Fighting COVID-19 and Future Pandemics With the Internet of Things: Security and Privacy Perspectives

Mohamed Amine Ferrag, Lei Shu, *Senior Member, IEEE*, and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

***Abstract*—The speed and pace of the transmission of severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2; also referred to as novel Coronavirus 2019 and COVID-19) have resulted in a global pandemic, with significant health, financial, political, and other implications. There have been various attempts to manage COVID-19 and other pandemics using technologies such as Internet of Things (IoT) and 5G/6G communications. However, we also need to ensure that IoT devices used to facilitate COVID-19 monitoring and treatment (e.g., medical IoT devices) are secured, as the compromise of such devices can have significant consequences (e.g., life-threatening risks to COVID-19 patients). Hence, in this paper we comprehensively survey existing IoT-related solutions, potential security and privacy risks and their requirements. For example, we classify existing security and privacy solutions into five categories, namely: authentication and access control solutions, key management and cryptography solutions, blockchain-based solutions, intrusion detection systems, and privacy-preserving solutions. In each category, we identify the associated challenges. We also identify a number of recommendations to inform future research.**

***Index Terms*—Blockchain, COVID-19, healthcare, privacy, SARS-CoV-2, security.**

I. Introduction

THE global outbreak of the novel coronavirus 2019 (COVID-19) was declared by the World Health Organization (WHO) on 30 January 2020 [1]. The clinical symptoms of COVID-19 are predominantly pulmonary, although serious cardiovascular side effects were also observed in a number of patients [2]. Fig. 1 presents an overview of COVID-19 symptoms and protective strategies. Existing preventative solutions, include frequent hand wash using soap and water, or a hydro-alcoholic solution, and digital technologies such as mobile applications (e.g., contact tracing applications), artificial intelligence (AI), blockchain technology, drones, and robots to detect and limit the spread of the virus and track/monitor the movement of quarantined citizens [3]–[8].

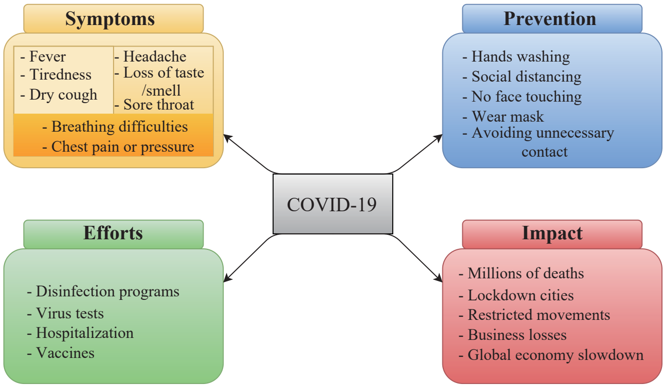


Fig. 1. Overview of COVID-19 symptoms and protective strategies.

A. COVID-19 Mobile Applications (Apps)

A number of governments/countries have introduced the use of official contact tracing apps for iOS and Android devices. Examples include Australia (COVIDSafe), Austria (Stopp Corona), Canada (COVID Alert), Denmark (Smittestop), Finland (Koronavilkku), France (StopCovid), Germany (Corona-Warn-App), Hong Kong, China (LeaveHomeSafe), Italy (Immuni), Singapore (TraceTogether), etc. In addition to these official contact tracing apps, some organizations (e.g., hospitals) have also used other systems and approaches such as COVID Symptom Tracker, HowWeFeel, COVID-19 Symptoms & Social Distancing Web Survey, Global COVID-19 Survey, and Beiwe, to facilitate the monitoring and management of the COVID-19 pandemic [9]. The COVID Symptom Tracker [10], for example, is created by medical doctors and scientists at Stanford University School of Medicine, King’s College London, Harvard T.H. Chan School of Public Health, and Massachusetts General Hospital, to track the spread of COVID-19 and study the symptoms of this virus.

Existing COVID-19 mobile apps can be categorised into six

Manuscript received March 8, 2021; revised April 9, 2021; accepted May 7, 2021. This work was supported in part by the Research Start-Up Fund for Talent Researcher of Nanjing Agricultural University (77H0603). The work of K.-K. R. Choo was supported only by the Cloud Technology Endowed Professorship. Recommended by Associate Editor Chenglin Liu. *(Corresponding author: Lei Shu.)*

Citation: M. A. Ferrag, L. Shu, and K.-K. R. Choo, “Fighting COVID-19 and future pandemics with the Internet of Things: Security and privacy perspectives,” *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 9, pp. 1477–1499, Sept. 2021.

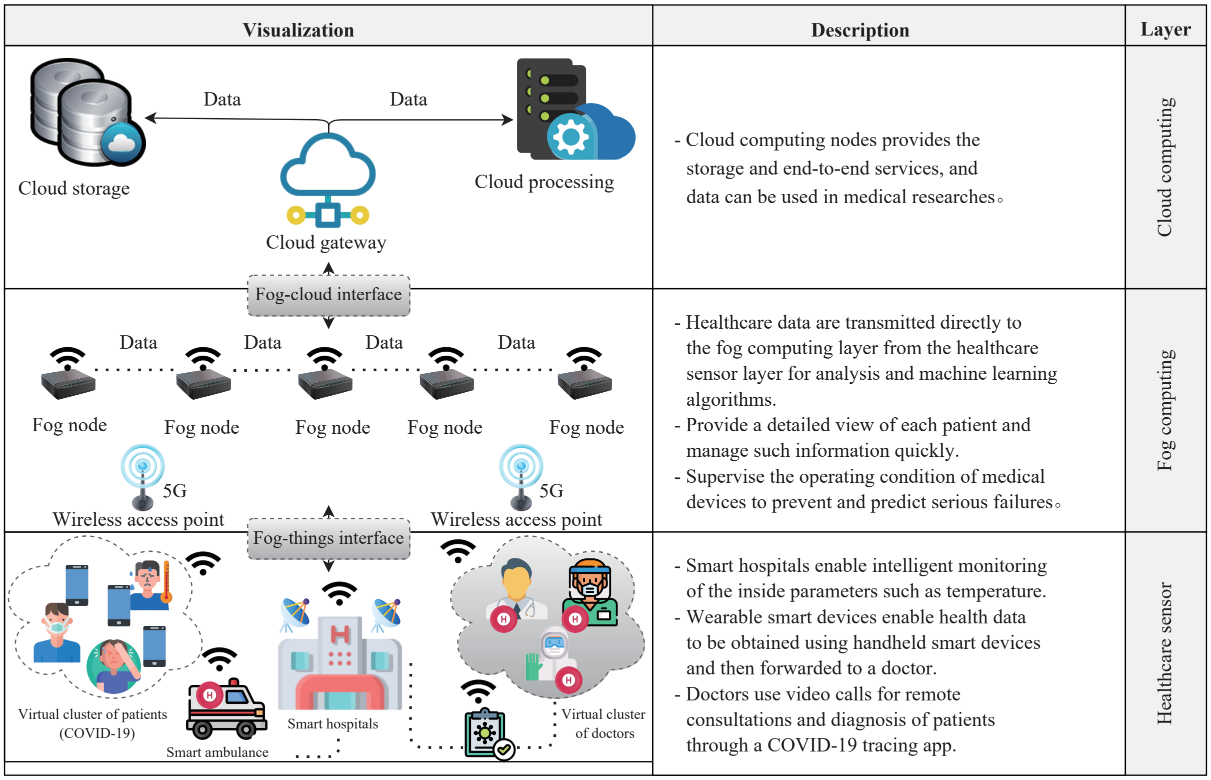
M. A. Ferrag is with the Department of Computer Science, Guelma University, B. P. 401, 24000, Algeria (e-mail: ferrag.mohamedamine@univ-guelma.dz).

L. Shu is with the College of Artificial Intelligence, Nanjing Agricultural University, Nanjing 210095, China, and also with the School of Engineering, University of Lincoln, Lincoln LN67TS, UK (e-mail: lei.shu@ieee.org).

K.-K. R. Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631 USA (e-mail: raymond.choo@fulbrightmail.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2021.1004087



Description	Layer
- Cloud computing nodes provides the storage and end-to-end services, and data can be used in medical researches。	Cloud computing
- Healthcare data are transmitted directly to the fog computing layer from the healthcare sensor layer for analysis and machine learning algorithms. - Provide a detailed view of each patient and manage such information quickly. - Supervise the operating condition of medical devices to prevent and predict serious failures。	Fog computing
- Smart hospitals enable intelligent monitoring of the inside parameters such as temperature. - Wearable smart devices enable health data to be obtained using handheld smart devices and then forwarded to a doctor. - Doctors use video calls for remote consultations and diagnosis of patients through a COVID-19 tracing app.	Healthcare sensor

Fig. 2. The use of IoT in healthcare systems during pandemics.

groups [11], namely: COVID-19 symptoms apps, COVID-19 contact tracing apps, COVID-19 health monitoring apps, COVID-19 research apps, telemedicine apps, and social distancing apps. These apps play different roles. For example, COVID-19 symptoms apps can facilitate users to monitor their own health, while COVID-19 contact tracing apps (e.g., COVIDWISE (for Virginia) and GuideSafe (for Alabama)) can be used by healthcare authorities to identify individuals who may have been in contact with an infected person. Also, data sensed/collected by COVID-19 health monitoring apps can be used by medical doctors to monitor the health of their patients. COVID-19 research apps can be used by research institutions to trace and study the spread of COVID-19, as well as its impacts. To enable video chat between medical doctors and their patients, telemedicine apps (e.g., Doctor On Demand, MDLive, and Amwell) can be adopted by healthcare providers. We also remark that these COVID-19 mobile apps can be integrated with other internet of things (IoT) devices and telecommunication networks (e.g., 5G) to enable public health institutions to further improve the quality of user experience and healthcare delivery, for example in terms of improved and real-time data and service access.

B. The Use of IoT Approaches to Fight Against COVID-19

The IoT is an ideal potential network for vaccine cold chain monitoring, healthcare management, healthcare delivery drones, remote patient monitoring, detecting and preventing infectious diseases such as COVID-19 [12]–[15]. As presented in Fig. 2, the use of IoT in healthcare systems to fight against epidemic situations like COVID-19 is structured in three layers, namely, the healthcare sensor layer, fog computing layer, and cloud computing layer. The healthcare sensor layer consists of IoT-enabled devices, including, smart hospitals, patients (COVID-19) with wearable smart devices, and doctors. The smart hospitals enable intelligent monitoring of the inside parameters such as temperature [16]. The wearable smart devices enable health data to be obtained using handheld smart devices and then forwarded to a doctor. The doctors use video calls for remote consultations and diagnosis of patients through a COVID-19 tracing app [17], [18]. The fog computing layer consists of network devices such as router, gateway, switch, and access points [19], [20]. The healthcare data are transmitted directly to the fog computing layer from the healthcare sensor layer via the 5G/6G wireless connectivity network for analysis and machine learning algorithms [21]. In addition, the fog computing layer provides a detailed view of each patient and manages such information quickly. The cloud computing layer consists of traditional cloud servers with sufficient computing resources to provides storage and end-to-end services [22].

The internet of bio-nanothings (IoBNT) concept considers the connectivity between the Internet and biological cells. The IoBNT's vision is to accelerate progress in biomedical research technologies based on synthetic biology, biosensors, integrated technologies, molecular communication, to achieve a better quality of life as well as human health, as discussed by Akyildiz *et al*. [23]. The advantages of using IoT approaches to fight against COVID-19 are presented in Table I. Regarding the diagnosis and treatment, the use of IoT approaches provides real-time patient monitoring based on IoT-powered telemedicine and reducing unnecessary medical visits as well as hospital stays. Therefore, thanks to the IoT

TABLE I
EXAMPLES OF IoT AND CONVENTIONAL APPLICATION USAGE DURING COVID-19 MANAGEMENT

Healthcare services	IoT-based approaches	Conventional approaches
Diagnosis and treatment	- Provide real-time patient monitoring based on IoT-powered telemedicine. - Reducing unnecessary medical visits as well as hospital stays.	- Patient monitoring is very slow. - Patients are required to visit the hospital for medical visits.
Drugs and equipment management	- Thanks to the IoT devices that are connected to the IoT network, drugs and equipment are efficiently administered and operated with lower costs.	- The cost of monitoring is extremely expensive with high error and loss rates.
Decision making	- The fog computing and cloud computing technologies enable cost-effective decision making using the data generated via IoT devices.	- Exposes patients to additional stress using the wrong decision.
Healthcare delivery	- IoT-enabled drones are used to deliver lightweight packages such as medical and vaccines.	- Patients are required to travel to buy drugs.
Vaccine cold chain monitoring	- Based on IoT sensors placed on the vaccine, the use of IoT applications can optimize the vaccine supply chain and can provide flexibility, efficiency, and speed.	- Lack of transparency and automating processes.
Disinfecting public spaces	- Provide real-time public spaces monitoring using IoT-enabled drones.	- Public spaces monitoring is very slow.
Digital medical passports and immunity certificates	- Blockchain-based solution stops the propagation of the COVID-19 virus using chained medical digital passports and immunity certificates.	- The integrity of immunity certificates is not confirmed and guaranteed.
COVID-linked symptoms	- LoRaWAN trackers and emerging wearables are used for detecting COVID-linked symptoms.	- Patients are required to visit the hospital.

devices that are connected to the IoT network, drugs and equipment are efficiently administered and operated with lower costs. The IoT architecture includes fog computing and cloud computing technologies which can enable cost-effective decision making using the data generated via IoT devices. Regarding healthcare delivery, IoT-enabled drones are used to deliver lightweight packages such as medical and vaccines. Based on IoT sensors placed on the vaccine, the use of IoT applications can optimize the vaccine supply chain and can provide flexibility, efficiency, and speed. The blockchain-based solution stops the propagation of the COVID-19 virus using chained medical digital passports and immunity certificates. In addition, LoRaWAN trackers and emerging wearables are used for detecting COVID-linked symptoms.

C. Related Works

In the literature, there are a number of recent surveys published in 2020 and 2021 for the use of IoT applications to fight against the COVID-19 pandemic. As shown in Table II, we categorize the related surveys according to the following criteria:

1) The Use of IoT Approaches: It indicates whether the survey described the use of IoT approaches.

2) Security and Privacy Requirements: It states if the survey has provided the security and privacy requirements as well as the threat models.

3) Security and Privacy Solutions: It indicates whether the survey presented a comparative analysis of potential solutions for security and privacy in epidemic situations like COVID-19.

4) Security and Privacy Challenges: It indicates whether the survey discussed the challenges and future research directions to combat COVID-19 as well as security and privacy challenges faced by the use of the IoT.

Most of the surveys on the use of IoT applications to fight against the COVID-19 pandemic outline the emerging technologies without focusing on security and privacy solutions. For example, a brief overview of solutions that IoT and associated sensor technologies have made to fight against the COVID-19 pandemic was discussed in [25], [26]. However, these surveys are very limited regarding detailed discussion on security and privacy solutions. Moreover, Ahmed *et al.* [24] provided an overview and detailed investigation of COVID-19 contact tracing apps with a discussion of users' concerns about their uses. Chamola *et al.* [4] presented a systematic survey that covers the role of various emerging technologies such as 5G, Blockchain, artificial intelligence, drones, and IoT in the fight against the COVID-19 pandemic. The feasibility of efficiency of edge computing and deep learning approaches for mitigating the COVID-19 pandemic were presented in [27]. Hussain *et al.* [28] provided a review on existing artificial intelligence techniques applied to the medical information-based pandemic as well as discussed the implementation of cloud and edge computing against COVID-19. The feasibility of efficiency of blockchain applications in combating the COVID-19 pandemic is presented in [31] and [32]. Table II summarizes the main focuses and major contributions of the previous comprehensive surveys on the use of IoT applications to fight against the COVID-19 pandemic. Although the above-mentioned surveys [28]–[30] have laid a solid foundation for the detection and classification of COVID-19 medical images using artificial intelligence techniques, our survey differs in several aspects. To the best of our knowledge, our survey is the first that thoroughly covers security and privacy solutions as well as challenges and future research directions faced by the use of IoT applications to combat COVID-19 and future pandemics.

