on observations and comments from different stakeholders. According to their preliminary research, this healthcare delivery paradigm can serve various populations and gain acceptability among multiple stakeholders. Using the capability approach lens, the potential impacts of this action were also investigated. The study encountered difficulties due to a lack of high-speed internet access, especially in remote, rural areas.

Elahraf et al[30] presented a service-oriented architecture for dynamically composing and managing tailored treatment plans, assuming an adequate knowledge base and internet service for the underlying systems of caregivers and service providers. The authors created a working prototype to show the practicality of their suggested model and explained the obstacles and problems resulting from putting it into practice. Nevertheless, the need for a sufficient knowledge base and internet services for the underlying systems of caregivers and service providers may not exist in some regions, particularly in distant, rural areas.

Collected telehealth intervention challenges

This section listed and categorised the challenges of the telehealth interventions summarised in online supplemental material, table 2. The reported challenges can be sorted into three categories: (1) technical challenges, (2) non-technical challenges and (3) policy and privacy issues. For more details about the challenges, you may refer to the references provided along with each challenge.

Technical challenges

The primary technical challenges mentioned in the reviewed studies are as follows; the challenges are listed based on their criticality; the top challenges are the most critical ones while the bottom ones are the less critical ones.

- ► Network issues (especially outside of the healthcare facility).[1 13 26 29–31]
- ► Difficulty in accurately differentiating between COVID-19 and typical pneumonia or other relevant diseases.[32 33]
- ► System reliability issues.[1 9 13 26 29]
- ► Performance and accuracy issues.[1 15 28 34]
- ► Compatibility issues.[12 35 36]
- ► Dataset availability issues.[2 9]
- ► Data imbalances between negative and positive samples.[2]
- ► A large amount of noisy data and rumours.[2]
- ► Scarcity of knowledge in the intersection of computer and medical sciences.[2]
- ► Power consumption.[9]
- ► Healthcare is highly resistant to change.[13]
- ► Technical glitches.[29]
- ► Insufficient bandwidth and resources, as well as effective effort maintenance.[29]
- ► Scalability, interoperability and auditability issues.[30]

Non-technical challenges

The primary non-technical challenges mentioned in the reviewed studies are as follows; similarly, the challenges are listed based on their criticality; the top challenges are the most critical ones while the bottom ones are the less critical ones.

- ► Lack of knowledge, technical literacy and skills needed to use virtual medical services (eg, not everybody can use telehealth services and disabled individuals and children need supervision to protect their integrity).[13 15 27 30 35–37]
- ► Cost associated with developing, subscribing, using or maintaining the system.[1 9 14 26 27 32]
- ► While telehealth technologies supply high-quality healthcare services, they cannot entirely replace physical treatment.[1 13 15 26 33]
- ► People's uncertainty about using technology.[15 26 29 33]
- ► Lack of public or private sector support for advancing medical technology that meets the demands of the populace.[15 29 37]
- ► Lack of knowledge and awareness about telemedicine and its benefits.[15 29]
- ► User service misuse.[26]
- ► Adoption rates are restricted to medical emergencies, which is insufficient.[13]
- ► Some users (especially those in rural areas) do not use phones.[29]
- ► It is difficult to have the same doctor(s) for follow-up appointments.[29]

Privacy and policy issues

The primary policy and privacy issues mentioned in the reviewed studies[2 9 11 13 26 29–31 37] are as follows:

- ► Local laws and stringent regulations could pose a challenge in installing systems, especially in remote areas.[26]
- ► Data privacy and human rights protection.[9]
- ► Ethical issues (eg, a clinician may improperly exploit patient data to conduct genetic or biological investigations or dispense medications that violate approved regulations).[37]
- ► A sound security system is needed to curb user service misuse.[26]

Collected telehealth intervention security issues

Telehealth devices provide aged, physically disabled patients and people in isolation due to COVID-19 with remote care such as surgeries, treatments and diagnoses. In this context, various systemic properties, such as security, must be met for telehealth systems to function correctly. Existing research examines various security incidents involving telehealth systems. This section discusses a comprehensive overview of the most reported telehealth application security issues and the presented remedies.

