Electronics and Electrical Engineering

AIMS Electronics and Electrical Engineering, 5(2): 146–157.
DOI: 10.3934/electreng.2021008
Received: 08 April 2021
Accepted: 25 April 2021
Published: 26 April 2021

http://www.aimspress.com/journal/ElectrEng

Review

Cyber security during the COVID-19 pandemic

Lidong Wang[1,*] **and Cheryl Ann Alexander**[2]

[1] Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA
[2] Institute for IT innovation and Smart Health, Mississippi, USA

*** Correspondence**: Email: lidong@iser.msstate.edu.

Abstract: COVID-19 has changed the way cyber security is viewed by corporations in the global community. Not only did COVID-19 make many individuals work at home, sometimes on their own computers, and using their own routers, virus protection, etc., the lack of cyber security protection that individuals can provide against hacker attacks, especially for highly sensitive information can be limited. This paper introduces major technologies (such as 5G, blockchain, telemedicine, and big data) in fighting COVID-19, cyber-attacks, and cyber risks (due to people's actions as well as systems and technology failures) during the COVID-19 pandemic, cyber security for telework, cyber security of Internet of Things (IoT) and telemedicine, and cyber security based on blockchain technology. Blockchain helps mitigate the risks of COVID-19 and improves the privacy and security of health systems.

Keywords: cyber security; COVID-19; cyber-attacks; IoT; telemedicine; artificial intelligence; blockchain; privacy; telework; SARS-CoV-2

1. Introduction

COVID-19 is a worldwide public health emergency. The Cybersecurity and Infrastructure Security Agency of the US Department of Homeland Security (DHS) announced an advisory memorandum regarding essential critical infrastructure workers March 28, 2020 [1]. Leadership for dealing with COVID-19 needs to break information silos and coordinate efforts for stopping or containing the new coronavirus that causes COVID-19. Sustainable human security is significant. A broader health system emphasizes security in healthcare, environmental pollution, foods, economy, and preparedness for future possible pandemics. South Korea has realized the importance of tracking infected individuals' movements and persons who had contacted with them [2,3].

Many people had to work at home, choose telemedicine, and perform distance learning and online schooling due to the COVID-19 pandemic. Requirements for these people include computers, the Internet, firewall software, cameras, etc. Meetings can be conducted via video conferencing.

Although calls can be encrypted for security, COVID19 generated new challenges in cybersecurity [3,4]. Work and study at home due to COVID-19 causes increased Internet uses, entices more people to spend much time online, and provides more opportunities for cybercrime [5]. Deadly cyber security threats include malware, spam email, malicious websites, ransomware, malicious domains, DDoS attacks, business email compromise, malicious social media messaging, etc. [6,7]. The development of ICT usage is submitted to security requirements. Factors related to the security include staff's awareness in ICT security, activities related to ICT security, policies regarding ICT security, etc. [8].

During the COVID-19 pandemic, it is important to avoid close contact with many people in daily life. Radio frequency identification (RFID) is helpful for shopping systems, supply chain management, and security. RFID utilizes radio waves and RFID tags with microchips for storing data and antennas for receiving and transmitting radio frequency signals. RFID can provide an extra anti-theft mechanism. Many RFID tags can be read at the same time and from a long distance. Therefore, RFID helps improve the efficiency, safety, and security of various systems during the COVID-19 pandemic [9] due to its simultaneously multiple readings and the capability of remote identification.

The purpose of this paper is to introduce cyber risks and cyber security during the COVID-19 pandemic. The subsequent sections of the paper are organized as follows: the second section introduces major technologies in fighting COVID-19, the third section presents cyber-attacks and cyber risks due to COVID-19, the fourth section introduces cyber security for telework, the fifth section presents cyber security of IoT and telemedicine, the sixth section deals with cyber security based on blockchain technology, and the seventh section is a conclusion.

2. Major technologies in fighting COVID-19

Tactile edge technology focusing on 5G or beyond 5G (B5G) helps control COVID-19 and is more powerful than 4G-enabled technology. The use of edge computation based on 5G wireless network facilitates the control process of the novel disease. A hierarchical system of edge computing has advantages, e.g., scalability, low latency, protecting training model data. Pervasive edge computing can be utilized to achieve better security. A B5G-based healthcare framework was developed to fight pandemics like COVID-19. The framework covers a cloud layer, an edge layer, and a stakeholder layer. It can be integrated with a surveillance system (for mask-wearing, social distancing, body temperature testing). The developed COVID-19 diagnostic method can help to identify patients without COVID-19 infection, avoid overcrowding in a hospital, and process sensitive personal data [10]. More technologies and their main applications in fighting against COVID-19 are summarized in Table 1.