D. Systematic Review and Meta-Analysis Methodology

The process of conducting our literature review is based on the following phases proposed by Snyder in [35]:

1) Designing the Review: The identification of literature for analysis in this paper was based on a keyword search, namely, "An IoT-based framework for COVID-19", "An IoT-based system for COVID-19", "An IoT-based protocol for COVID-

TABLE II
RELATED SURVEYS ON THE USE OF IOT APPLICATIONS TO FIGHT AGAINST THE COVID-19 PANDEMIC

Reference	Year	The use of IoT approaches	Security and privacy requirements	Security and privacy solutions	Security and privacy challenges	Main focus/contributions
Ahmed *et al*. [24]	2020	○	◐	◐	○	- An overview and detailed investigation of COVID-19 contact tracing apps.
Ndiaye *et al*. [25]	2020	●	○	○	◐	- A brief survey on the solutions that IoT and associated sensor technologies have made to fight against the COVID-19 pandemic.
Nasajpour *et al*. [26]	2020	●	○	○	○	- A review on the role of connected technologies for IoT in the fight against COVID-19.
Chamola *et al*. [4]	2020	●	○	○	◐	- A systematic survey that covers the role of emerging technologies such as 5G, Blockchain, artificial intelligence, drones, and IoT.
Sufian *et al*. [27]	2020	◐	○	○	○	- Feasibility of efficiency of edge computing and deep learning approaches for mitigating the COVID-19 pandemic.
Hussain *et al*. [28]	2020	◐	○	○	○	- A review on existing artificial intelligence techniques applied to COVID-19.
Siriwardhana *et al*. [21]	2020	◐	○	○	◐	- Feasibility of efficiency of 5G and IoT to fight against the COVID-19 pandemic.
Albahri *et al*. [29]	2020	○	○	○	○	- An overview of the detection and classification of COVID-19 medical images using artificial intelligence techniques.
Shi *et al*. [30]	2020	○	○	○	○	- An overview and detailed investigation of artificial intelligence techniques with X-ray and computed tomography for COVID-19.
Marbouh *et al*. [31]	2020	◐	○	○	◐	- A brief survey on blockchain applications in combating the COVID-19 pandemic.
Kalla *et al*. [32]	2020	◐	○	○	○	- A brief survey on the suitability of the blockchain as a potential key technology to combat the COVID-19 pandemic.
Jahmunah *et al*. [33]	2021	●	○	○	◐	- A literature review of contact tracing approaches and applications to combat the COVID-19 pandemic.
Nawaz *et al*. [34]	2021	○	○	○	○	- An overview and detailed investigation of artificial intelligence techniques for COVID-19 genome analysis.
Our survey	–	●	●	●	●	- A comprehensive survey on future research directions to combat COVID-19 as well as security and privacy challenges faced by the use of the IoT.

●: discussed, ◐: mentioned, ○: not mentioned.

19", and "An IoT-based scheme for COVID-19". Searching for these keywords in academic databases such as medRxiv, SCOPUS, Web of Science, Wiley Online Library, Google Scholar, and ACM Digital Library, an initial set of relevant sources were located. The search process provided a significant number of results, which only proposed IoT-based schemes for COVID-19 were collected.

2) Conducting the Review: The collected references have been evaluated based on the following key factors: a) reputation, b) pertinence, c) originality, and d) most influential articles in the topic area.

3) Analyze Data: After conducting the literature review and selecting a final sample, the articles are evaluated and analyzed according to the following key factors: a) network model, b) solution type, c) countermeasures, d) security and privacy requirements, e) resistance to attacks, f) advantages and disadvantages, and g) motivation and design goals for COVID-19.

4) Synthesize Data: Based on the evaluation and analysis of the articles, the sections are structured and synthesized to provide different types of information and different levels of details. Specifically, the final review article is structured in five sections, which offer an overview of future research directions to combat COVID-19 as well as security and privacy challenges faced by the use of IoT applications.

E. Our Contributions

The major challenge of IoT deployment for COVID-19 does not reside in the implementation of the emerging technologies, but primarily in the guarantee of security and privacy since the deployment of thousands of IoT based devices is in an open field [36]. For example, an adversary can use many cyber attacks, such as DDoS attacks to makes a service unavailable and then injects false data, which affects vaccine cold chain monitoring, healthcare management, healthcare delivery drones, and remote patient monitoring.

Our contributions in this work are:

1) We discuss the use of IoT applications to fight against the

COVID-19 pandemic, including, for diagnosis and treatment, drugs and equipment management, decision making, healthcare delivery, vaccine cold chain monitoring, disinfecting public spaces, digital medical passports, immunity certificates, and COVID-linked symptoms.

2) We overview security and privacy requirements as well as the threat models, and the challenges associated with developing IoT-based frameworks for COVID-19.

3) Based on review and a new taxonomy of state-of-the-art solutions, we provide a classification into five categories, namely, authentication and access control solutions, key management and cryptography solutions, blockchain-based solutions, intrusion detection systems, and privacy-preserving solutions.

4) We outline challenges and future research directions to combat COVID-19 as well as security and privacy challenges faced by the use of the IoT, such as the use of the internet of bio-nano things, applications of industry 4.0, IoTs solutions for vaccine shipments, computer vision for remote diagnosis, private patient information issues, vulnerabilities of machine learning techniques, compliance with healthcare data protection regulation, etc.

The remaining part of this paper is structured as Fig. 3. Section II focuses on security and privacy requirements. Section III describes threat models. Section IV presents security and privacy solutions to combat COVID-19. Section V describes future research against epidemic situation applications like COVID-19. Lastly, Section VI presents conclusions.

II. Security and Privacy Requirements

Due to continuing serious cyber attacks on public and private healthcare services, the proposal of a security and privacy solution to fight against epidemic situations like COVID-19 should provide and achieve the following requirements.

1) Conditional Privacy Preserving: Viewed as an essential characteristic of privacy protection, which there are two aspects: the protection of user privacy and the targeted retrieval of device information. In other words, the user's confidential data will be stored securely during the whole session. The unauthorized tracking to a specific device will not be permitted to be successful.

2) Differential Privacy: Refers to a set of mathematical techniques (e.g., stable transformations, randomized response, Laplace mechanism, and sensitivity) that enable big data analysis on epidemic situation applications to be performed without disclosing individual information.

3) Patient Anonymity: The open wireless transmission functionalities mean that communication channels of epidemic situation applications can be eavesdropped on by malicious devices. An adversary can analyze eavesdropped information such as user location, which seriously affects the user's privacy. Hence, the anonymity of each device in epidemic situation applications must be guaranteed. The security solution should assure that an adversary is unable to determine a user's true identity through intercepted data.

4) Unforgeability: In practical transmission of epidemic situation applications, an adversary can forge selectively legitimate credentials, authentication session keys, or other signatures in order to complete the verification process successfully [37]. Therefore, unforgeability against the chosen message attack is the main characteristic of a secured exchange of information.

5) Mutual Authentication: In the design of epidemic situation applications, mutual authentication is the primary and principal safety feature, which ensures that both units (Fog device, IoT device, Cloud center, etc.) in a session of communication can mutually authenticate each other. Thus, the identity theft attacks to specific equipment can be prevented [38].

6) Untraceability: The untraceability of patients of COVID-19 when a program is under the surveillance of an adversary is the characteristic that the adversary is unable to track the patients when moving from one location to the next destination. Usually, the security protocols achieves untraceability using identities, current timestamps, and random nonces.

7) Non-Repudiation: It guarantees the reliability of the data communicated in epidemic situation applications, where the originator of the data is not able to deny the validity of the signature transmitted.

8) Session Key Establishment: When mutual authentication takes place, one single session key between individual device and epidemic situation application system must be provided to ensure secure communication [39].

9) Session-Key Security: It maintains a secret session key between an approved member and an authorized device after they have successfully authenticated each other.

10) Perfect Forward Secrecy: To ensure the security of data previously sent, the security solutions for epidemic situation applications need to provide the perfect forward secrecy, which means that an adversary is unable to retrieve a session key from a previous session of two users, although the adversary may compromise the two users' private keys [40].

11) Patient Location Privacy: The idea of location privacy can be described as the ability of patients COVID-19 to choose exactly when and how their location credentials may be shared with other parties and for what purposes.

12) Patient Identity Privacy: It consists of applying protection technologies to minimize the disclosure of patient data that allow attackers to infer a patient's identity.

13) Patient Traceability: The medical center is capable of extracting the true identity of the patient by scanning pertinent information when requested. He *et al.* [41] designed a cross-domain handshake solution based on hierarchical identity-based cryptography, which can provide patient traceability.

14) Data Integrity: The integrity is one of the essential basic security requirements for the benign function of epidemic situation applications. Data integrity is the confirmation that the data that has been sent, received, or stored is complete and has not been altered. Therefore, security solutions use hash functions to provide data integrity. The blockchain-based solutions have integrity protection built-in since it is a tamper-proof and immutable ledger.

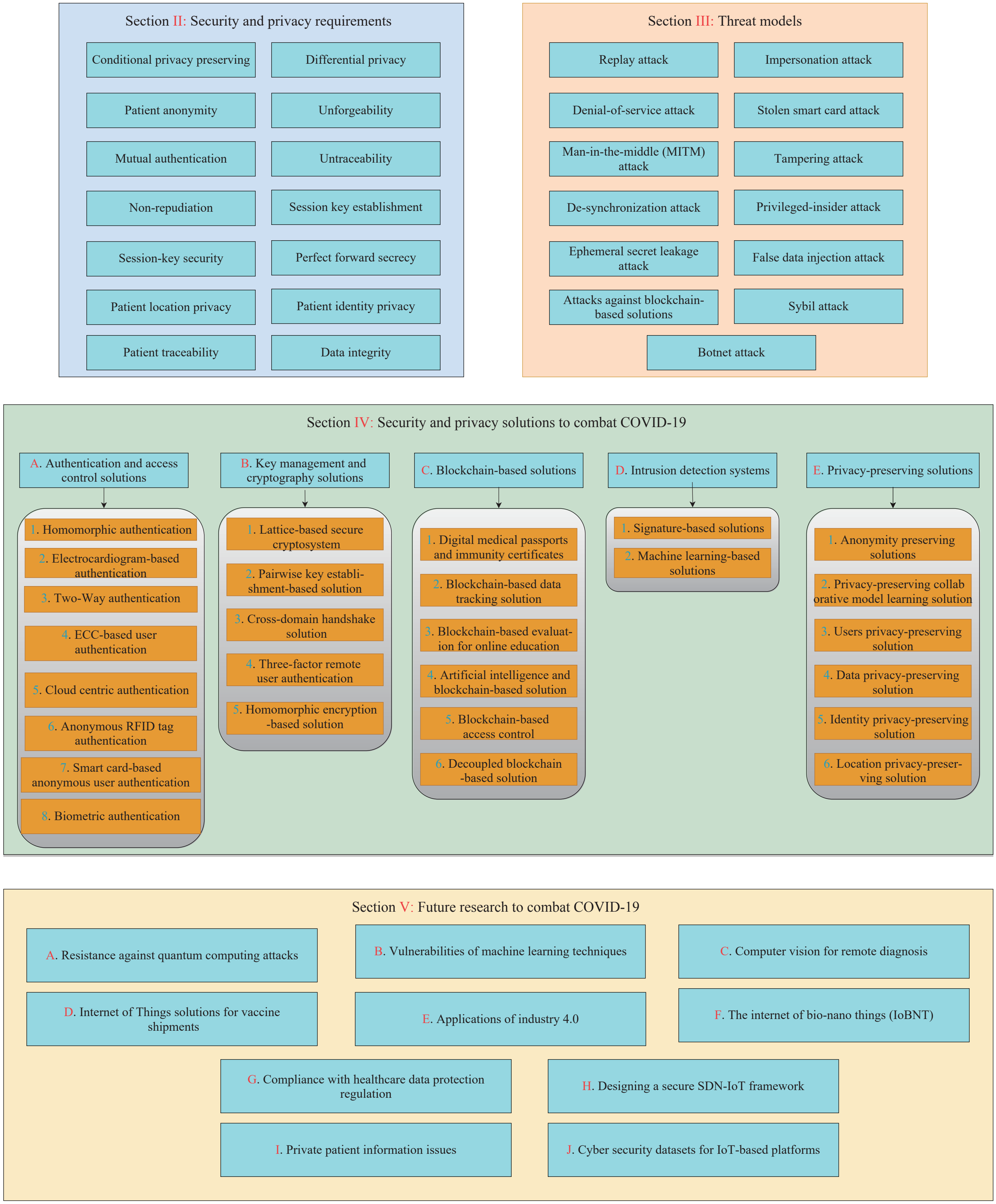

Section II: Security and privacy requirements
Conditional privacy preserving
Differential privacy
Patient anonymity
Unforgeability
Mutual authentication
Untraceability
Non-repudiation
Session key establishment
Session-key security
Perfect forward secrecy
Patient location privacy
Patient identity privacy
Patient traceability
Data integrity
Section III: Threat models
Replay attack
Impersonation attack
Denial-of-service attack
Stolen smart card attack
Man-in-the-middle (MITM) attack
Tampering attack
De-synchronization attack
Privileged-insider attack
Ephemeral secret leakage attack
False data injection attack
Attacks against blockchain-based solutions
Sybil attack
Botnet attack
Section IV: Security and privacy solutions to combat COVID-19
A. Authentication and access control solutions
B. Key management and cryptography solutions
C. Blockchain-based solutions
D. Intrusion detection systems
E. Privacy-preserving solutions
1. Homomorphic authentication
2. Electrocardiogram-based authentication
3. Two-Way authentication
4. ECC-based user authentication
5. Cloud centric authentication
6. Anonymous RFID tag authentication
7. Smart card-based anonymous user authentication
8. Biometric authentication
1. Lattice-based secure cryptosystem
2. Pairwise key establi-shment-based solution
3. Cross-domain handshake solution
4. Three-factor remote user authentication
5. Homomorphic encryption -based solution
1. Digital medical passports and immunity certificates
2. Blockchain-based data tracking solution
3. Blockchain-based evaluat-ion for online education
4. Artificial intelligence and blockchain-based solution
5. Blockchain-based access control
6. Decoupled blockchain -based solution
1. Signature-based solutions
2. Machine learning-based solutions
1. Anonymity preserving solutions
2. Privacy-preserving collab orative model learning solution
3. Users privacy-preserving solution
4. Data privacy-preserving solution
5. Identity privacy-preserving solution
6. Location privacy-preser-ving solution
Section V: Future research to combat COVID-19
A. Resistance against quantum computing attacks
B. Vulnerabilities of machine learning techniques
C. Computer vision for remote diagnosis
D. Internet of Things solutions for vaccine shipments
E. Applications of industry 4.0
F. The internet of bio-nano things (IoBNT)
G. Compliance with healthcare data protection regulation
H. Designing a secure SDN-IoT framework
I. Private patient information issues
J. Cyber security datasets for IoT-based platforms

Fig. 3. Organization of this paper.

III. Threat Models

Since the COVID-19 sensitive patient information will be transmitted through an open channel (i.e., the Internet), the potential for misuse of this information can happen. Hence, we propose the following threat models against epidemic situation applications like COVID-19. Specifically, we consider the widely accepted Dolev-Yao (DY) threat model [42] according to which two parties are allowed to interact through a public (unsecured) network. In the DY model, an adversary A launches the following attacks to interrupt the data that are exchanged between parties but can also alter or eliminate the content of the data and can insert false data during the communication. Fig. 4 classifies the prevalent threats in the IoT-based healthcare systems on the basis of the layer it affects.

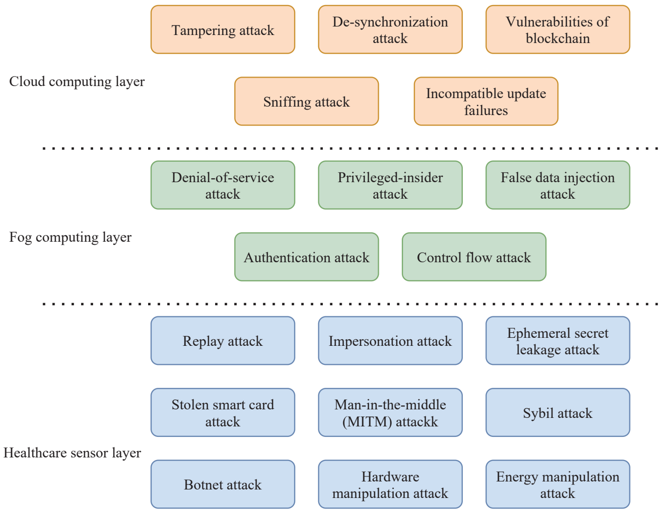

Tampering attack
De-synchronization attack
Vulnerabilities of blockchain
Cloud computing layer
Sniffing attack
Incompatible update failures
Denial-of-service attack
Privileged-insider attack
False data injection attack
Fog computing layer
Authentication attack
Control flow attack
Replay attack
Impersonation attack
Ephemeral secret leakage attack
Stolen smart card attack
Man-in-the-middle (MITM) attackk
Sybil attack
Healthcare sensor layer
Botnet attack
Hardware manipulation attack
Energy manipulation attack

Fig. 4. Classification of security threats in IoT-based healthcare systems to fight against epidemic situations like COVID-19.

1) Replay Attack: To provide replay attacking resistance in epidemic situations, Tan *et al.* [43] designed a practical homomorphic authentication framework, which is based on the fresh timestamps used in each calculation. Usually, the use of timestamps can resist against replay attack.