Marquez et al[23] recently performed a systematic mapping investigation to detect, organise and characterise telehealth systems' security vulnerabilities. The authors also
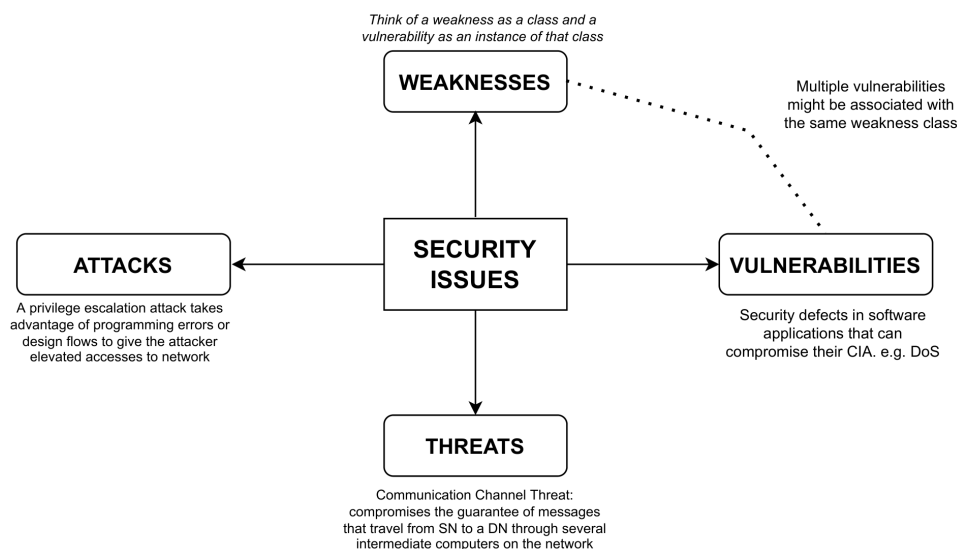
Figure 2 Most common telehealth security issues. SN, source node; DN, destination node; CIA, confidentiality, integrity and availability; DoS, denial of service.

noted how software engineering could aid in developing safe telehealth systems. The findings of their study show that: (1) the most reported security issues fall into four categories (ie, attacks, vulnerabilities, weaknesses and threats); (2) three security mechanisms (ie, detect attacks, stop or mitigate attacks and react to attacks) characterise security solutions and (3) the most related research topics are attributed to insecure data transmission and privacy. The study's findings also suggest that software design, requirements and models are vital areas that need to be focused on to develop secure telehealth systems.

Marquez et al[23] also reported that network protocol, such as HTTP (Hypertext Transfer Protocol), is the telehealth component most affected by security issues, followed by watermark, database and access control. Furthermore, in terms of medical supplies affected by security issues, the authors found that the electronic patient record is the most affected supply, followed by medical images, medical robots, wireless medical data and biosensors.

Specifying the most affected components/supplies could help researchers and developers know which components to put more effort into to mitigate reported security issues. Details about the most reported telehealth application security issues and proposed solutions are provided in the following subsections.

Most common telehealth privacy and security issues
Figure 2 illustrates the four most common telehealth security issues discussed in the following paragraphs.

Attacks
According to Marquez et al,[23] a privilege escalation attack uses programming faults or design defects to grant a hacker higher network access. The two types of privilege escalation are vertical and horizontal. Vertical privilege escalation needs an attacker to grant themselves greater authority. Horizontal privilege escalation entails the

attacker assuming the identity of another user with identical privileges while using the same level of privileges he already has.

Vulnerabilities
Software vulnerabilities (SVs) are security flaws in software applications that can compromise their confidentiality, integrity and availability.[1] Exploiting SVs can harm the operation and reputation of millions of software applications and organisations worldwide and cause significant financial losses. Therefore, it is crucial to remediate critical SVs as soon as possible.