An authentication scheme for cloud-assisted vehicular ad hoc networks (VANETs) was developed [12]. Passengers' physical status can be measured timely and without any contact based on vehicular cloud (VC). A vehicle recording mechanism based on blockchain was fulfilled using edge units and the VC. Requirements for COVID-19 control can be met [12]. Table 2 shows main security features for a VANET security scheme.

Table 1. Main applications of some technologies in fighting COVID-19 [11].

Technologies	Main applications
Virus genome sequencing technology	• Deciding the genome sequence pattern and monitoring the genome mutation of the virus. • Detecting the virus behavior for its controlling.
IoT	• Creating a network of electronic communications between various tools and reducing physical communications. • Collecting real-time data from people who are infected with COVID-19.
Drones	• Disinfecting places, e.g., hospitals. • Transporting food, water, medicine, and laboratory samples of patients. • Detecting people with high-risk behaviors and guiding them.
Geographic information system	• Performing complex spatial analyses to extract the geographical distribution of COVID-19 transmission. • Prioritizing service delivery according to the need for medical services or the prevalence of COVID-19.
Artificial intelligence (AI)	• Estimating the structure of coronavirus proteins. • Analyzing the information related to COVID-19. • Differentiating COVID-19 from other infectious pulmonary diseases. • Epidemiological modeling of the number of patients. • Diagnosing new coronavirus infection.
Telemedicine	• Distance learning to prevent COVID-19. • Tele-monitoring synchronously in mobile health centers. • Tele-triage to monitor people, especially in quarantine conditions. • Post-discharge follow-up.
Big data and blockchain	• Gathering huge amounts of data into a secure platform. • Conducting analyses, extracting models of virus behaviors, and finding appropriate vaccines and drugs.
Robots	• Distributing medicines and personal protective equipment. • Distributing food among quarantined people. • Cleaning and disinfecting hospitals. • Controlling contaminated waste. • Reducing direct contact with patients by performing lab tests, measuring vital signs, etc. • Controlling social interactions and training individuals to fight COVID-19.

Table 2. Major security features for a VANET security scheme [12].

Security features	Description
Mutual authentication	Leading security feature, preventing impersonation attacks on certain devices.
Conditional privacy protection	Targeted vehicle information retrieving and user privacy preserving are the aspects of conditional privacy. The VC is responsible for managing the VANET system and should enable showing identities of suspect vehicles.
Unforgeability	Unforgeability against chosen message attack is the major property in secure data exchange.
Non-repudiation	The validity of transmitted information is guaranteed.
Anonymity	The anonymity of ever VANET device needs to be ensured.
Session key establishment	The session key between the VANET system and an individual vehicle is unique. It needs to be created for following data exchange with security.

3. Cyber-attacks and cyber risks during the COVID-19 pandemic

The disruption due to COVID-19 has disclosed the weaknesses of existing institutions in protecting human health and well-being. A lack of timely and accurate data and widespread misinformation have caused ever-increasing harms and growing tension between public health concerns and data privacy. In the absence of accurate data and reliable information, the suffering due to COVID-19 has been worse. The COVID-19 crisis is an information crisis as well as a trust crisis. It has underlined failures of existing systems in trust and data sharing. During the crisis, main supply chain failures have been noticed, especially for personal protective equipment (PPE) and lifesaving ventilators in clinics and hospitals [13].

Digital methods have played a significant role during the COVID-19 pandemic. However, there are telemedicine challenges and other digital approaches in privacy and security for protected information [14]. Since the beginning of the COVID-19 pandemic, there has been remarkable increase in the number of cyber-attacks. During the pandemic, major cyber risks are caused by people's actions as well as failures of systems and technology. The source of operational risk includes people's actions, for example, deliberate (e.g., theft, sabotage, fraud, and vandalism), inadvertent (i.e., omissions, errors, and mistakes), and inaction (e.g., availability, knowledge, skills, and guidance). Failures of systems and technology lie in software (i.e., coding practices, testing, security settings, change control, configuration management, and compatibility), hardware (i.e., capacity, performance, maintenance, and obsolescence), and system (i.e., specifications, design, integration, and complexity) [15]. Table 3 lists part of malicious and non-malicious breaches. Some potential attack scenarios are shown in Table 4.