2) Impersonation Attack: An adversary assumes the identity of one of the legitimate entities in a communication protocol or a system. Alladi *et al.* [44] proposed an authentication framework for providing two-way authentication based on physical unclonable functions, which can resist impersonation attacks.

3) Denial-of-Service Attack: This attack aims to make an epidemic situation application unable to respond to the requests of its users. Challa *et al.* [45] proposed an authentication framework based on ECC cryptography and three-factor, which can resist the denial-of-service attacks.

4) Stolen Smart Card Attack: This implies that if an adversary takes the smart card of a user of an epidemic situation application, he may have the opportunity to impersonate this user identity or to initiate a new attack. Usually, the use of cryptography methods (e.g., Elliptic Curve Cryptography) can resist against stolen smart card attack.

5) Man-in-the-Middle (MITM) Attack: It is an attack that uses at least three devices. Two devices use an epidemic situation application and communicate with each other. The third (i.e., an adversary) in the middle breaks the link between the two devices and masquerades as the other device. In other words, it intercepts and redirects the communications, and can also modify the exchanged data. Srinivas *et al.* [46] designed a cloud-based user authentication framework for enhanced medical data authentication, which can resist to the MITM attack since the random nonces and timestamps are used in encrypted data.

6) Tampering Attack: It is a form of web-based attack where some parameters in the epidemic situation application or web page form field data that are submitted by a user are altered without that user's authorization.

7) De-Synchronization Attack: This type of attack means that the private data exchanged between a specific tag and the main server can be desynchronized using a number of attack techniques.

8) Privileged-Insider Attack: This attack means that any person with special access (e.g., login information) to critical systems, servers and databases in epidemic situation applications can be viewed as an internal threat, as everyone's access is a vulnerable point.

9) False Data Injection Attack: These attacks are designed to compromising the readings of several medical sensors and healthcare data with the objective of misleading control and operations.

10) Ephemeral Secret Leakage Attack: When ephemeral secrets are compromised, an adversary is able to divulge patients' private keys, and the session key will be revealed from the listened messages.

11) Attacks Against Blockchain-Based Solutions: These attacks are designed to create the vulnerabilities of the blockchain systems such as 51% vulnerability, selfish and reputation-based behaviors, private key leakage, double spending, and transaction privacy leakage. For more information about the threat models against blockchain systems, we refer the reader to the work [47].

12) Sybil Attack: With this attack, an adversary generates a number of additional node identities based on a single physical device in order to acts in the same way as if it were a larger number of nodes.

13) Botnet Attack: Botnets are malware-controlled and infected networks of electronic devices used to carry out DDoS or other types of cyber attacks.

IV. Security and Privacy Solutions

According to the security and privacy models, we classify the security and privacy solutions to combat COVID-19 into five categories, namely, 1) Authentication and access control solutions, 2) Key management and cryptography solutions, 3) Blockchain-based solutions, 4) Intrusion detection systems, and 5) Privacy-preserving solutions. The summary of potential solutions for security and privacy to combat epidemic situations like COVID-19 is presented in both Tables III and IV. The opportunities for these security and privacy solutions are presented in Fig. 5.

A. Authentication and Access Control Solutions

According to authentication models, we classify the authentication and access control solutions to combat COVID-19 into nine categories, namely, 1) Homomorphic authentication, 2) Electrocardiogram-based authentication, 3) Two-Way authentication, 4) ECC-based user authentication, 5) Fine-grained data access control, 6) Cloud-centric

TABLE III
SUMMARY OF POTENTIAL SOLUTIONS FOR SECURITY AND PRIVACY IN EPIDEMIC SITUATIONS LIKE COVID-19 (PART 1)

Solution	Year	Network model	Solution type	Methods	Pros (+)	Cons (-)	Motivation and design goals for epidemic situations
Hasan *et al.* [48]	2020	COVID-19 epidemic situation	Blockchain-based solutions	- Proxy re-encryption framework - Blockchain technology - Self-sovereign identity	+ Provide confidentiality and privacy	- The resistance against attacks in not provided	Monitoring and tracing of COVID-19 test-takers using blockchain technology
Marbouh *et al.* [20]	2020	COVID-19 epidemic situation	Blockchain-based solutions	Decentralized Ethereum network - Blockchain technology	+ Provides authenticity and transparency	- The differential privacy is not considered	Evaluation of COVID-19 data collected from a diversity of sources using blockchain technology
Shukla *et al.* [49]	2020	COVID-19 epidemic situation	Blockchain-based solutions	- Blockchain technology	+ Provide data privacy among the system's stakeholders	The latency of consensus algorithm under attacks is not analyzed	Provide data privacy and transparency in the online education system during COVID-19 epidemic situation
Tan *et al.* [43]	2020	Cloud-assisted vehicle ad-hoc networks	Authentication and access control solutions	- One-way hash function - Elliptic curve cryptosystem - Homomorphic Encryption	+ Improving healthcare surveillance and infection monitoring	- The physical security is not considered	Use the integrated cloud-based VANET infrastructure for automated tracking of infections for pandemic
Alladi *et al.* [44]	2020	Healthcare IoT networks	Authentication and access control solutions	- Physical Unclonable Functions	+ Ensure session key uniqueness and resist against node tampering attack	- The differential privacy is not considered	Providing two-way authentication between various entities in epidemic situation applications
Huang *et al.* [50]	2019	IoT-based healthcare	Authentication and access control solutions	- The Laplace mechanism	+ Provide the differential privacy and resist attacks against electrocardiogram biometrics	- The anonymous RFID tag authentication is not considered	Authenticate patients based on noisy electrocardiogram data
Zhang *et al.* [51]	2018	Smart healthcare systems	Authentication and access control solutions	- Parallel electrocardiogram	+ Provide comfortability, accessibility, and inimitability	- The resistance against attacks is not provided	The electrocardiogram can be used as tool for authenticate the terminals of epidemic situation applications
Challa *et al.* [45]	2018	Wireless healthcare sensor networks	Authentication and access control solutions	- One-way hash function - Elliptic curve cryptography - Bilinear pairing	+ Guarantee user anonymity and mutual authentication	- The untraceability is not achieved	Authenticate entities based on ECC cryptography and three-factor
Roy *et al.* [52]	2018	Healthcare applications using mobile cloud computing	Authentication and access control solutions	- Attribute-based encryption - Hash function	+ Provides untraceability and user anonymity	- The anonymous RFID tag authentication is not considered	Realize fine-grained data access control for epidemic situation applications
Srinivas *et al.* [46]	2018	Cloud centric authentication for wearable healthcare monitoring system	Authentication and access control solutions	- 160-bit secret key Hash function such as SHA-256	+ Providing medical data authentication using cloud-based user authentication framework	- The anonymous RFID tag authentication is not considered	Authenticate the terminals of epidemic situation applications with an accessible wearable sensor node
Wu *et al.* [53]	2018	e-healthcare applications	Authentication and access control solutions	- Secret key - Pseudo-identity - Hash functions	+ Provide forward and backward untraceability	- The differential privacy is not considered	Authenticate the terminals of epidemic situation applications with an anonymous RFID tag authentication framework
Chaudhary *et al.* [54]	2018	Smart healthcare systems	Key management and cryptography solutions	- Lattice-based cryptosystem - Hash functions	+ Low computation and communication costs	- Resistance to network attacks are not provided	Provide secure data transmission with a lightweight key exchange
Das *et al.* [55]	2017	Wireless medical sensor networks	Authentication and access control solutions	- Hash functions - Symmetric-key encryption/decryption - Public-key elliptic curve cryptosystem	+ Resistance against identity and password guessing attack, stolen verifier attack, and privileged-insider attack	- Location privacy is not protected	Authenticate the terminals of epidemic situation applications using smart card-based anonymous user authentication
Zhang *et al.* [56]	2017	E-health Systems	Authentication and access control solutions	- Biometric authentication	+ User anonymity is fully preserved	- Non-repudiation is not achieved	Protects patient's identity privacy in epidemic situation applications
Wazid *et al.* [57]	2017	Implantable medical devices	Key management and cryptography solutions	- Elliptic curve cryptography - Hash functions	- Provide session key security and preserves both anonymity and untraceability properties	- Location privacy is not protected	Authenticate the terminals of epidemic situation applications using a lightweight three-factor remote user authentication framework

Table III (Continued)

Solution	Year	Network model	Solution type	Methods	Pros (+)	Cons (-)	Motivation and design goals for epidemic situations
He *et al.* [41]	2016	m-healthcare social networks	Key management and cryptography solutions	- Hierarchical identity-based cryptography - Elliptic curve cryptosystem - Hash functions	+ Provides patient anonymity as well as patient traceability	- Vulnerable to password guessing attack	Secure communication in epidemic situation applications using handshake solution
Zhou *et al.* [58]	2015	Cloud-assisted e-healthcare systems	Key management and cryptography solutions	- Homomorphic encryption - Hash functions	+ Provide privacy-preserving	- Vulnerable to privileged-insider attack	Provide the privacy-preserving using homomorphic data aggregation
Zhou *et al.* [59]	2015	m-healthcare social networks	Key management and cryptography solutions	- Pairwise key establishment - Hash functions	+ Provide both identity and location privacy	- Non-repudiation is not achieved	Protects patient's identity privacy in epidemic situation applications

TABLE IV
SUMMARY OF POTENTIAL SOLUTIONS FOR SECURITY AND PRIVACY IN EPIDEMIC SITUATIONS LIKE COVID-19 (PART 2)

Solution	Year	Network model	Solution type	Methods	Pros (+)	Cons (–)	Motivation and design goals for epidemic situations
Masud *et al.* [60]	2020	Internet of Medical Things in COVID-19 Patients Care	Key management and cryptography solutions	- Bit-wise XOR operations - Physical unclonable functions - Nonce and one-way hash function	+ Resistance to cloning, tampering and side-channel attacks	- The intrusion detection is not considered	Secure communication from adversarial threats through secure sessions.
Wazid *et al.* [61]	2020	Internet of Things (IoT) UAV-assisted healthcare service	Blockchain-based solutions	- Elliptic curve digital signature algorithm - Hash functions	+ Resistance against privileged-insider attacks, impersonation attacks, man-in-the-middle attacks, and replay attacks	- Non-repudiation is not considered	Secure communication in medicine delivery services during pandemic of COVID-19
Saha *et al.* [62]	2020	IoT-enabled healthcare systems	Blockchain-based solutions	- Elliptic curve digital signature algorithm - Hash functions Blockchain technology	+ Resistance against impersonation attacks, replay attacks, and ephemeral secret leakage attacks	- Location privacy is not acheived	Authenticate patients (COVID-19) with a hospital's trusted authority
Aujla *et al.* [63]	2020	Edge and IoT-enabled healthcare systems	Blockchain-based solutions	Lightweight Blockchain mechanism - Hash functions	+ Reduce the preparation time of blocks and generation of headers	- Vulnerable to crypto-mining attacks	Enables the transmission of internal healthcare surveillance data to the cloud by leveraging edge nodes
Thami *et al.* [64]	2020	Internet of Medical Things	Intrusion detection systems	- Machine learning algorithms	+ Achieve high detection accuracy	- The privacy preserving is not considered	Identify anomalies in the sensor data as well as intrusions at the network level
Yu *et al.* [65]	2020	Medical research support platform	Privacy-preserving solutions	- Pseudonym mechanism of blockchain technology	+ Protecting the copyright of research results	- The intrusion detection is not considered	Enables efficient sharing of information while maintaining privacy against COVID-19
Garg *et al.* [7]	2020	IoT-based COVID-19	Privacy-preserving solutions	- Blockchain technology	+ Assist the public in protecting their privacy through voluntary cooperation in tracking contacts	- The intrusion detection is not considered	Enables moving devices to be able to send or receive alerts when they are in close proximity to a reported, suspected or confirmed case of disease
Kumar *et al.* [66]	2020	Internet of medical things environment	Intrusion detection systems	- Random Forest - Naive Bayes - Decision Tree	+ The proposed system achieves an accuracy of 96.35 %	- The privacy-preserving is not considered	Deploy an IDS in the cloud side (i.e., Infrastructure as a Service) and in the fog nodes (i.e., Software as a Service)
Li *et al.* [67]	2019	IoT environments for smart healthcare	Intrusion detection systems	Signature-based framework - Blockchain technology	+ Guarantee detection efficiency by only applying verified and reliable signatures	- The privacy-preserving is not considered	Ensure that signatures are shared securely against malicious nodes in IoT applications against COVID-19
He *et al.* [68]	2019	Connected healthcare systems	Intrusion detection systems	- Stacked autoencoder	+ Reduces the size of the attributes with an accuracy of 97.83 %	- Roc curve is not calculated	Identify and detect attacks in connected healthcare systems

Table IV (Continued)

Solution	Year	Network model	Solution type	Methods	Pros (+)	Cons (–)	Motivation and design goals for epidemic situations
Wang *et al.* [69]	2019	Medical online diagnostic service	Privacy-preserving solutions	- Multi-party vector comparison algorithm - Distributed skyline computation - Paillier cryptosystem	+ Achieve the confidentiality of the diagnosis model	- Non-repudiation is not achieved	Ensures that any local diagnostic models are encoded by the local community before they are delivered to the cloud
Wang *et al.* [70]	2019	mobile eHealthcare	Privacy-preserving solutions	- Single-attribute encryption technique - SHA-256 hash function	+ Achieve privacy-preservation requirements	- The resistance to attacks is not provided	Access the disease risk prediction and hospital recommendation services provided by the health service provider
Zheng *et al.* [71]	2019	Outsourced eHealthcare data	Privacy-preserving solutions	- Homomorphic encryption method	+ Perform a k-NN computation on data encrypted with a computing complexity $O(lklogN)$	- The data integrity is not achieved	The encrypted data is efficiently stored in the cloud
Yang *et al.* [72]	2018	E-healthcare systems	Privacy-preserving solutions	- Bloom filter technique - Homomorphic cryptographic algorithm - Keyed-cryptographic hash function	+ Reduce the communication overhead and encryption times	- The intrusion detection is not considered	Achieves the privacy requirements of medical users
Zhang *et al.* [73]	2018	Cloud-based e-Healthcare system	Privacy-preserving solutions	- Single-layer perceptron learning algorithm	+ Minimize privacy disclosure	- The integrity is not achieved	Maintain identity privacy using prediction models
Zhu *et al.* [74]	2016	Online medical prediagnosis	Privacy-preserving solutions	- Polynomial aggregation and lightweight multi-party random masking techniques - Nonlinear kernel support vector machine	+ Protecting users' medical information	- Resistance to network attacks are not provided	Maintaining the diagnosis model secret from users
Liu *et al.* [75]	2015	Clinical decision support system	Privacy-preserving solutions	- Additive homomorphic proxy aggregation technique - Naive bayes classifier	+ Achieve privacy-preserving requirements	- The intrusion detection is not considered	Ensure the protection of the privacy of historical data (e.g., location privacy)

authentication, 7) Anonymous RFID tag authentication, 8) Smart card-based anonymous user authentication, and 9) Biometric authentication.

1) Homomorphic Authentication: Based on the new intelligent transportation system (ITS)'s emerging advantages, Vehicle ad-hoc networks (VANETs) can capture and processing valuable vehicle data to enhance the driving environment and road safety. Tan *et al.* [43] addressed improving healthcare surveillance and infection monitoring for high-mobility transportation systems, which is not achievable for pandemic control. The automated tracking of infections for pandemic control can be performed consequently. Specifically, the authors designed a practical homomorphic authentication framework for cloud-assisted VANETs, where healthcare surveillance for any involved passengers is delivered. The proposed framework includes the use of the integrated cloud-based VANET infrastructure, where the medical data collection module is connected to the hybrid medical data acquisition module. To provide the infection monitoring on a specific vehicle and person, the mechanism of decentralized vehicle registration based on the blockchain is implemented cooperatively between vehicular cloud and edge units.

2) Electrocardiogram-Based Authentication: The electrocardiogram can be used as tool for authenticate the telemedical terminals of epidemic situation applications. Zhang *et al.* [51] proposed an authentication framework based on the parallel electrocardiogram, named PEA, which can be applied for epidemic situation applications. The PEA framework provides a method of hybrid electrocardiogram feature extraction which includes features based on fiducial- and non-fiducial for extracting enhanced electrocardiogram features to improve the stability of the authentication. Huang *et al.* [50] introduced an authentication framework that can authenticate patients based on noisy electrocardiogram data and guarantee the privacy of the patterns stored in the system. The proposed framework can be adopted for epidemic situation applications like COVID-19 which is able to track movements and adjust the algorithm depending on the current state of the movement.

3) Two-Way Authentication: With the new use of IoT in health care, a large number of data on patients of COVID-19 are communicated and provided online. Alladi *et al.* [44] proposed an authentication framework, named HARCI, for providing two-way authentication, which can be applied between various entities in epidemic situation applications.