Threats
The guarantee of information travelling from a source point to a destination via numerous intermediate channels on a network is threatened by the communication channel threats.[38] Hussain et al[38] and Chryssanthou et al[39] describe how social/community threats jeopardise telemedicine system security and name three types of threats: (1) technical, (2) ethical and (3) legal. The details of these threats can be found in Hussain et al.[38]

Weaknesses
While a vulnerability is often described in terms of weakness, defining a weakness itself can be difficult. A weakness can be considered a class and a vulnerability as an instance of that class because multiple vulnerabilities might be associated with the same weakness class. A single vulnerability could relate to two or more defects exploited concurrently or sequentially. In this regard, a vulnerability is a collection of one or more instances of weakness.

Most common solutions to telehealth privacy and security issues
As reported by Marquez et al[23] and illustrated in figure 3, the three most common telehealth security solutions are
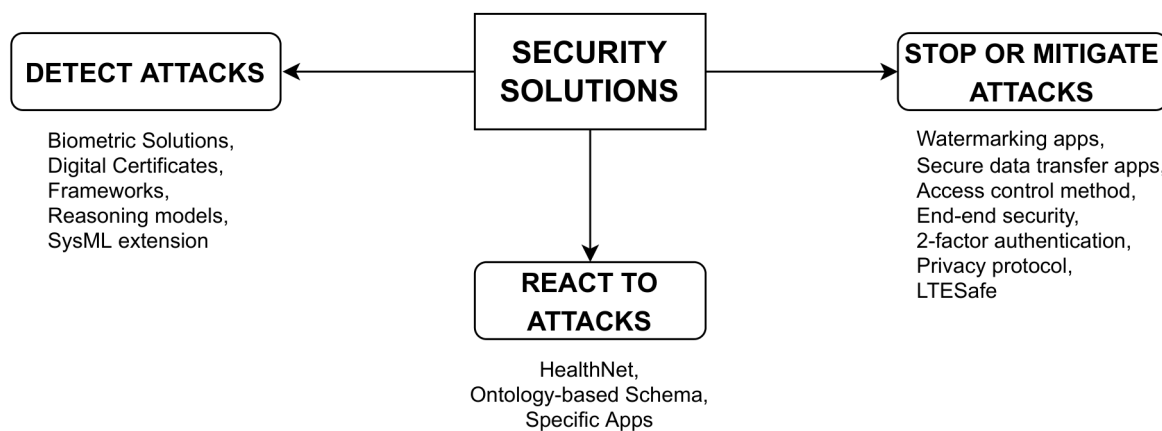
Figure 3 Most common telehealth security solutions.

to: detect attacks (eg, biometric solutions[40]), stop or mitigate attacks (eg, LTESafe,[34] watermarking apps[41]) and react to attacks (eg, healthNet[42]). LTESafe[34] is a cellular-assisted, privacy-preserving COVID-19 contact tracking tool that uses a deep neural network-based feature extractor to translate cellular CSI to a high-dimensional feature space, where the Euclidean distance between points represents device closeness. In this system, user privacy is protected by concealing the physical locations of devices while achieving excellent accuracy.

DISCUSSION
Summary and comparison of the proposed telehealth interventions
Online supplemental material, table 2 summarises and distinguishes the findings of the identified telehealth interventions based on the following criteria; this section discusses and compares the existing telehealth interventions summarised in online supplemental material, table 2.

▶ Intervention type: denotes the type of application. As discussed in Section 'Methods', there are two main categories. AI-based and non-AI-based systems.

▶ Scope: specifies the country/area where a particular application was developed or the intended origin of users/study.

▶ Technology used: denotes the kind of telecommunication or technical systems used to achieve telehealth purposes.

▶ Advantages/services: specifies the proposed intervention's uses, benefits and contributions in mitigating the COVID-19 pandemic.

▶ Challenges/limitations: specifies the key issues and constraints of the proposed systems.

As shown in online supplemental material, table 2, 12 out of the 20 (ie, 60%) of our surveyed telehealth interventions are AI-based systems,[1 2 9 11 13 26–28 33 34] while the remaining 8 (40%) are non-AI-based systems.[12 14 15 29 30 35–37] The research covered 11 different countries: the USA,[1 34] the UK,[26] China,[14 28 33] Austria,[32] Bangladesh,[31] Turkey,[11] India,[12 27 29] Ecuador,[15] Pakistan,[30] Qatar,[36] KSA[35] and

Brazil.[37] However, some reports[2 9 13] are surveys or reviews which are considered global.