Table 3. Some malicious and non-malicious breaches [16].

Types	Description
Stolen device	Stolen smartphone, laptop, hard drive, portable memory device, etc., and data (e.g., sensitive information) along with the device.
Insider fraud	A person (e.g., a contractor or employee) with legitimate access intentionally breaches information.
Outside fraud, not device	Discarded, lost, or stolen nonelectronic records (e.g., paper documents); fraud (involving credit or debit cards) without being accomplished via hacking.
Malware or hacking	Electronic entry by an outside party, malware, spyware.
Accidental disclosure	Sensitive information publicly posted on a website, mishandled, or sent to a wrong party via fax, email, or mail.

Table 4. Some potential attack scenarios [17].

Attacks	Description
Linking attack	An attacker collects auxiliary information of a target from various sources, combines the information, creates an overall picture of the target, and performs attack.
Sybil attack	Attacking data redundancy mechanisms.
Spoofing attack	One object pretends to be another object's identity for gaining trust, entering the system, spreading malware, stealing data, etc.
DoS/DDoS	Attackers use Denial of Service (DoS) or Distributed DoS (DDoS) to block users from accessing services on the network by initiating a huge useless information and therefore causing network congestion.

It is necessary for organizations to solve problems about the security and privacy of all stakeholders' personal data through creating applicable frameworks for data governance. From an ethical point of view, technical compliance with data and privacy laws is often insufficient to protect

organizations from frustrated consumers. There should be adequate incorporated safeguards to handle ethical risks and possible risks in security and reputation of organizations. From a legal point of view, organizations should employ suitable processes to guarantee compliance with laws related to data capture, storage, utilization, and disclosure [18].

4. Cyber security for telework

Working at home due to COVID-19 is the "new normal". Many individuals will not return to an office when the pandemic is over; most individuals in a "work from home" setting will continue in that mode, even after the vaccine has been fully distributed. Schools will most likely be returning from the 14-month hiatus this coming (i.e., 2021) fall. Security and risks in reputation, especially for businesses with sensitive data which have been a concern after regulations of self-isolation pushed people to work at home and organizations had to adapt their business models to accommodate a remarkable increase of network activities. Many hackers have consistently redirected their activities from attacking business toward activities that could reach consumers or employees at their homes through platforms, e.g., Netflix or Zoom [18]. Table 5 shows some items of risky cyber security behaviors.

Table 5. Some risky cyber security behaviors [5].

No	Items
1	Clicking on a link in an unsolicited email from an unidentified source.
2	Utilizing the same password on various websites.
3	Downloading free software of anti-virus from an unidentified source.
4	Entering payment information on a website without clear security information/certification.
5	Downloading materials from a website on a work computer without verifying its authenticity.
6	Downloading digital media (games, movies, and music) from unknown sources.
7	Utilizing free-to-access public Wi-Fi
8	Utilizing an online storage system to keep and exchange sensitive or personal information.
9	Saving organization's information on a personal electronic device such as laptop, tablet, or smartphone.

Table 6. Some technologies and targeted technology brands [19].

Technology types	Targeted/impersonated technology brands	Situational factors	Cybercrimes
Online system for payments	Paypal	Small business loans	Fake website domain
Emails	Gmail	Donation	Fake emails (e.g., phishing)
Video sharing websites	YouTube	Leisure/entertainment	Fake products
Social media technology	Facebook	Social networking	Fake social media profiles
Cloud file hosting services	One Drive	Remote work	Fake products
Companies with broadband and telecoms	4 G (fake company)	Internet/free data	Fake products
Videotelephony and chat services online	Zoom	Remote work	Fake products
Streaming media service (movies and television)	Netflix	Entertainment/ leisure	Fake products

During the COVID-19 pandemic, many organizations perform the teleworking model, causing insufficient cyber security for employees. A lot of employees' networks at home may consist of outdated PCs and insecure devices of IoT. The pandemic has caused technological and end-user vulnerabilities and cyber criminals are exploiting telework vulnerabilities [19]. Tables 6 shows technologies, targeted/impersonated technology brands, situational factors, and cybercrimes.

COVID-19 has caused a shift from ecosystems to a virtual workplace for employees, which brough up challenges in cyber security risks because there are more vulnerabilities on employee's personal computers and their home Internet [20]. Table 7 lists telework cyber security recommendations for remote employees.