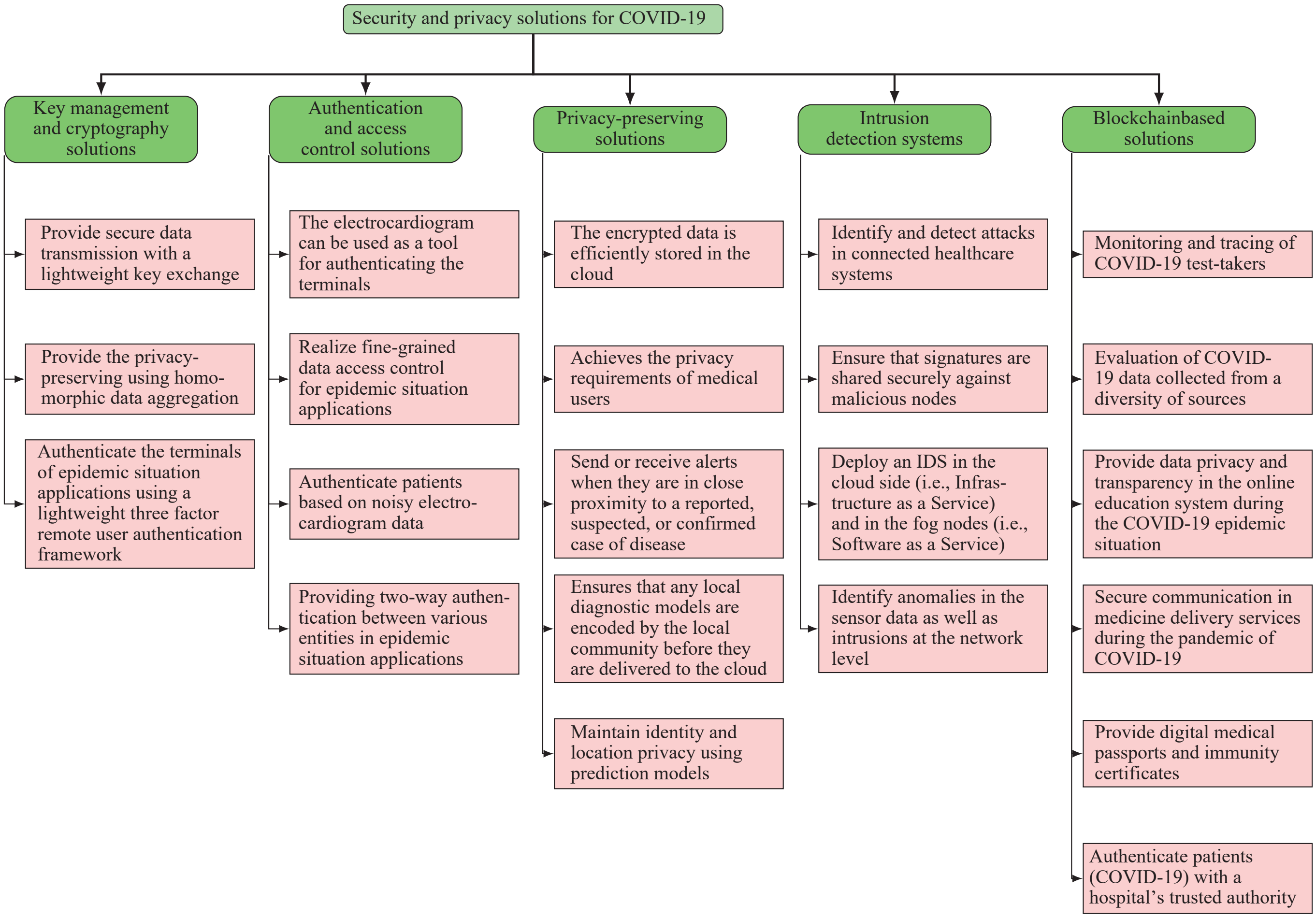

Security and privacy solutions for COVID-19
Key management and cryptography solutions
Provide secure data transmission with a lightweight key exchange
Provide the privacy-preserving using homomorphic data aggregation
Authenticate the terminals of epidemic situation applications using a lightweight three factor remote user authentication framework
Authentication and access control solutions
The electrocardiogram can be used as a tool for authenticating the terminals
Realize fine-grained data access control for epidemic situation applications
Authenticate patients based on noisy electrocardiogram data
Providing two-way authentication between various entities in epidemic situation applications
Privacy-preserving solutions
The encrypted data is efficiently stored in the cloud
Achieves the privacy requirements of medical users
Send or receive alerts when they are in close proximity to a reported, suspected, or confirmed case of disease
Ensures that any local diagnostic models are encoded by the local community before they are delivered to the cloud
Maintain identity and location privacy using prediction models
Intrusion detection systems
Identify and detect attacks in connected healthcare systems
Ensure that signatures are shared securely against malicious nodes
Deploy an IDS in the cloud side (i.e., Infrastructure as a Service) and in the fog nodes (i.e., Software as a Service)
Identify anomalies in the sensor data as well as intrusions at the network level
Blockchainbased solutions
Monitoring and tracing of COVID-19 test-takers
Evaluation of COVID-19 data collected from a diversity of sources
Provide data privacy and transparency in the online education system during the COVID-19 epidemic situation
Secure communication in medicine delivery services during the pandemic of COVID-19
Provide digital medical passports and immunity certificates
Authenticate patients (COVID-19) with a hospital's trusted authority

Fig. 5. Opportunities for security and privacy solutions to fight against epidemic situations like COVID-19.

The HARCI framework uses IoT devices with limited resources and architecture of three layers, including, healthcare cloud server, sink nodes, and patient nodes. Therefore, the HARCI framework can offer end-to-end authenticity by providing a single session key for each step of the authentication process. Based on a formal security proof called the Mao-Boyd logic, the HARCI framework is proven that it can ensure session key uniqueness and resist against node tampering attack, reply attack, man-in-the-middle (MITM) attack, and impersonation attack.

4) ECC-Based User Authentication: The elliptic curve cryptography (ECC) is used by security protocols for providing authentication. Challa *et al.* [45] proposed an authentication framework based on ECC cryptography and three factors for wireless healthcare sensor networks, which can be applied for epidemic situation applications. Through formal security analysis techniques (e.g., BAN logic, AVISPA tool, and real-or-random (ROR) model), the proposed framework is proven to be secure against replay attack, denial-of-service attack, stolen smart card attack, offline password guessing attack, impersonation attack, privileged-insider attack. In addition, the proposed framework guarantees user anonymity and mutual authentication.

5) Fine-Grained Data Access Control: In smart healthcare where an epidemic situation application is used, some attributes of the server database information may be accessible only to privileged users. Roy *et al.* [52] proposed a security framework that combines fine-grained access control and mutual authentication for healthcare applications using mobile cloud computing, which can be applied for epidemic situation applications like COVID-19. Based on the attribute-based encryption techniques and hash functions, the proposed framework can provide untraceability and user anonymity.

6) Cloud Centric Authentication: Security and privacy are key issues in cloud computing-based epidemic situation applications, where people are restricted in their access to data stored at remote sites operated by various providers. Srinivas *et al.* [46] designed a cloud-based user authentication framework for enhanced medical data authentication, which can be applied for epidemic situation applications like COVID-19. Based on mutual successful authentication performed by a patient and a handheld sensor node, both parties create a secret session key which is then applied for secure communications in the future. Based on the ROR model and AVISPA tool, the proposed framework is proven secure against wearable sensor node capture attack as well as password change attack.

7) Anonymous RFID Tag Authentication: The epidemic situation applications like COVID-19 use the low-cost radio frequency identification (RFID) tag to communicate with the servers and access points. Wu *et al.* [53] designed an anonymous RFID tag authentication framework for e-healthcare systems, which can be applied for epidemic situation applications. The proposed framework employs three techniques, namely, the secret key, the pseudo-identity, and the hash functions, which can provide anonymity for both the tag and the reader. Based on the game theory model, the proposed framework can provide forward and backward untraceability as well as can resist data forgery attacks and de-synchronization attacks.

8) Smart Card-Based Anonymous User Authentication: A wireless medical sensor network is a network of sensors composed of lightweight devices with limited resources, limited memory, low computational performance, and low energy battery power. The healthcare sensor devices (e.g., ECG monitoring electrodes, heart rate monitors, oxygen, temperature, and blood pressure sensors) are placed on a user' s body, forming a wireless body network. Das *et al.* [55] designed a smart card-based anonymous user authentication framework for wireless body networks, which can be applied to counter epidemic situations like COVID-19. Based on the BAN Logic and AVISPA tool, the proposed framework is proven that can provides user anonymity as well as resistance against the following five attacks: replay attack, identity and password guessing attack, stolen verifier attack, and privileged-insider attack.

9) Biometric Authentication: Biometric authentication is a security concept that is based on an individual‘s unique biological characteristics to ensure that they are exactly who the individuals say they are. Biometric authentication technologies are based on the comparison of a biometric data capture with authentic data stored and validated in a database. Zhang *et al.* [56] proposed an authenticated key agreement system, which can address the security and computational requirements of eHealth applications. In the proposed system, the medical server is in charge of controlling the validity of the user. To protect the server from the possibility of identifying the biometric template, a random string is associated with it using the gold-exclusive operation. In addition, these hidden strings are protected by hash or biohach functions throughout the authentication and key negotiation procedures. This enables the medical server to check the biometric features in epidemic situations like COVID-19 directly without storing and retrieving the exact values. Biometric templates in storage devices such as smart cards and databases are protected by random numbers, ensuring that only the user has the actual value.

B. Key Management and Cryptography Solutions

According to key management models, we classify the key management and cryptography solutions to combat COVID-19 into five categories, namely, 1) Lattice-based secure cryptosystem; 2) Pairwise key establishment-based solution; 3) Cross-domain handshake solution; 4) Three-factor remote user authentication; and 5) Homomorphic encryption-based solution.

1) Lattice-Based Secure Cryptosystem: To securely processing COVID-19 data, it very important to use key management and cryptography solutions for providing security and privacy. Chaudhary *et al.* [54] designed a security protocol that is based on the lattice, named LSCSH, providing security of smart healthcare, which can be applied to counter epidemic situations. The security key used by the proposed LSCSH protocol is computed using lattice-based vector equations. The LSCSH protocol enables the validation of demands from cloud storage to various end-users including doctors and patients. In addition, the LSCSH protocol can resist to quantum attacks since breaking the security of Lattice vectors is equal to trying to solve NP-difficult problems.

2) Pairwise Key Establishment-Based Solution: The idea of the pairwise key establishment is adopted by Zhou *et al.* [59] for designing a privacy-preserving key management framework, named 4S, in the m-healthcare social network, which can be applied to counter epidemic situations. Based on the collaboration of patients affected by similar pathologies in the same community, the proposed framework can withstand both time-based and location-based mobile attacks. Due to the symmetrical structure of the body, sensors for body monitoring such as electrocardiogram and electroencephalography are usually placed on patients symmetrically to track their vital symptoms. By extending the proactive secret-sharing approach, the proposed framework is proven that can provide both identity and location privacy.

3) Cross-Domain Handshake Solution: The handshake solution is an example of an effective cryptography method, that can enable secure communication in epidemic situation applications like COVID-19. Based on hierarchical identity-based cryptography, He *et al.* [41] designed a cross-domain handshake solution, named CDHS, for secure communication in mobile healthcare social networks. For securing epidemic situation applications, two patients who are registered at various health institutions can obtain mutual authentication and then create a session key, where the elliptic curve cryptography is applied. In addition, using the random oracle model, the CDHS solution was proven secure assuming the intractability of the inversion computational diffie-Hellman (ICDH) problem. Therefore, to provide anonymity in internet of medical things with COVID-19 patients care, Masud *et al.* [60] designed a secure key establishment scheme. The proposed scheme uses some cryhptographics methods, including, Bit-wise XOR operations, physical unclonable functions, nonce, and one-way hash function. Based on these lightweight cryptography primitives, the proposed scheme is proven that can secure communication from adversarial threats through secure sessions as well as providing resistance to cloning, tampering and side-channel attacks.

4) Three-Factor Remote User Authentication: Implantable medical devices (IMDs) are artificial devices that can be placed in the patient's body to enhance the operation of different parts of the body. IMDs are used to control and process the human physiological status (e.g., blood glucose monitoring by insulin pumps). In this type of communications infrastructure, however, security and privacy issues such as health data leakage and IMD malfunction through unauthorized access are always present. Wazid *et al.* [57] designed a lightweight three-factor remote user authentication framework for secure IMDs, which can be applied for epidemic situation applications like COVID-19. Based on the

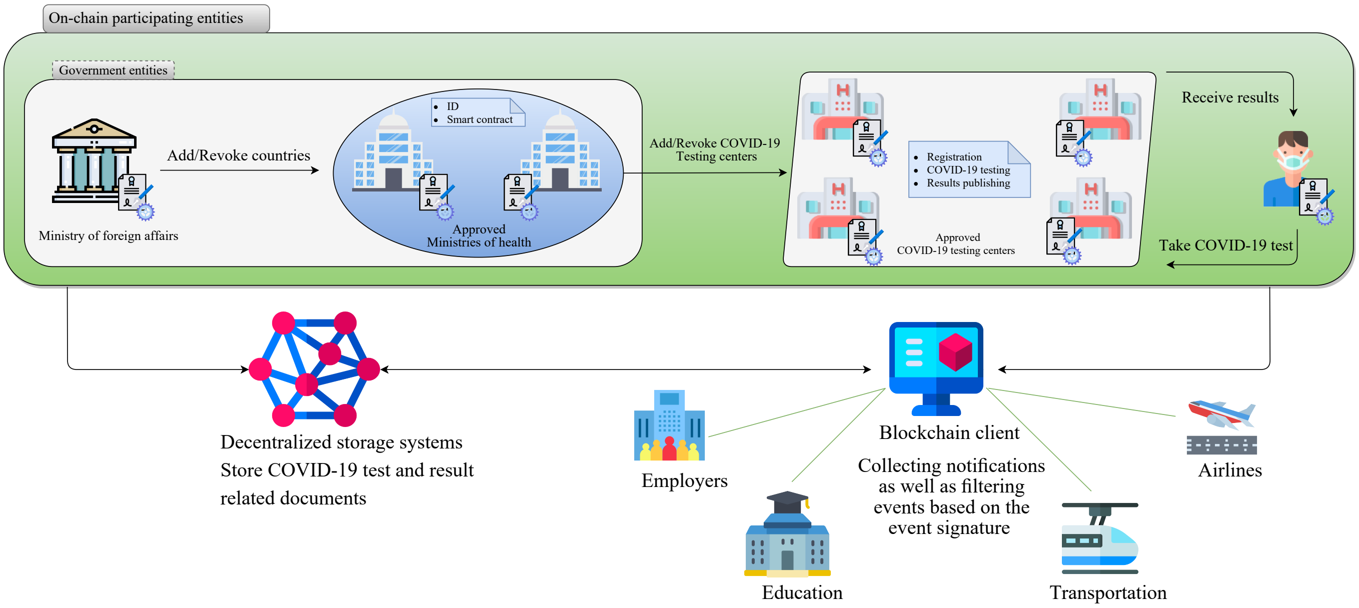


Fig. 6. Blockchain-based solution for security and privacy to counter epidemic situations like COVID-19.

security verification tool, the proposed framework can provide protection against some attacks, namely, replay attack, controller node impersonation attack, user impersonation attack, and privileged-insider and offline password guessing attack. In addition, the proposed framework can provide session key security and preserve both anonymity and untraceability properties.

5) Homomorphic Encryption-Based Solution: E-health systems are enabling the monitoring of health conditions like COVID-19, facilitating disease models and rapid intervention, as well as providing evidence-based medical intervention through medical text mining and the extraction of image characteristics. Zhou *et al.* [58] designed a privacy-preserving fully holomorphic data aggregation framework, named PPDM, for securing data exchanged between parties. Based on the formal security proof, the PPDM framework can achieve a higher security level of privacy preservation.