Many telecommunications and technical systems have been used to help achieve remote healthcare. The technologies include but are not limited to mobile and tablet devices, wearable sensor devices, video conferencing tools, online portals, mobile apps/platforms, robotic systems, 3D pose, cameras, IoMT devices, GPS (Global Positioning System) technologies, ultra-wideband, radar sensor devices, smart bracelets, APIs, thermistors, and deep learning and machine learning tools.

A significant number of services and their usage have been reported in this paper. The most studied are patient tracking, triage and monitoring, disease detection and diagnosis, online consultations and prescriptions, disease spread analysis, healthcare accessibility-related challenge mitigation, and COVID-19 symptom checking. In addition, several challenges and limitations have been reported, and details are provided in Section ' Collected Telehealth Intervention Challenges'.

Principal findings
Overall, a total of 27 studies were selected, studied and analysed. The reported telehealth interventions were classified into two main categories: AI-based and non-AI-based interventions; their major contributions to tackling COVID-19 are in the aspects of disease detection and diagnosis, pathogenesis and virology, vaccine and drug development, transmission and epidemic predictions, online patient consultation, tracing, and observation; 28 telehealth intervention challenges/issues have been reported. The collected challenges/issues are classified into three main categories: technical, non-technical, and privacy, and policy issues. Fourteen technical challenges, 10 non-technical challenges and 4 privacy, and policy issues have been reported. Network issues (especially outside of the healthcare facility), system reliability issues, performance, accuracy, and compatibility issues are the most critical technical issues reported in at least 6, 5, 4 and 3 sources of our included studies, respectively. The skills required, hardware/software cost, inability to entirely replace physical treatment, and people's

uncertainty about using the technology are the most critical non-technical challenges reported in at least 7, 6, 5 and 4 sources of our included studies, respectively. Moreover, stringent laws/regulations, ethical issues are some of the policy, and privacy, issues affecting the development of the telehealth interventions reported in the literature. Furthermore, attacks, vulnerabilities, weaknesses and threats are the most common telehealth security issues reported in the literature, while three security mechanisms (ie, detect attacks, stop or mitigate attacks, and react to attacks) characterise the most common telehealth security solutions reported in the literature.

LIMITATIONS AND FUTURE WORK

Most of the selected research papers that introduced novel solutions about telehealth communicate their methodologies and testing procedures poorly or incompletely. They do not elaborate enough on the methods and criteria followed to reach their assumptions or findings. Considerable care and attention have been made to ensure this study's rigour. However, like any chosen research method, it is subject to validity threats. This research focused on a handful of well-known, top-ranking venues (such as *IEEE, ACM, JMIR, BMJ*), which limited our selection of papers and the overall quality of the papers selected. Even though other journals such as PubMed, MEDLINE, Ovid are not as well-known, highly ranked, as those selected for this paper (according to Google Scholar metrics), they still have the potential to offer higher-quality and more relevant research papers. Future work should include more research journals, regardless of how well known they are. Because the topic of this paper is related to the broad field of medicine, articles about telehealth are abundant. Thus, future research should also focus on a specific field in telehealth, such as 'remote monitoring devices' or application-based 'telehealth apps'.

CONCLUSION

This article presents an extensive survey that names and categorises digital health interventions, and their challenges, policy, privacy, and security issues are discussed. The digital health interventions found are mainly classified into AI-based and non-AI-based telehealth interventions. Moreover, the telehealth challenges are categorised into technical challenges (such as network, performance, accuracy, reliability and dataset availability issues) and non-technical challenges (such as cost, uncertainty and user service misuse). In addition, local laws, stringent regulations, ethical issues, data privacy and human rights protection, etc have been reported as policy, privacy and security issues affecting telehealth interventions. The authors of this paper believe that this paper's outcome should motivate scholars to continue to maximise the benefits of these techniques in the fight against COVID-19 and other future diseases. However, the identified

challenges, policy, privacy and security issues should be considered when designing and developing future telehealth applications.

ORCID iD
Muhammad Tukur http://orcid.org/0000-0003-1103-9659

REFERENCES

1. Shen Y, Guo D, Long F, *et al*. Robots under COVID-19 pandemic: a comprehensive survey. *IEEE Access* 2021;9:1590–615.
2. Chen J, Li K, Zhang Z, *et al*. A survey on applications of artificial intelligence in fighting against COVID-19. *ACM Comput Surv* 2022;54:1–32.
3. WorldMeter. World meters information - Corona virus cases. 2021. Available: https://www.worldometers.info/coronavirus/
4. Tuckson RV, Edmunds M, Hodgkins ML. Telehealth. *N Engl J Med* 2017;377:1585–92.
5. Zeng K, Bernardo SN, Havins WE. The use of digital tools to mitigate the COVID-19 pandemic: comparative retrospective study of six countries. *JMIR Public Health Surveill* 2020;6:e24598.
6. Chamola V, Hassija V, Gupta V, *et al*. A comprehensive review of the COVID-19 pandemic and the role of iot, drones, Ai, blockchain, and 5G in managing its impact. *IEEE Access* 2020;8:90225–65.
7. Hollander JE, Carr BG. Virtually perfect? Telemedicine for COVID-19. *N Engl J Med* 2020;382:1679–81.
8. Shachar C, Engel J, Elwyn G. Implications for telehealth in a postpandemic future: regulatory and privacy issues. *JAMA* 2020;323:2375–6.
9. Ding X, Clifton D, Ji N, *et al*. Wearable sensing and telehealth technology with potential applications in the Coronavirus pandemic. *IEEE Rev Biomed Eng* 2020;14:48–70.
10. Greenhalgh T, Koh GCH, Car J. Covid-19: a remote assessment in primary care. *BMJ* 2020;368:m1182.
11. Dilibal C. Development of edge-Iomt computing architecture for smart Healthcare monitoring platform. 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT); Istanbul, Turkey. IEEE, 2020

12 Gupta R, Bedi M, Goyal P, *et al*. Analysis of COVID-19 tracking tool in India: case study of Aarogya Setu mobile application. *Digital Government: Research and Practice* 2020;1:1–8.

13 Barr JR, D'Auria D, Persia F. Telemedicine, homecare in the era of COVID-19 & beyond. 2020 Third International Conference on Artificial Intelligence for Industries (AI4I); Irvine, CA, USA. IEEE, 2020

14 Li Q, Gravina R, Ye L, *et al*. A multi-sensor based method for self-isolated patient monitoring. In 2021 29th Mediterranean Conference on Control and Automation (MED); IEEE, 2021:651–6

15 Perez-Noboa B, Soledispa-Carrasco A, Padilla VS, *et al*. Teleconsultation apps in the COVID-19 pandemic: the case of Guayaquil city, Ecuador. *IEEE Eng Manag Rev* 2021;49:27–37.

16 Guo C, Tian P, Choo K-KR. Enabling privacy-assured fog-based data aggregation in e-healthcare systems. *IEEE Trans Ind Inf* 2020;17:1948–57.

17 Abd-Alrazaq A, Alajlani M, Alhuwail D, *et al*. Artificial intelligence in the fight against COVID-19: scoping review. *J Med Internet Res* 2020;22:e20756.

18 Wang Y, Hu M, Li Q, *et al*. Abnormal respiratory patterns classifier may contribute to large-scale screening of people infected with COVID-19 in an accurate and unobtrusive manner. *arXiv Preprint arXiv:200205534* 2020.

19 Monaghesh E, Hajizadeh A. The role of telehealth during COVID-19 outbreak: a systematic review based on current evidence. *BMC Public Health* 2020;20:1193.

20 Garfan S, Alamoodi AH, Zaidan BB, *et al*. Telehealth utilization during the COVID-19 pandemic: a systematic review. *Comput Biol Med* 2021;138:104878.

21 Khoshrounejad F, Hamednia M, Mehrjerd A, *et al*. Telehealth-based services during the COVID-19 pandemic: a systematic review of features and challenges. *Front Public Health* 2021;9:711762.