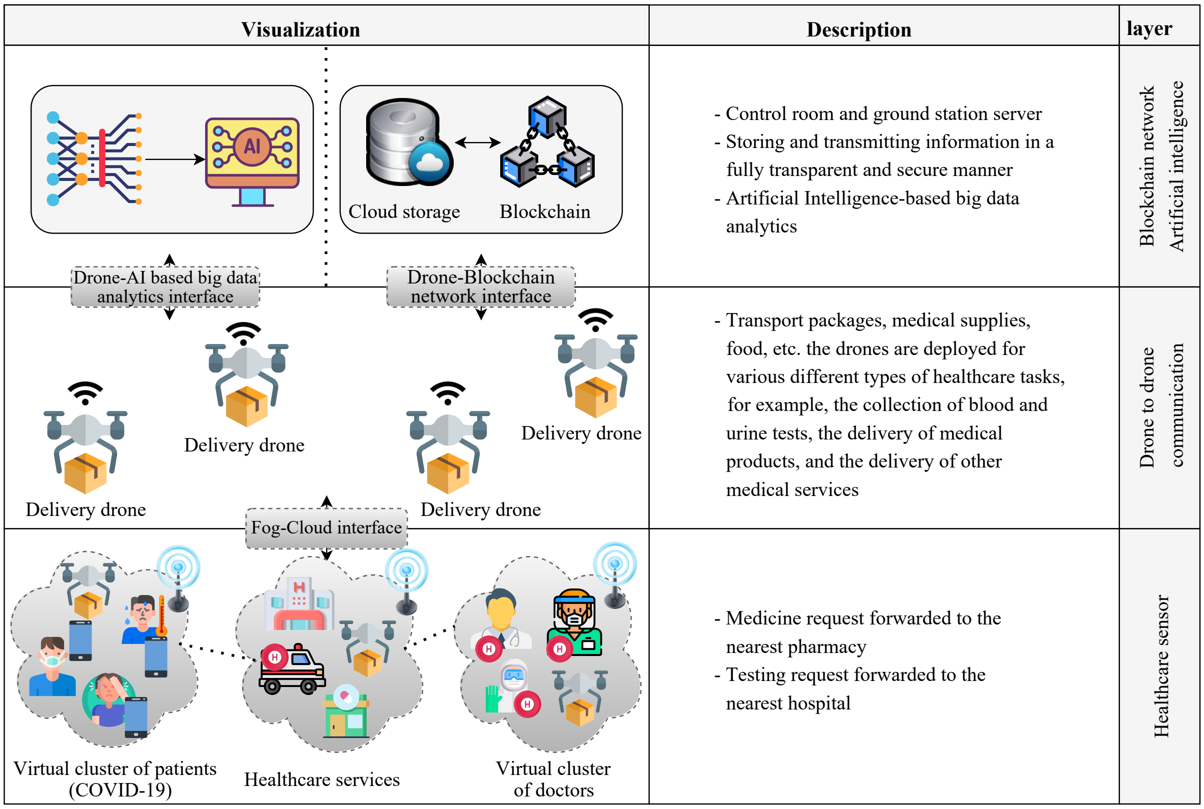
C. Blockchain-Based Solutions

The blockchain technology [76] is identified by the European parliament's research service (EPRS) as one of the ten key enabling strategies to combat COVID-19, as discussed by Kalla *et al.* [32], where blockchain-based systems can be used for 1) tracking of contacts, 2) emergency assistance and insurance, 3) sharing patient data, 4) automated monitoring and contactless delivery, etc. According to the case used, we classify the blockchain-based solutions to combat COVID-19 into six categories, namely, 1) Digital medical passports and immunity certificates, 2) Blockchain-based data tracking solution, 3) Blockchain-based evaluation for online education, 4) Artificial intelligence and blockchain-based solution, 5) Blockchain-based access control, and 6) Decoupled blockchain-based solution.

1) Digital Medical Passports and Immunity Certificates: The basic idea of the blockchain data structure is based on a chained list, i.e., it is distributed between all nodes of the network where each node stores its local copy of all blocks started from the block of genesis. Hasan *et al.* [48] designed a blockchain-based solution based on proxy re-encryption for digital medical passports and immunity certificates, as presented in Fig. 6. The proposed solution employs programmable Ethereum Smart Contracts to perform function calls and produce events which inform entities involved of health data, updates on tests and other requirements. Therefore, the proposed solution helps stop the propagation of the COVID-19 virus using chained medical digital passports and immunity certificates. Because the information broadcast on the network is immutable, it can be reliable because it comes from an affiliated source. In addition, in the proposed solution, all notifications are reported by trusted authorities affiliated with high authorities such as the COVID-19 testing centers, the Ministry of Health, and the Ministry of Foreign Affairs.

2) Blockchain-Based Data Tracking Solution: To guarantee that the data collected by the public and government organizations are dependable and trusted, the implementation of a blockchain-based tracking system is essential to fight against the COVID-19 pandemic. Marbouh *et al.* [31] designed a blockchain-based tracking solution based on Ethereum smart contracts and oracles to monitor data reported on a number of new infections, mortality, and recovery rates from reliable information sources. In the proposed solution, there three smart contracts used by the blockchain system, namely, aggregator Smart contract, reputation contract, and registration contract. The aggregator smart contract consists of recovering the most recent updates and forwarding that information to front-end users. The reputation contract involves attributing a reputation rating to an oracle obtained from the assessment of web data sources that are evaluated to recover data. The registration contract contains details of web sources and stakeholders involved.

3) Blockchain-Based Evaluation for Online Education: Online education is now required internationally during the COVID-19 pandemic situations. Therefore, it is necessary to



Visualization	Description	layer
Cloud storage Blockchain Drone-AI based big data analytics interface Drone-Blockchain network interface	- Control room and ground station server - Storing and transmitting information in a fully transparent and secure manner - Artificial Intelligence-based big data analytics	Blockchain network Artificial intelligence
Delivery drone Delivery drone Delivery drone Delivery drone Fog-Cloud interface	- Transport packages, medical supplies, food, etc. the drones are deployed for various different types of healthcare tasks, for example, the collection of blood and urine tests, the delivery of medical products, and the delivery of other medical services	Drone to drone communication
Virtual cluster of patients (COVID-19) Healthcare services Virtual cluster of doctors	- Medicine request forwarded to the nearest pharmacy - Testing request forwarded to the nearest hospital	Healthcare sensor

Fig. 7. Artificial intelligence and blockchain-based solution for drone-aided healthcare services including the current pandemic of COVID-19.

improve e-learning technology for the preservation of data privacy and transparency in the education system. Shukla *et al.* [49] introduced a blockchain-based evaluation framework, named BDoTs, for securing online education during the COVID-19 pandemic situations. The BDoTs framework is based on three layers, including, instructor layer, middleware layer, and student layer. The instructor layer ensures pedagogical support by providing the required content to support learning. The middleware contains the Ethereum blockchain, while the student layer consists of the registration of students in the system. These layers develop smart contracts on blockchain technology to ensure accountability, trust between parties involved, and a secure payment system in the online education environment.

4) Artificial Intelligence and Blockchain-Based Solution: The artificial intelligence-based IoT UAV-assisted healthcare service is a dedicated framework that can be deployed for various different types of healthcare tasks, for example, the collection of blood and urine tests, the delivery of medical products, and the delivery of other medical services, such as the present COVID-19 pandemic, as presented in Fig. 7. Wazid *et al.* [61] designed a security solution using a private blockchain for securing communications in an IoT-activated UAV-assisted healthcare communication infrastructure. Based on the elliptic curve digital signature algorithm and blockchain technology, the proposed solution can resist some attacks, such as privileged-insider attacks, impersonation attacks, man-in-the-middle attacks, and replay attacks.

5) Blockchain-Based Access Control: Access control is a critical security measure required for an authorized user equipped with IoT that uses his or her intelligent wireless enabled device to authenticate with a hospital's trusted authority. Saha *et al.* [62] proposed an access control framework using private blockchain technology for secure communications for IoT-enabled healthcare systems, which can be applied to counter epidemic situations like COVID-19. Based on the elliptic curve cryptography approach, the proposed framework is proven that can provide anonymity and untraceability as well as resistance against impersonation attacks, replay attacks, ephemeral secret leakage attacks, offline guessing attacks, and man-in-the-middle attacks.

6) Decoupled Blockchain-Based Solution: The internal monitoring sensors in COVID-19 form a large IoT network which monitors and sends data to nearby equipment or computers on a permanent basis. The networking of these IoT-based sensors with various devices, however, results in security vulnerabilities that can be taken by an adversary due to the availability of data. Aujla *et al.* [63] designed a decoupled blockchain-based solution for ensuring the security and privacy of information in the internal healthcare surveillance ecosystem. The proposed solution enables the transmission of internal healthcare surveillance data to the cloud by leveraging edge nodes. The proposed network model is organized in two parts, including: i) in-home health monitoring model and ii) lightweight and decoupled blockchain architecture. The in-home health monitoring model includes three layers, namely, IoT-Healthcare layer, Edge-Blockchain layer, and Cloud layer. The findings in terms of blockchain and tensor-based metrics of evaluation demonstrate the efficiency of the proposed solution.

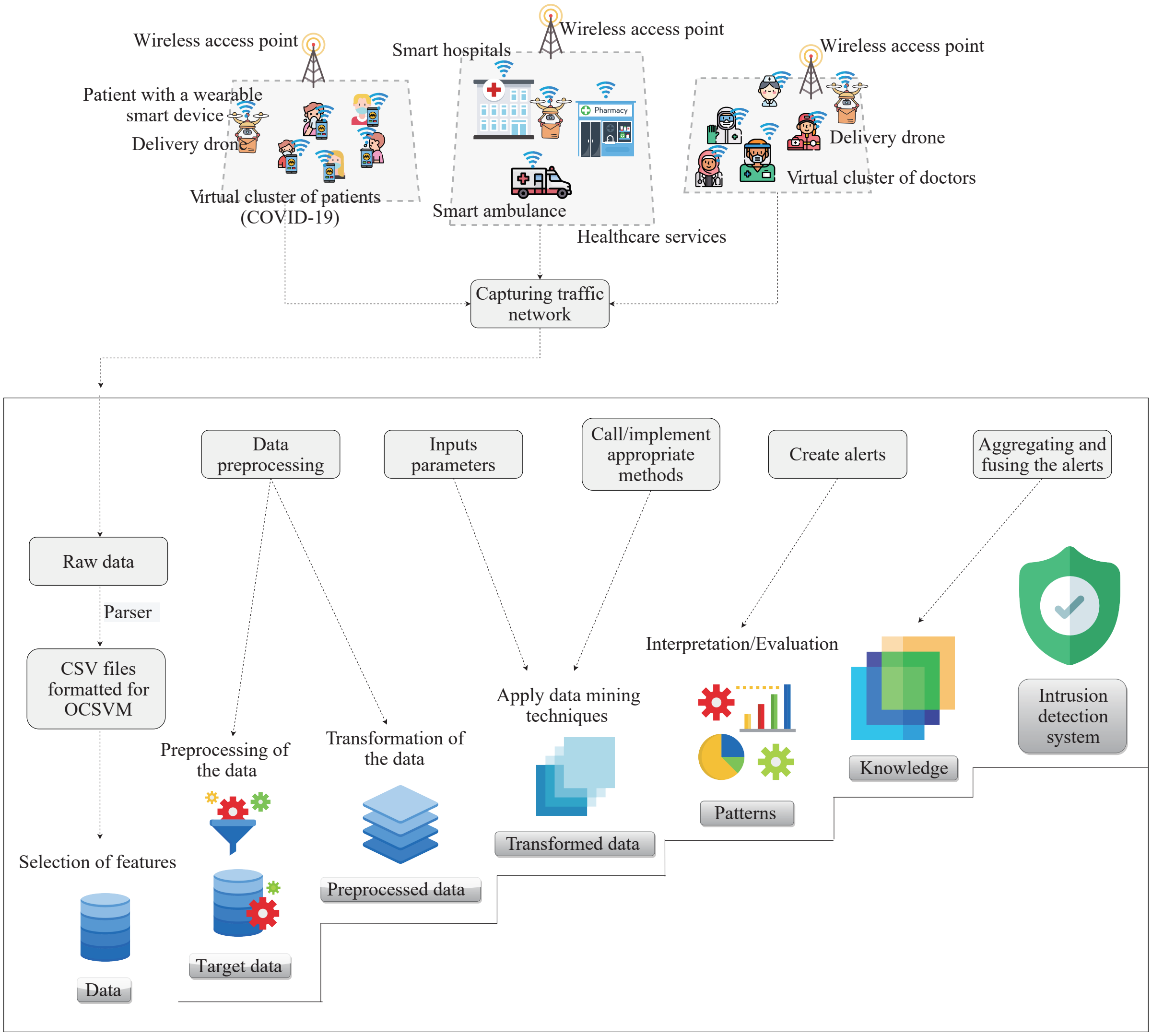

Wireless access point
Patient with a wearable smart device
Delivery drone
Virtual cluster of patients (COVID-19)
Smart hospitals
Wireless access point
Pharmacy
Smart ambulance
Healthcare services
Wireless access point
Delivery drone
Virtual cluster of doctors
Capturing traffic network
Data preprocessing
Inputs parameters
Call/implement appropriate methods
Create alerts
Aggregating and fusing the alerts
Raw data
Parser
CSV files formatted for OCSVM
Selection of features
Data
Preprocessing of the data
Target data
Transformation of the data
Preprocessed data
Apply data mining techniques
Transformed data
Interpretation/Evaluation
Patterns
Knowledge
Intrusion detection system

Fig. 8. Intrusion detection system-based solution for healthcare services including the current pandemic of COVID-19.

D. *Intrusion Detection Systems*

Intrusion detection systems (IDSs) have become one of the most important security techniques for identifying threats in smart healthcare networks. To enhance the detection capabilities of a single IDS, collaborative intrusion detection systems or networks are frequently deployed in smart hospitals, enabling a set of IDS nodes to communicate with each other by exchanging alarms, signatures, and other information such as COVID-19 alarms. The process of building an IDS-based solution for healthcare services including the current pandemic of COVID-19 is presented in Fig. 8 [77]. The first step consists of creating an environment of communications, including, IoT devices, Access Points, SDN, Cloud Computing, Edge Computing, etc. The second step consists of launching different network attacks using Kali Linux. The third step includes capturing and recording the data including the network traffic (Pcaps) and event logs (windows and Ubuntu event Logs) per machine. The fourth step consists of generating the CSV files from Pcaps files and analyzing the data (e.g., using the CICFlowMeter tool). The fifth step consists of splitting the dataset into a training dataset and a test dataset. The sixth step consists of training using machine learning approaches to build a model. The last step consists of testing using this model to identify and detect attacks on medical devices. Therefore, there are two categories of IDS solutions, namely, 1) Signature-based solutions and 2) Machine learning-based solutions.

1) Signature-Based Solutions: This technique is based on the description of suspicious behaviors through rules, called signatures. These signatures are used to describe state machines, pattern queries, or statistical analyses. The main disadvantage of this technique resides in the need to having a regularly updated rules base. Li *et al.* [67] proposed a generic blockchain-based framework, named CBSigIDS, which is a signature-based IDS. The CBSigIDS framework can ensure that signatures are shared securely against malicious nodes in IoT environments for smart healthcare. The main concept behind this is to deploy blockchain technology to build up a database of trusted signatures over time. This approach can guarantee detection efficiency by only applying verified and reliable signatures in a collaborative IoT network such as smart healthcare. Therefore, Mitchell *et al.* [78] provided and studied a rule-based approach for the specification of behavioral rules for intrusion detection of medical devices integrated into a medical cyber physical system where patient protection has high priority.

2) Machine Learning-Based Solutions: This technique is based on the use of machine learning and data mining algorithms to identify and detect attacks on medical devices including fake data injection, message alteration, and eavesdropping, which can affect patient safety, security, and reliability of critical systems such as the COVID-19 applications. To ensure the security of the connected medical device network, Thamilarasu *et al.* [64] introduced an intrusion detection system based on a mobile agent. The proposed system is hierarchy-based, self-contained, and uses self-learning and regression algorithms to identify anomalies in the sensor data as well as intrusions at the network level. There are five machine learning algorithms evaluated, including, random forests, decision trees, k-nearest neighbor, naive bayes classifier, and support vector machines, where the results show that random forests achieves the highest classification accuracy of approximately 100%. He *et al.* [68] proposed an intrusion detection system based on stacked autoencoder to identify and detect attacks in connected healthcare systems, which can be applied for healthcare critical systems such as the COVID-19 applications. The proposed system uses a stacked autoencoder to extracting the attributes, which reduces not only the size of the attributes but also the memory necessary to compute the covariance matrix. Based on the ensemble learning technique, Kumar *et al.* [66] designed an intrusion detection system for securing the internet of medical things environment that combines Cloud architecture with Fog computing. The performance evaluation on the ToN_IoT dataset shows that the proposed system achieves an accuracy of 96.35%.

E. Privacy-Preserving Solutions

According to the privacy model, we classify the privacy-preserving solutions to combat COVID-19 into six categories, namely, 1) Anonymity preserving solutions, 2) Privacy-preserving collaborative model learning solution, 3) Users privacy-preserving solution, 4) Data privacy-preserving solution, 5) Identity privacy-preserving solution, and 6) Location privacy-preserving solution.