22 Hatef E, Wilson RF, Hannum SM, *et al*. Use of telehealth during the COVID-19 era: a systematic review. AHRQ publication No.23-EHC005. 2023. 10.23970/AHRQEPCSRCOVIDTELEHEALTH

23 Marquez G, Astudillo H, Taramasco C. Security in telehealth systems from a software engineering' viewpoint: a systematic mapping study. *IEEE Access* 2020;8:10933–50.

24 Tricco AC, Lillie E, Zarin W, *et al*. Prisma extension for Scoping reviews (Prisma-SCR): checklist and explanation. *Ann Intern Med* 2018;169:467–73.

25 Topol E. *Deep medicine: how artificial intelligence can make healthcare human again*. Hachette UK, 2019.

26 Ganesh D, Seshadri G, Sokkanarayanan S, *et al*. Autoimpilo: smart automated health machine using iot to improve telemedicine and telehealth. 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE); Bengaluru, India. IEEE, 2020

27 Talukder A, Haas R. Aiot: Ai meets iot and web in smart healthcare. WebSci '21; Virtual Event United Kingdom. New York, NY, USA, 2021

28 Karanam S, Li R, Yang F, *et al*. Towards contactless patient positioning. *IEEE Trans Med Imaging* 2020;39:2701–10.

29 Raj D, Srikanth TK. Assisted telemedicine model for rural healthcare ecosystem. WebSci '21; Virtual Event United Kingdom. New York, NY, USA, 2021

30 Elahraf A, Afzal A, Akhtar A, *et al*. A service-oriented framework for developing personalized patient care plans for COVID-19. *Proc Int Conf Digit Gov Res* 2021;2021:234–41.

31 Kaiser MS, Mahmud M, Noor MBT, *et al*. Iworksafe: towards healthy workplaces during COVID-19 with an intelligent Phealth app for industrial settings. *IEEE Access* 2021;9:13814–28.

32 Munsch N, Martin A, Gruarin S, *et al*. Diagnostic accuracy of web-based COVID-19 symptom checkers: comparison study. *J Med Internet Res* 2020;22:e21299.

33 Leyang L, Guixing C, Jun L. Review of method to automatic detection of COVID-19. ICIAI 2021; Xia men China. 2021

34 Yi F, Xie Y, Jamieson K. Cellular-assisted COVID-19 contact tracing. MobiSys '21; Virtual WI USA. New York, NY, USA, 2021

35 Alghamdi SM, Alqahtani JS, Aldhahir AM. Current status of Telehealth in Saudi Arabia during COVID-19. *J Fam Community Med* 2020;27:208.

36 Al Khal A, Al-Kaabi S, Checketts RJ. Qatar's response to COVID-19 pandemic. *Heart Views* 2020;21:129–32.

37 Caetano R, Silva AB, Guedes A, *et al*. Challenges and opportunities for Telehealth during the COVID-19 pandemic: ideas on spaces and initiatives in the Brazilian context. *Cad Saude Publica* 2020;36:e00088920.

38 Hussain M, Al-Haiqi A, Zaidan AA, *et al*. A security framework for Mhealth apps on android platform. *Computers & Security* 2018;75:191–217.

39 Chryssanthou A, Varlamis I, Latsiou C. Security and trust in virtual healthcare communities. PETRA '09; Corfu Greece. New York, NY, USA: Association for Computing Machinery, 2009

40 Zhang GH, Poon CC, Li Y, *et al*. A biometric method to secure telemedicine systems. *Annu Int Conf IEEE Eng Med Biol Soc* 2009;2009:701–4.

41 Giakoumaki AL, Perakis K, Tagaris A, *et al*. Digital watermarking in telemedicine applications--towards enhanced data security and accessibility. *Conf Proc IEEE Eng Med Biol Soc* 2006;2006:6328–31.

42 Barnickel J, Karahan H, Meyer U. Security and privacy for mobile electronic health monitoring and recording systems. 2010 IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks; Montreal, QC, Canada. IEEE, 2010:1–6