1) Anonymity Preserving Solutions: Automating electronic contacts is one of the most cost-effective and efficient additional non-pharmaceutical strategies for reducing and controlling diseases such as Coronavirus 2019. To provide anonymity-preserving, Garg *et al.* [7] created and implemented an anonymous IoT privacy framework with an RFID proof of concept. Based on blockchain technology, the proposed model solution enables moving devices to be able to send or receive alerts when they are in close proximity to a reported, suspected or confirmed case of disease. Yu *et al.* [65] developed a blockchain-based framework to enhance the support of medical research, which can enable efficient sharing of information while maintaining privacy against COVID-19. In the first stage, both hospitals and medical research organizations are considered as nodes in the alliance chain, allowing consensus and data sharing between the nodes. Secondly, researchers, medical doctors, COVID-19 patients are required to be authenticated at different locations. In addition, medical doctors and researchers are required to be registered with the Fabric Certification Authority. To protect privacy, The COVID-19 patient uses the pseudonym mechanism of blockchain technology. The performance evaluation demonstrates that the security performance of reading and writing and security on blockchain satisfies the specifications, which can support a large application of the results of scientific research to combat COVID-19.

2) Privacy-Preserving Collaborative Model Learning Solution: To enhance the medical online diagnostic service accuracy, Wang *et al.* [69] designed a privacy-preserving collaborative model learning framework, named PCML, for secure E-Healthcare, which can be applied to combat COVID-19. With the proposed PCML framework, medical institutions can more safely train a comprehensive global diagnostic model from their cloud-based local diagnostic models, and each medical institution's critical data is fully secured using the paillier cryptosystem. Besides, the proposed PCML framework employs a secure multi-party vector comparison algorithm which ensures that any local diagnostic models are encoded by the local community before they are delivered to the cloud and can be used immediately without decryption.

3) Users Privacy-Preserving Solution: To provide the development of predictions of disease risk and recommendations for hospitals, Wang *et al.* [70] designed a privacy-preserving pre-clinical guidance framework, called PGuide, which can be applied to combat COVID-19. Using the PGuide framework, a user requiring health services is able to access the disease risk prediction and hospital recommendation services provided by the health service provider while maintaining the privacy of the user and the service provider. Based on the performance evaluation, the PGuide framework is proven efficient in terms of communication overhead and computational cost. Note that the single-attribute encryption technique is used to achieve privacy-preservation requirements.

4) Data Privacy-Preserving Solution: The online health care provider can offer a trusted data service (e.g., k-NN query) to doctors for more accurate diagnosis with the help of health data. For encrypted outsourced eHealthcare data, Zheng *et al.* [71] proposed a privacy-preserving k-NN query framework based on the homomorphic encryption method. The proposed framework can perform a k-NN computation on data encrypted with a computing complexity $O(lk\log N)$, in which l and N refer to the size of data and the number of data, respectively. Therefore, there is another potential solution that uses the homomorphic cryptographic method, where Yang *et al.* [72] designed a privacy-preserving disease risk prediction framework, named EPDP, which can be applied to combat COVID-19. The proposed EPDP framework performs two phases of disease risk prediction overall, i.e., training in the disease model and disease prediction, while maintaining confidentiality.

5) Identity Privacy-Preserving Solution: To provide an identity privacy-preserving solution, Zhang *et al.* [73] introduced a privacy-preserving disease prediction system, named PPDP, for securing cloud-based e-Healthcare system which can be applied to combat COVID-19. With the proposed PPDP framework, the historical medical data collected from COVID-19 patients are encrypted and transferred to the cloud server, which can then be used to build prediction patterns through the Perceptron Single-Layer learning algorithm to maintain identity privacy. The disease risk for future medical data can be calculated on the basis of prediction models. Based on the nonlinear kernel support vector machine, Zhu *et al.* [74] designed a privacy-preserving online medical pre-diagnosis scheme, named eDiag, for secure healthcare systems. The eDiag scheme enables that critical personal health data can be managed anonymously during the process of online pre-diagnosis. In addition, the eDiag scheme uses polynomial aggregation and lightweight multi-party random masking techniques for providing privacy-preserving.

6) Location Privacy-Preserving Solution: To identify the risk of patient disease in a privacy-sensitive environment, Liu *et al.* [75] designed a privacy-preserving patient-centric clinical decision support framework. In the proposed framework, historical data of previous patients is stored in the cloud and can be applied to build the naive Bayesian classifier without disclosing the patients' individual medical data, then the built classifier can be implemented to calculate the risk of disease for new patients in the future and also allow these patients to recover the names of the most popular diseases depending on their own preferences. Therefore, the additive homomorphic proxy aggregation technique is used to ensure the protection of the privacy of historical data (e.g., location privacy).

V. Future Research

To complete our study, we outline both open challenges and future research opportunities to combat COVID-19. Table V summarizes research challenges in terms of security and privacy for fighting COVID-19 and future pandemics with the IoT.

A. Resistance Against Quantum Computing Attacks

With the new emerging technologies that are evolving all the time, such as quantum computing, the potential solutions of cybersecurity to fight against epidemic situations like COVID-19 will continue to be adapted [104]. As we have seen in this study, through public-key cryptography and hash functions, the blockchain-based solution can provide accountability, redundancy, and transparency. Therefore, the rapid advances in quantum computing technologies are making attacks based on Grover and Shor's methods possible in the near future. Such methods menace both public-key cryptography and hash functions, which require the rethinking of blockchains to use encryption systems that are resistant to quantum attacks. The development of quantum-resistant cryptosystems is one of the significant research challenges, which will help the blockchain-based solutions to combat COVID-19.

B. Vulnerabilities of Machine Learning Techniques

Artificial intelligence is currently employed as a tool to contribute to the fight against the viral pandemic which has infected the world since the beginning of 2020 [105]. The predictions of the virus structure generated by machine learning techniques helped scientists to gain many months of experimentation. The American start-up Moderna is renowned for its control of new biotechnology techniques based on messenger ribonucleic acid (mRNA). With the support of bioinformatics, which includes machine learning techniques, the company has reduced significantly the time needed to design a prototype vaccine testable on humans [106]. However, during learning and classification, an adversarial attack on deep learning can allow an adversary to inject false data into the target system, which will disturb the predictions of the virus structure. Hence, potential vulnerabilities of machine learning algorithms should be carefully designed to find the best predictions of the virus structure.

C. Computer Vision for Remote Diagnosis

Computer vision, as a sub-field of artificial intelligence, has had a big success in the solution of several complex healthcare challenges and has the opportunity to support the control of COVID-19. There have been many computer vision approaches proposed so far, addressing various dimensions of controlling the COVID-19 pandemic. Recently, Ulhaq *et al.* [107] proposed a classification of computer vision techniques to combat COVID-19 into three main research areas: 1) disease treatment and management, 2) disease prevention and control, and 3) diagnosis and prognosis. However, these computer vision techniques are vulnerable to adversarial preprocessing techniques such as image-scaling attacks [108], [109], which will affect the classification of image features (e.g., classify the COVID-19 as a bacterial condition). A possible research direction in this topic could be related to the development of new defenses against image-scaling attacks.

D. IoT Solutions for Vaccine Shipments

On December 11, 2020, the U.S. Food and Drug Administration issued its approval authority stamp for the authorization of Pfizer BioNTech COVID-19 vaccine for use as an emergency product in the United States. However, the Pfizer vaccine faces a challenge in terms of logistics, which shippers are required to maintain it in exceptionally cold temperatures of minus 70 degrees Celsius [110]. The progress of the internet of things technologies can allows monitoring this temperatures of vaccine shipments in transit and can significantly contribute to improving the public's assurance that vaccines are both reliable and cost-effective [111]. The use of the IoT solutions for vaccine shipments is one of the significant research challenges.

E. Applications of Industry 4.0

Industry 4.0 is the implementation of advanced new technologies such as, the IoT, cyber-physical system, cloud computing, fog computing, and Big data analytics, etc., that enable reliability flexibility, visibility, and traceability in an intelligent production system [112]. The use of industry 4.0 as an implementation of a smart factory can contribute to developing a vaccine for COVID-19, which the industrial internet of things (IIoT) will be implemented to integrate the

TABLE V
SUMMARY OF RESEARCH CHALLENGES FOR FIGHTING COVID-19 AND FUTURE PANDEMICS WITH THE IOT

Emerging IoT technologies	Platforms	Advantages for fighting COVID-19 and future pandemics	Future contributions	Research opportunities in terms of security and privacy
Cloud computing	- The cloud computing-based IoT platform includes infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), such as IBM Cloud [79], Google Cloud platform [80], Microsoft Azure [81], and Amazon Web services (AWSs) [82].	- Collect and analyze data from a variety of resources, such as patients with COVID-19. - Doctors can access the files of patients with COVID-19 over a private cloud.	- A cloud computing framework for real-time and remote service of patients with COVID-19.	- How to provide secure data exchange between parties involved in the healthcare process and ensure connectivity with patients?
Edge computing	- Extend services and functionalities offered by the cloud at the edge of the network using the following edge computing products: DELL EMC [83], FUJITSU IoT Solution INTELLIEDGE [84], Google's Edge TPU [85], and Microsoft's Vision AI Toolkit [86].	- Help gather COVID-19-related data and obtain real-time analysis, which will provide a response to medical emergencies.	- Resource-efficient edge computing for healthcare IoT systems.	- How to provide authentication and access control between IoT devices and Edge nodes?
Smart IoT devices	- The COVID-19 essential medical devices such as computed tomography scanners, pulse oximeter, thermometers, COVID-19 test kit PCR, COVID-19 test kit antigen, ingestible sensors, and contact tracing apps, etc.	- Enable real-time monitoring, which can save the lives of patients with COVID-19. - Collect and transfers health data, including, electrocardiogram, blood sugar levels, blood pressure, body heat, and oxygen.	- Reliable IoT devices for long-term connectivity.	- A special IoT device that gives a complete medical report of a patient with COVID-19. - The IoT devices must comply with privacy and security regulations. - The choice of encryption methods is a challenge since the power complexities of IoT devices.
Softwarization and virtualization (SDN and NFV)	- The following SDN/NFV platforms can be used for the abstraction of the network design and structure: Lighty.io [87], Cherry [88], Open Baton [89], ONOS [90], Open NFV [91], and OpenDaylight [92].	- Enable to intelligently route traffic and optimize the use of network resources.	- An SDN-enabled architecture for healthcare IoT systems.	- How to achieve mutual authentication and key agreement between the SDN controller and IoT devices?
Machine learning and AI	- The deep learning approaches can be used to predict COVID-19 health risks as well as for cyber security intrusion detection (e.g., deep belief networks (DBN), deep Boltzmann machine (DBM), Stacked Auto-Encoders, recurrent neural networks (RNNs), and convolutional neural network (CNN) [93]–[95].	- Enable the detection of the likelihood of COVID-19 infection. - Help the development of next-generation vaccines and biopharmaceuticals for COVID-19 as well as future pandemics.	- New machine learning approach for image-based diagnosis of COVID-19.	- A possible research direction in this topic could be related to the development of new defenses against image-scaling attacks. - Identifying potential vulnerabilities of machine learning algorithms should be carefully designed to find the best predictions of the virus structure.
Flying IoT	- The following companies can be used for vaccine drone delivery plans: Boeing [96], DHL Parcelcopter [97], Zipline [98], Wingcopter [99], Flytrex [100], UPS Flight Forward [101], Amazon Prime Air [102], and Wing [103].	- Unmanned aerial vehicles (UAVs) deliver vaccines and other medical supplies directly to patients with COVID-19 in rural areas.	- Reliable flying IoT networks for delivering vaccines.	- Proposing new privacy-preserving schemes to resist against steal the data routing over flying UAVs.
5G/6G wireless connectivity network	- Standard: ITU IMT-2020; - Frequency: 700 MHz-72 GHz; - Data Rate: 20 Gbps; - Max. Range: 28 Km;	- Supporting massive interconnectivity and enabling the transfer of data from patients with COVID-19 to different IoT nodes (i.e., edge nodes).	- Advanced sensing techniques for 6G enabled massive IoT.	- Evaluate threat models in 6G enabled massive IoT. - Proposing new privacy-preserving techniques for 6G enabled massive IoT.
IoT-enhanced supply chain	- GPS-based solutions; - RFID-based solutions; - Sensors-based solutions;	- Allow monitoring the temperatures of vaccine shipments in transit and can significantly contribute to improving the public's assurance that vaccines are both reliable and cost-effective.	- Efficient vaccine distribution planning using IoT-enhanced supply chain.	- How to integrate blockchain technology for sustainable supply chain management? - Proposing new secure data sharing frameworks based on blockchain technology.

underlying equipment resources and guarantee cooperation among equipment as well as the quality-of-service (QoS) of the network. Hence, smart factory architecture should be carefully designed to improve the management of manufacturing resources.

F. The Internet of Bio-Nano Things (IoBNT)

The IoBNT concept is introduced by Akyildiz *et al.* [113], which is defined as the basic structure and function parts that are uniquely identifiable and interact with each other in the biological system. This concept executes functions and processes in connected bio-nano sensors and devices, such as sensing, analysis, operation, and communication with each other. The nano-senors can operate inside the human body and transmit the data (i.e., ECG, heart rate monitors, oxygen, temperature, and blood pressure sensors) to edge nodes for data analysis, and then cloud data centers for storage and end-to-end services [114]. However, a group of attackers can use many cyber attacks (i.e., attacks against Cloud data centers, attacks against Fog-nodes, and attacks against nano-sensors) as presented in Fig. 9, which will disclose sensitive

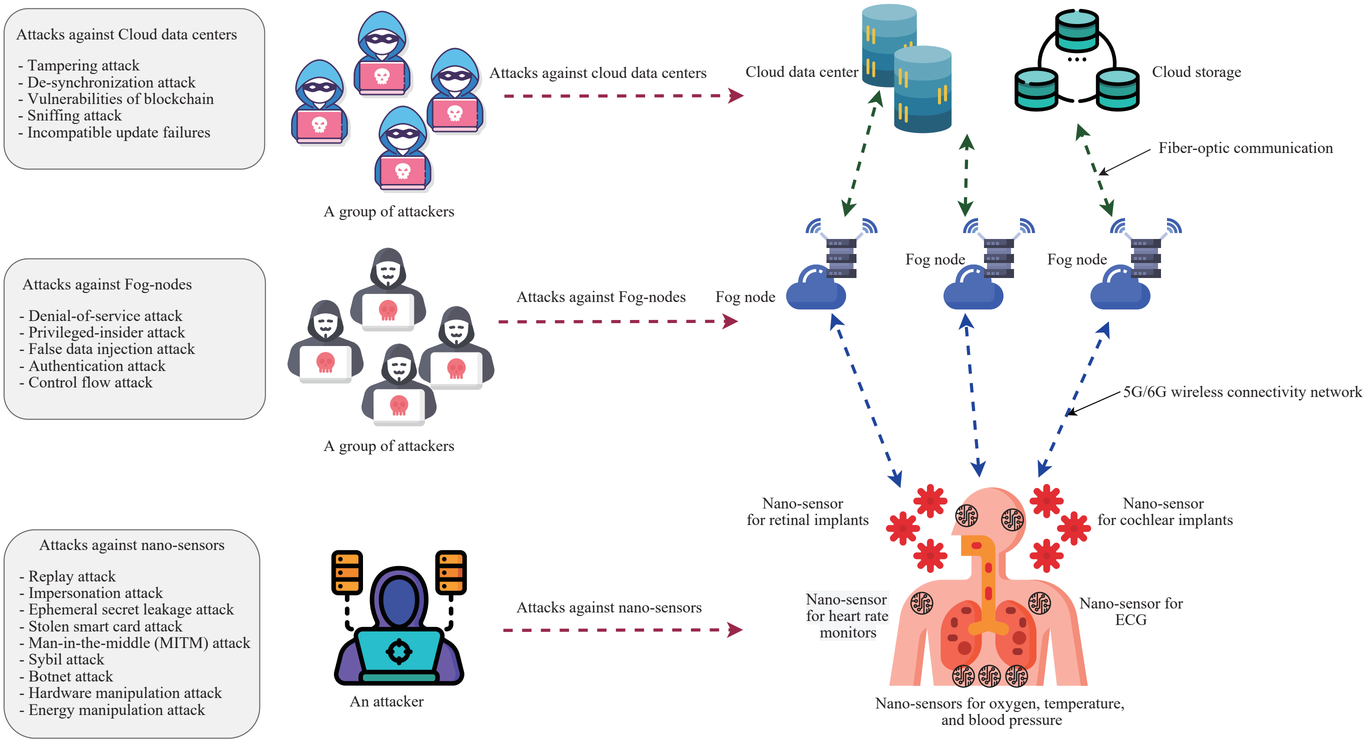

Attacks against Cloud data centers
- Tampering attack
- De-synchronization attack
- Vulnerabilities of blockchain
- Sniffing attack
- Incompatible update failures
A group of attackers
Attacks against cloud data centers
Cloud data center
Cloud storage
Fiber-optic communication
Attacks against Fog-nodes
- Denial-of-service attack
- Privileged-insider attack
- False data injection attack
- Authentication attack
- Control flow attack
A group of attackers
Attacks against Fog-nodes
Fog node
Fog node
Fog node
5G/6G wireless connectivity network
Attacks against nano-sensors
- Replay attack
- Impersonation attack
- Ephemeral secret leakage attack
- Stolen smart card attack
- Man-in-the-middle (MITM) attack
- Sybil attack
- Botnet attack
- Hardware manipulation attack
- Energy manipulation attack
An attacker
Attacks against nano-sensors
Nano-sensor for retinal implants
Nano-sensor for cochlear implants
Nano-sensor for heart rate monitors
Nano-sensor for ECG
Nano-sensors for oxygen, temperature, and blood pressure

Fig. 9. Security threats in the IoBNT architecture with nano-scale devices.

information and affect the smooth operation of the IoBNT networks, such as remote patient monitoring, healthcare delivery drones, and healthcare management, etc. Hence, critical security issues arise as follows:

1) How to provide secure data exchange between parties involved in the healthcare process and ensure connectivity with patients?

2) How to provide authentication and access control between nano-sensors and Edge nodes?

3) How to preserve the privacy of location and identity of nano-sensors?

G. Compliance With Healthcare Data Protection Regulation

To track COVID-19 in countries, some nations like China, Israel, Singapore, and South Korea, the government uses each person's cellphone and credit card information in order to track the moving information as well as know and control whether a person has once been to a high-risk area [115]. In this kind of control, there is no privacy for hiding the visited places from the government. Another thing, some researchers mentioned that they can use the cellphone to record all the potentially contacted (i.e., pass by) people to allow the government to quickly identify and localize the potentially affected people, in this scenario, there is no privacy for hiding from the government. Therefore, the European Union (EU) applies the General Data Protection Regulation (GDPR), which addresses EU law on data protection and privacy, but does not take people's privacy into consideration in epidemic situations like COVID-19. Hence, new technical and organizational measures must be implemented by controllers and processors of personal data in epidemic situations, which is a promising area of research for the near future.

H. Designing a Secure SDN-IoT Framework

The IoT architecture to combat COVID-19 is a fusion of a heterogeneous collection of several technologies, where each technology carries a different set of security challenges and weaknesses. The software defined network (SDN), along with its special features of separating the control plan from the data plan and providing maintenance of a centralized programmable controller, has become increasingly important in overcoming the security issues and challenges associated with the IoT environment [116]. However, the design of a secure SDN-IoT framework to combat COVID-19 is particularly challenging as it requires applying a security protection scheme for various IoT network technologies and management aspects while taking into account the sensitivities of each IoT sub-system.

I. Private Patient Information Issues

Hospitals store an incredible quantity of data on COVID-19 patients. This confidential data is highly valuable to hackers who can easily market it, which makes the industry a rising target. Since the healthcare staff need to access data remotely, the IoT devices can be used as an entry point for attackers to launch an attack such as man-in-the-middle attacks and DoS attacks, which will prevent health care institutions to provide life-saving treatment to COVID-19 patients [117]–[119]. To monitors the system for such attacks, some countermeasures like public key infrastructure (PKI), TLS/SSL-based communication, cryptographic algorithms and protocols, and differential privacy techniques have been proposed. A possible research direction in this topic could be related to developing efficient secure and privacy-preserving schemes using these countermeasures in order to preserve private patient information. In addition, the optimization of computing cost needs to be taken into consideration since the connected bio-nano sensors and devices are characterized by limited resources.

J. Cyber Security Datasets for IoT-Based Platforms

When proposing intrusion detection systems for identifying threats in smart healthcare networks, the finding of complete and valid cyber security datasets is incredibly challenging since there are few IoT-based network traffic datasets with malicious attack behaviors such as BoT-IoT dataset [120]. Therefore, security researchers also use other cyber security datasets such as UNSW-NB15, DARPA/KDD Cup99, NSL-KDD, ISCX 2012, CICIDS 2017, etc. [121]. These cyber security datasets are not simulated for smart healthcare environments to fight against COVID-19. Hence, the development of a new cyber security dataset to build a network intrusion detector under an IoT-based smart healthcare environment is one of the significant research challenges to fight against COVID-19.

VI. Conclusion

In this paper, we provided a comprehensive survey of potential solutions for security and privacy challenges faced by the use of IoT applications for fighting against epidemic situations like COVID-19. Specifically, we presented the security and privacy requirements as well as the threat models, and the challenges associated with developing IoT-based frameworks for COVID-19. Based on review and a new taxonomy of state-of-the-art solutions, we provided a classification into five categories, namely, authentication and access control solutions, key management and cryptography solutions, blockchain-based solutions, intrusion detection systems, and privacy-preserving solutions. The works presented in each class have been crisply summarized and compared with each other. Finally, we discussed and highlighted open challenges and future research directions, including, 1) resistance against quantum attacks, 2) Vulnerabilities of machine learning techniques, 3) computer vision for remote diagnosis, 4) internet of things solutions, 5) applications of industry 4.0, 6) the internet of bio-nano things, 7) compliance with healthcare data protection regulation, 8) designing a secure SDN-IoT framework, 9) private patient information issues, and 10) cyber security datasets for IoT-based platforms. We hope that this survey will help security and privacy protocol designers to design efficient solutions for fighting COVID-19 and future pandemics with the use of IoT applications.

References

[1] WHO, "Novel coronavirus (2019-nCoV): Situation report-10, " World Health Organization, Jan. 2020.

[2] Y. Y. Zheng, Y. T. Ma, J. Y. Zhang, and X. Xie, "COVID-19 and the cardiovascular system," *Nat. Rev. Cardiol.*, vol. 17, no. 5, pp. 259–260, Mar. 2020.

[3] D. S. W. Ting, L. Carin, V. Dzau, and T. Y. Wong, "Digital technology and COVID-19," *Nat. Med.*, vol. 26, no. 4, pp. 459–461, Mar. 2020.

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

[5] M. C. Chang and D. Park, "How can blockchain help people in the event of pandemics such as the COVID-19?" *J. Med. Syst.*, vol. 44, no. 5, Article No. 102, Apr. 2020.

[6] V. Shubina, S. Holcer, M. Gould, and E. S. Lohan, "Survey of decentralized solutions with mobile devices for user location tracking, proximity detection, and contact tracing in the COVID-19 Era," *Data*, vol. 5, no. 4, Article No. 87, Sep. 2020.

[7] L. Garg, E. Chukwu, N. Nasser, C. Chakraborty, and G. Garg, "Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model," *IEEE Access*, vol. 8, pp. 159402–159414, Aug. 2020.

[8] D. Vekaria, A. Kumari, S. Tanwar, and N. Kumar, "Boost: An AI-based data analytics scheme for COVID-19 prediction and economy boosting, " *IEEE Internet Things J.*, doi: 10.1109/JIOT.2020.3047539

[9] Harvard College. Surveys, app. to track COVID-19. [Online]. Available: https://www.hsph.harvard.edu/coronavirus/covid-19-response-public-health-in-action/surveys-apps-to-track-covid-19/, Accessed on: Dec. 27, 2020.

[10] Covid symptom study. [Online]. Available: https://covid.joinzoe.com/us-2, Accessed on: Dec. 27, 2020.

[11] Covid symptom study. [Online]. Available: https://www.webmd.com/lung/coronavirus-apps, Accessed on: Dec. 27, 2020.

[12] A. H. M. Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, "IoMT amid COVID-19 pandemic: Application, architecture, technology, and security," *J. Netw. Comput. Appl.*, vol. 174, p. 102886, Jan. 2021. DOI: 10.1016/j.jnca.2020.102886.

[13] M. Kolhar, F. Al-Turjman, A. Alameen, and M. M. Abualhaj, "A three layered decentralized IoT biometric architecture for city lockdown during COVID-19 outbreak," *IEEE Access*, vol. 8, pp. 163608–163617, Sept. 2020.

[14] I. Ahmed, A. Ahmad, and G. Jeon, "An IoT based deep learning framework for early assessment of COVID-19, " *IEEE Internet Things J.*, doi: 10.1109/JIOT.2020.3034074

[15] Z. Fadlullah, M. M. Fouda, A. S. K. Pathan, N. Nasser, A. Benslimane, and Y. D. Lin, "Smart IoT solutions for combating the COVID-19 pandemic," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 10–11, Oct. 2020.

[16] S. Misra, P. K. Deb, N. Koppala, A. Mukherjee, and S. W. Mao, "S-NAV: Safety-aware IoT navigation tool for avoiding COVID-19 hotspots," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6975–6982, Nov. 2020.

[17] S. Munzert, P. Selb, A. Gohdes, L. F. Stoetzer, W. Lowe, "Tracking and promoting the usage of a COVID-19 contact tracing app," *Nature Human Behaviour*, vol. 5, no. 2, pp. 247–255, 2021.

[18] A. Roy, F. H. Kumbhar, H. S. Dhillon, N. Saxena, S. Y. Shin, and S. Singh, "Efficient monitoring and contact tracing for COVID-19: A smart IoT-based framework," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 17–23, Oct. 2020.

[19] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, Sept. 2017.

[20] Y. Abdulsalam and M. S. Hossain, "COVID-19 networking demand: An auction-based mechanism for automated selection of edge computing services, " *IEEE Trans. Netw. Sci. Eng.*, doi: 10.1109/TNSE.2020.3026637

[21] Y. Siriwardhana, C. De Alwis, G. Gur, M. Ylianttila, and M. Liyanage, "The fight against the COVID-19 pandemic with 5G technologies," *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 72–84, Aug. 2020.

[22] M. Mukherjee, M. A. Ferrag, L. Maglaras, A. Derhab, and M. Aazam, "Security and privacy issues and solutions for fog, " *Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics*, pp. 353–374, 2020.

[23] I. F. Akyildiz, M. Ghovanloo, U. Guler, T. Ozkaya-Ahmadov, A. F. Sarioglu, and B. D. Unluturk, "PANACEA: An internet of bio-nano things application for early detection and mitigation of infectious diseases," *IEEE Access*, vol. 8, pp. 140512–140523, Jul. 2020.

[24] N. Ahmed, R. A. Michelin, W. L. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, "A survey of COVID-19 contact tracing apps," *IEEE Access*, vol. 8, pp. 134577–134601, Jul. 2020.

[25] M. Ndiaye, S. S. Oyewobi, A. M. Abu-Mahfouz, G. P. Hancke, A. M. Kurien, and K. Djouani, "IoT in the wake of COVID-19: A survey on contributions, challenges and evolution," *IEEE Access*, vol. 8, pp. 186821–186839, Oct. 2020.

[26] M. Nasajpour, S. Pouriyeh, R. M. Parizi, M. Dorodchi, M. Valero, and H. R. Arabnia, "Internet of things for current COVID-19 and future pandemics: An exploratory study," *J. Healthc. Inform. Res.*, vol. 4, no. 4, pp. 325–364, Nov. 2020.

[27] A. Sufian, A. Ghosh, A. S. Sadiq, and F. Smarandache, "A survey on deep transfer learning to edge computing for mitigating the COVID-19 pandemic," *J. Syst. Arch.*, vol. 108, p. 101830, Sep. 2020. DOI: 10.1016/j.sysarc.2020.101830.

[28] A. A. Hussain, O. Bouachir, F. Al-Turjman, and M. Aloqaily, "AI techniques for COVID-19," *IEEE Access*, vol. 8, pp. 128776–128795, Jul. 2020.

[29] O. S. Albahri, A. A. Zaidan, A. S. Albahri, B. B. Zaidan, K. H. Abdulkareem, Z. T. Al-Qaysi, A. H. Alamoodi, A. M. Aleesa, M. A. Chyad, R. M. Alesa, L. C. Kem, M. M. Lakulu, A. B. Ibrahim, and N. A. Rashid, "Systematic review of artificial intelligence techniques in the detection and classification of COVID-19 medical images in terms of evaluation and benchmarking: Taxonomy analysis, challenges, future solutions and methodological aspects," *J. Infection Public Health*, vol. 13, no. 10, pp. 1381–1396, Oct. 2020.

[30] F. Shi, J. Wang, J. Shi, Z. Y. Wu, Q. Wang, Z. Y. Tang, K. L. He, Y. H. Shi, and D. G. Shen, "Review of artificial intelligence techniques in imaging data acquisition, segmentation, and diagnosis for COVID-19," *IEEE Rev. Biomed. Eng.*, vol. 14, pp. 4–15, Apr. 2020.

[31] D. Marbouh, T. Abbasi, F. Maasmi, I. A. Omar, M. S. Debe, K. Salah, R. Jayaraman, and S. Ellahham, "Blockchain for COVID-19: Review, opportunities, and a trusted tracking system," *Arab. J. Sci. Eng.*, vol. 45, no. 12, pp. 9895–9911, Oct. 2020.

[32] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, "The role of blockchain to fight against COVID-19," *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 85–96, Aug. 2020.

[33] V. Jahmunah, V. K. Sudarshan, S. L. Oh, R. Gururajan, R. Gururajan, X. J. Zhou, X. H. Tao, O. Faust, E. J. Ciaccio, K. H. Ng, and U. R. Acharya, "Future IoT tools for COVID-19 contact tracing and prediction: A review of the state-of-the-science," *Int. J. Imaging Syst. Technol.*, vol. 31, no. 2, pp. 455–471, Jun. 2021.

[34] M. S. Nawaz, P. Fournier-Viger, A. Shojaee, and H. Fujita, "Using artificial intelligence techniques for COVID-19 genome analysis," *Appl. Intell.*, vol. 51, no. 5, pp. 3086–3103, Feb. 2021.

[35] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, pp. 333–339, Nov. 2019.

[36] H. Lin, S. Garg, J. Hu, X. D. Wang, M. J. Piran, and M. S. Hossain, "Privacy-enhanced data fusion for COVID-19 applications in intelligent internet of medical things, " *IEEE Internet Things J.*, doi: 10.1109/JIOT.2020.3033129

[37] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Secur. Commun. Netw.*, vol. 2019, May 2019.

[38] M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, "Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues," *Telecommun. Syst.*, vol. 73, no. 2, pp. 317–348, Feb. 2020.

[39] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, Jan. 2018.

[40] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. M. Jiang, and L. Shu, "Authentication protocols for internet of things: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2017, Nov. 2017.

[41] D. B. He, N. Kumar, H. Q. Wang, L. N. Wang, K. K. R. Choo, and A. Vinel, "A provably-secure cross-domain handshake scheme with symptoms–matching for mobile healthcare social network," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 633–645, Jul. 2016.

[42] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[43] H. W. Tan, P. Kim, and I. Chung, "Practical homomorphic authentication in cloud-assisted VANETs with Blockchain-based healthcare monitoring for pandemic control," *Electronics*, vol. 9, no. 10, p. 1683, Oct. 2020. DOI: 10.3390/electronics9101683.

[44] T. Alladi, V. Chamola, and Naren, "HARCI: A two-way authentication protocol for three entity healthcare IoT networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 361–369, Feb. 2021.

[45] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, Jul. 2018.

[46] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 5, pp. 942–956, Sep.-Oct. 2020.

[47] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[48] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based solution for COVID-19 digital medical passports and immunity certificates," *IEEE Access*, vol. 8, pp. 222093–222108, Dec. 2020.

[49] A. Shukla, N. Patel, S. Tanwar, B. Sadoun, and M. S. Obaidat, "BDoTs: Blockchain-based evaluation scheme for online teaching under COVID-19 environment, " in *Proc. Int. Conf. Computer, Information and Telecommunication Systems*, Hangzhou, China, 2020, pp. 1–5.

[50] P. Huang, L. K. Guo, M. Li, and Y. G. Fang, "Practical privacy-preserving ECG-based authentication for IoT-based healthcare," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9200–9210, Jul. 2019.

[51] Y. Zhang, R. Gravina, H. M. Lu, M. Villari, and G. Fortino, "PEA: Parallel electrocardiogram-based authentication for smart healthcare systems," *J. Netw. Comput. Appl.*, vol. 117, pp. 10–16, Sept. 2018.

[52] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. P. C. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Trans. Ind. Inform.*, vol. 15, no. 1, pp. 457–468, Jan. 2019.

[53] F. Wu, L. L. Xu, S. Kumari, X. Li, A. K. Das, and J. Shen, "A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications," *J. Ambient Intell. Human. Comput.*, vol. 9, no. 4, pp. 919–930, Aug. 2018.

[54] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, "LSCSH: Lattice-based secure cryptosystem for smart healthcare in smart cities environment," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 24–32, Apr. 2018.

[55] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Pers. Commun.*, vol. 94, no. 3, pp. 1899–1933, Jun. 2017.

[56] L. P. Zhang, Y. X. Zhang, S. Y. Tang, and H. Luo, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795–2805, Mar. 2018.

[57] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.

[58] J. Zhou, Z. F. Cao, X. L. Dong, and X. D. Lin, "PPDM: A privacy-preserving protocol for cloud-assisted e-healthcare systems," *IEEE J. Sel. Top. Signal Process.*, vol. 9, no. 7, pp. 1332–1344, Oct. 2015.

[59] J. Zhou, Z. F. Cao, X. L. Dong, N. X. Xiong, and A. V. Vasilakos, "4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," *Inf. Sci.*, vol. 314, pp. 255–276, Sep. 2015.

[60] M. Masud, G. S. Gaba, S. Alqahtani, G. Muhammad, B. B. Gupta, P. Kumar, and A. Ghoneim, "A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care, " *IEEE Internet Things J.*, doi: 10.1109/JIOT.2020.3047662

[61] M. Wazid, B. Bera, A. Mitra, A. K. Das, and R. Ali, "Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services, " in *Proc. 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and*

Beyond, London, UK, 2020, pp. 37–42.

[62] S. Saha, A. K. Sutrala, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "On the design of blockchain-based access control protocol for IoT-enabled healthcare applications, " in *Proc. IEEE Int. Conf. Communications*, Dublin, Ireland, 2020, pp. 1–6.

[63] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, Feb. 2021.

[64] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for internet of medical things," *IEEE Access*, vol. 8, pp. 181560–181576, Sept. 2020.

[65] K. P. Yu, L. Tan, X. L. Shang, J. J. Huang, G. Srivastava, and P. Chatterjee, "Efficient and privacy-preserving medical research support platform against COVID-19: A blockchain-based approach," *IEEE Consum. Electron. Mag.*, vol. 10, no. 2, pp. 111–120, Mar. 2021.

[66] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110–124, Jan. 2021.

[67] W. J. Li, S. Tug, W. Z. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," *Future Gener. Comput. Syst.*, vol. 96, pp. 481–489, Jul. 2019.

[68] D. J. He, Q. Qiao, Y. Gao, J. J. Zheng, S. Chan, J. X. Li, and N. Guizani, "Intrusion detection based on stacked autoencoder for connected healthcare systems," *IEEE Netw.*, vol. 33, no. 6, pp. 64–69, Nov.–Dec. 2019.

[69] F. W. Wang, H. Zhu, X. M. Liu, R. X. Lu, J. F. Hua, H. Li, and H. Li, "Privacy- preserving collaborative model learning scheme for e-healthcare," *IEEE Access*, vol. 7, pp. 166054–166065, Nov. 2019.

[70] G. M. Wang, R. X. Lu, C. Huang, and Y. L. Guan, "An efficient and privacy-preserving pre-clinical guide scheme for mobile eHealthcare," *J. Inf. Secur. Appl.*, vol. 46, pp. 271–280, 2019.

[71] Y. D. Zheng, R. X. Lu, and J. Shao, "Achieving efficient and privacy-preserving k-NN query for outsourced ehealthcare data," *J. Med. Syst.*, vol. 43, no. 5, Article No. 123, Mar. 2019.

[72] X. Yang, R. X. Lu, J. Shao, X. H. Tang, and H. M. Yang, "An efficient and privacy-preserving disease risk prediction scheme for e-healthcare," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3284–3297, Apr. 2019.

[73] C. Zhang, L. H. Zhu, C. Xu, and R. X. Lu, "PPDP: An efficient and privacy- preserving disease prediction scheme in cloud-based e-healthcare system," *Future Gener. Comput. Syst.*, vol. 79, pp. 16–25, Feb. 2018.

[74] H. Zhu, X. X. Liu, R. X. Lu, and H. Li, "Efficient and privacy-preserving online medical prediagnosis framework using nonlinear SVM," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 3, pp. 838–850, May 2017.

[75] X. M. Liu, R. X. Lu, J. F. Ma, L. Chen, and B. D. Qin, "Privacy-preserving patient-centric clinical decision support system on naive Bayesian classification," *IEEE J. Biomed. Health Inform.*, vol. 20, no. 2, pp. 655–668, Mar. 2016.

[76] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial, " *IEEE Internet Things J.*, doi: 10.1109/JIOT.2021.3078072

[77] L. Maglaras, T. Cruz, M. A. Ferrag, and H. Janicke, "Teaching the process of building an intrusion detection system using data from a small-scale SCADA testbed," *Internet Technol. Lett.*, vol. 3, no. 1, p. e132, Feb. 2020.

[78] R. Mitchell and I. R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 16–30, Jan.–Feb. 2015.

[79] IBM. Cloud. [Online]. Available: https://www.ibm.com/cloud, Accessed on: Mar. 04, 2021.

[80] Google cloud platform. [Online]. Available: https://www.bbsmax.com/A/kPzO8jL7Jx/, Accessed on: Mar. 04, 2021.

[81] Microsoft azure. [Online]. Available: https://azure.microsoft.com/en-us/, Accessed on: Mar. 04, 2021.

[82] Amazon Web Services. [Online]. Available: https://aws.amazon.com/, Accessed on: Mar. 04, 2021.

[83] Dell EMC. [Online]. Available: https://www.delltechnologies.com/en-in/service-providers/edge-computing.htm, Accessed on: Mar. 04, 2021.

[84] FUJITSU IoT solution INTELLIEDGE. [Online]. Available: https://www.fujitsu.com/global/products/computing/pc/edge-computing/, Accessed on: Mar. 04, 2021.

[85] Google's edge TPU. [Online]. Available: https://cloud.google.com/edge-tpu, Accessed on: Mar. 04, 2021.

[86] Microsoft's vision AI toolkit. [Online]. Available: https://azure.github.io/Vision-AI-DevKit-Pages/, Accessed on: Mar. 04, 2021.

[87] Lighty. [Online]. Available: https://lighty.io/, Accessed on: Mar. 04, 2021.

[88] Cherry. [Online]. Available: https://github.com/superkkt/cherry/, Accessed on: Mar. 04, 2021.

[89] OpenBaton. [Online]. Available: https://openbaton.github.io/, Accessed on: Mar. 04, 2021.

[90] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, W. Snow, and Parulkar G, "ONOS: Towards an open, distributed SDN OS, " in *Proc. 3rd Workshop on Hot Topics in Software Defined Networking*, Chicago, USA, 2014, pp. 1–6.

[91] OPENFV. [Online]. Available: https://www.opnfv.org/, Accessed on: Mar. 04, 2021.

[92] Z. K. Khattak, M. Awais, and A. Iqbal, "Performance evaluation of OpenDaylight SDN controller, " in *Proc. 20th IEEE Int. Conf. Parallel and Distributed Systems*, Hsinchu, Taiwan, China, 2014, pp. 671–676.

[93] M. A. Ferrag, L. Maglaras, H. Janicke, and R. Smith, "Deep learning techniques for cyber security intrusion detection: A detailed analysis, " in *Proc. 6th Int. Symp. for ICS & SCADA Cyber Security Research*, 2019, pp. 126–136.

[94] A. M. Ismael and A. Sengur, "Deep learning approaches for COVID-19 detection based on chest X-ray images," *Exp. Syst. Appl.*, vol. 164, p. 114054, Feb. 2021. DOI: 10.1016/j.eswa.2020.114054.

[95] M. M. Islam, F. Karray, R. Alhajj, and J. Zeng, "A review on deep learning techniques for the diagnosis of novel coronavirus (COVID-19)," *IEEE Access*, vol. 9, pp. 30551–30572, Feb. 2021.

[96] Boeing. [Online]. Available: https://www.boeing.com/defense/autonomous-systems/index.page, Accessed on: Mar. 04, 2021.

[97] DHL parcelcopter. [Online]. Available: https://discover.dhl.com/business/business-ethics/parcelcopter-drone-technology, Accessed on: Mar. 04, 2021.

[98] Zipline. [Online]. Available: https://flyzipline.com/, Accessed on: Mar. 04, 2021.

[99] Wingcopter. [Online]. Available: https://wingcopter.com/, Accessed on: Mar. 04, 2021.

[100] Flytrex. [Online]. Available: https://flytrex.com/, Accessed on: Mar. 04, 2021.

[101] UPS. UPS flight forwardTM drone delivery. [Online]. Available: https://www.ups.com/us/en/services/shipping-services/flight-forward-drones.page, Accessed on: Mar. 04, 2021.

[102] Amazon prime air. [Online]. Available: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node8037720011, Accessed on: Mar. 04, 2021.

[103] Wing. [Online]. Available: https://wing.com/, Accessed on: Mar. 04, 2021.

[104] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, Jan. 2020.

[105] M. S. Hossain, G. Muhammad, and N. Guizani, "Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics," *IEEE Netw.*, vol. 34, no. 4, pp. 126–132, Jul.–Aug. 2020.

[106] "AI puts Moderna within striking distance of beating COVID-19, " [Online]. Available: https://digital.hbs.edu/artificial-intelligence-machine-learning/ai-puts-moderna-within-striking-distance-of-beating-COVID-19/, Accessed on: Dec. 27, 2020.

[107] A. Ulhaq, J. Born, A. Khan, D. P. S. Gomes, S. Chakraborty, and M. Paul, "COVID-19 control by computer vision approaches: A survey," *IEEE Access*, vol. 8, pp. 179437–179456, Sept. 2020.

[108] E. Quiring, D. Klein, D. Arp, M. Johns, and K. Rieck, "Adversarial preprocessing: Understanding and preventing image-scaling attacks in machine learning, " in *Proc. 29th USENIX Security Symp.*, 2020.

[109] A. Rahman, M. S. Hossain, N. A. Alrajeh, and F. Alsolami,

"Adversarial examples–security threats to COVID-19 deep learning systems in medical IoT devices, " *IEEE Internet Things J.*, doi: 10.1109/JIOT.2020.3013710

[110] H. Ledford, D. Cyranoski, and R. Van Noorden, "The UK has approved a COVID vaccine-here's what scientists now want to know," *Nature*, vol. 588, no. 7837, pp. 205–206, Dec. 2020.

[111] ZDNET. IoT solutions power safe, speedy and cold COVID-19 vaccine delivery. [Online]. Available: https://www.zdnet.com/article/iot-solutions-power-safe-speedy-and-cold-COVID-19-vaccine-delivery/, Accessed on: Dec. 27, 2020.

[112] B. T. Chen, J. F. Wan, L. Shu, P. Li, M. Mukherjee, and B. X. Yin, "Smart factory of industry 4.0: Key technologies, application case, and challenges," *IEEE Access*, vol. 6, pp. 6505–6519, Dec. 2017.

[113] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The internet of bio-nano things," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 32–40, Mar. 2015.

[114] N. Saeed, M. H. Loukil, H. Sarieddeen, T. Y. Al-Naffouri, and M. S. Alouini, "Body-centric terahertz networks: Prospects and challenges, " Pre-print, 2020. [Online]. Available: http://hdl.handle.net/10754/664913.

[115] CNBC. Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends. [Online]. Available: https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html, Accessed on: Dec. 27, 2020.

[116] P. Mishra, A. Biswal, S. Garg, R. X. Lu, M. Tiwary, and D. Puthal, "Software defined internet of things security: Properties, state of the art, and future research," *IEEE Wirel. Commun.*, vol. 27, no. 3, pp. 10–16, Jun. 2020.

[117] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "BeepTrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3915–3929, Mar. 2021.

[118] P. V. Klaine, L. Zhang, B. P. Zhou, Y. Sun, H. Xu, and M. Imran, "Privacy-preserving contact tracing and public risk assessment using blockchain for COVID-19 pandemic," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 58–63, Sept. 2020.

[119] P. F. Wang, C. Lin, M. S. Obaidat, Z. Yu, Z. Q. Wei, and Q. Zhang, "Contact tracing incentive for COVID-19 and other pandemic diseases from a crowdsourcing perspective, " *IEEE Internet Things J.*, doi: 10.1109/JIOT.2020.3049024

[120] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: BoT-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, pp. 779–796, Nov. 2019.

[121] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, p. 102419, Feb. 2020.

Mohamed Amine Ferrag received the bachelor degree (June, 2008), master degree (June, 2010), Ph.D. degree (June, 2014), HDR degree (April, 2019) from Badji Mokhtar-Annaba University, Algeria, all in computer science. Since October 2014, he is a Senior Lecturer in the Department of Computer Science, Guelma University, Algeria. Since July 2019, he is a Visiting Senior Researcher, NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing Agricultural University. His research interests include wireless network security, network coding security, and applied cryptography. He is featured in Stanford University's list of the world's Top 2% scientists for the year 2019. He has been conducting several research projects with international collaborations on these topics. He has published more than 80 papers in international journals and conferences in the above areas. Some of his research findings are published in top-cited journals, such as the *IEEE Communications Surveys and Tutorials*, *IEEE Internet of Things Journal*, *IEEE Transactions on Engineering Management*, *IEEE Access*, *Journal of Information Security and Applications* (Elsevier), *Transactions on Emerging Telecommunications Technologies* (Wiley), *Telecommunication Systems* (Springer), *International Journal of Communication Systems* (Wiley), *Sustainable Cities and Society* (Elsevier), and *Journal of Network and Computer Applications* (Elsevier). He is currently serving on various editorial positions such as Editorial Board Member in Journals (Indexed SCI & Scopus) such as, *IET Networks*, *International Journal of Internet Technology and Secured Transactions* (Inderscience Publishers), *Security and Communication Networks* (Wiley), and *MDPI Journal of Sensor and Actuator Networks*. His current H-index is 20, i10-index is 29, and 1866 citations in Google Scholar Citation.

Lei Shu (M'07–SM'15) received the B.S. degree in computer science from South Central University for Nationalities in 2002, and the M.S. degree in computer engineering from Kyung Hee University, South Korea, in 2005, and the Ph.D. degree from the Digital Enterprise Research Institute, National University of Ireland, Ireland, in 2010. From 2010 to 2012, he was a Specially Assigned Researcher with the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Japan. He is currently a Distinguished Professor with Nanjing Agricultural University, and a Lincoln Professor with the University of Lincoln, U.K. He is also the Director of the NAU-Lincoln Joint Research Center of Intelligent Engineering. He has published over 400 papers in related conferences, journals, and books in the areas of sensor networks and Internet of Things. His current H-index is 62 and i10-index is 244 in Google Scholar Citation. His current research interests include wireless sensor networks and Internet of Things. He has also served as a TPC Member for more than 160 conferences, such as ICDCS, DCOSS, MASS, ICC, GLOBECOM, ICCCN, WCNC, and ISCC. He was a Recipient of the 2014 Top Level Talents in Sailing Plan of Guangdong Province, China, the 2015 Outstanding Young Professor of Guangdong Province, and the GLOBECOM 2010, ICC 2013, ComManTel 2014, WICON 2016, SigTelCom 2017 Best Paper Awards, the 2017 and 2018 IEEE Systems Journal Best Paper Awards, the 2017 Journal of Network and Computer Applications Best Research Paper Award, and the Outstanding Associate Editor Award of 2017, and the 2018 IEEE ACCESS. He has also served over 60 various Co-Chair for international conferences/workshops, such as IWCMC, ICC, ISCC, ICNC, Chinacom, especially the Symposium Co-Chair for IWCMC 2012, ICC 2012, the General Co-Chair for Chinacom 2014, Qshine 2015, Collaboratecom 2017, DependSys 2018, and SCI 2019, the TPC Chair for InisCom 2015, NCCA 2015, WICON 2016, NCCA 2016, Chinacom 2017, InisCom 2017, WMNC 2017, and NCCA 2018.

Kim-Kwang Raymond Choo (SM'15) received the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2006. He currently holds the Cloud Technology Endowed Professorship with The University of Texas at San Antonio, USA. He is the Founding Chair of IEEE Technology and Engineering Management Society's Technical Committee on Blockchain and Distributed Ledger Technologies, an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor (2021–2023), and included in Web of Science's Highly Cited Researcher in the field of Cross-Field - 2020. He is named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn) in 2016, and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the Outstanding Associate Editor of 2018 for IEEE Access, the British Computer Society's 2019 Wilkes Award Runner-up, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award in 2008. He has also received best paper awards from the IEEE Systems Journal in 2021, IEEE Consumer Electronics Magazine for 2020, EURASIP Journal on Wireless Communications and Networking in 2019, IEEE TrustCom 2018, and ESORICS 2015; the Korea Information Processing Society's Journal of Information Processing Systems (JIPS) Outstanding Research Award (Most-cited Paper) for 2020 and Survey Paper Award (Gold) in 2019; the IEEE Blockchain 2019 Outstanding Paper Award; and Best Student Paper Awards from Inscrypt 2019 and ACISP 2005.