Table 7. Cyber security recommendations for telework employees [20].

Aspects	Recommendations
Authentication	Implement two-factor or multi-factor authentication: a text code or a call for authentication is sent to an employee' phone before access to an organizational network is granted.
Management of mobile application and mobile devices	Implement security measures such as malware scans, data encryption, etc.
Security patches and virus protection	Guarantee mobile devices and computers for accessing work networks have virus protection and updated security patches.
Implementation of policies	• Do not share work computers, reducing risks in inadvertent or unauthorized access to secured company information. • Do not access company's information systems while on public Wi-Fi with the utilization of a VPN. • Do not download organization's sensitive information and save it to cloud services (e.g., Google Drive) or personal devices (e.g., thumb drives and employee's computers).
Training of employees	• Train employees on how sensitive data are safeguarded and encrypted at home. • Train them on using Virtual Private Networks (VPNs) to guarantee that the use of Internet is encrypted and that an employee user's location is private when assessing company's network.

5. Cyber security of IoT and telemedicine

Cyber risks are one of main barriers to wide applications of IoT in healthcare. Patients' privacy needs to be protected, ensuring to prevent unauthorized tracking and verification. IoT may provide opportunities for cyber-attacks and for personal information to be captured improperly. Applications based on IoT are vulnerable to cyber-attacks for two reasons: 1) many communications are wireless, making eavesdropping relatively easy when high encryption is not used; 2) low energy is a feature of most IoT components; however, it is hard for them to perform schemes for a guarantee of security [21]. Realizing interoperability across IoT platforms helps deliver more accessible and safer services in healthcare. Data sharing across various countries is also a concern. Data security, confidentiality, and privacy should be federally implemented; however, international hosts or suppliers might not follow domestic laws or regulations [22].

A model for remote health monitoring that uses a lightweight block encryption approach to provisioning security for health in an IoT environment based on the cloud was developed. Data mining was used to analyze biological data generated from IoT devices and a patient's health status is obtained through the analysis. The patients' sensitive data are protected using the encryption approach [23]. IoT has been employed in the control of COVID-19, but there are security issues and privacy risks during data storage and transmission [17].

Telehealth offers opportunities in reducing visits to hospitals, which protects patients and others from the COVID-19 infection. However, telehealth creates cyber security and privacy risks because a patient's home may not have enough protections in place. Telehealth also provides new opportunities in the sharing of health information with security and privacy implications [24]. Telemedicine security threat areas are shown in Table 8 [25–28].

Table 8. Telemedicine security threat areas.

Security threat areas	Description
Internet	Telemedicine systems are vulnerable to security risks related to sniffing, privilege escalations, and alteration/forgery because medical, private, and health information as well as prescriptions are transmitted via the Internet.
Home networks	They include Bluetooth, Wi-Fi, local area network, near field communication, etc. A telemedicine service system based on the home network is vulnerable to security attacks related to end-to-end plaintext transmission and man-in-the-middle (MITM) threats.
Gateway devices	A gateway acts as an intermediary between a patient and a telemedicine system, making the system vulnerable to security attacks related to rogue gateway, the theft/loss of the gateway, and MITM threats.
Telemedicine devices	A telemedicine terminal based on an embedded-type real-time operating system is safe from unauthorized access, but a device (e.g., smartphone) based on a general-purpose operating system uses external apps; therefore, it is vulnerable to security attacks.
The telemedicine system	It handles the data of patients and is possibly connected to related agencies via a governmental network hub. It can be utilized for wireless communication between computers and patients' exercise equipment for teleconsultation. It attracts security threats related to malicious code, illegal network access, MITM attacks, and telemedicine app alteration/forgery.
Patients or users	Most of them live in a remote region, without any training regarding cyber security or with little interest in cyber security; therefore, it is easy for their utilization of telemedicine terminals to receive security attacks due to device loss, weak passwords, device use errors, etc.
Telemedicine service providers	A telemedicine system mainly involves doctor-to-patient and doctor-to-doctor interactions. It is vulnerable to security attacks due to wiretapping, leakage of important data, prescription alterations, and device use errors.

For many organizations, increased investments in compliance (privacy), information security (telework/business continuity), supply chain, and emergency management will help develop infrastructures. Telemedicine allows a greater number of patients to be examined by health care providers while following disease containment protocols of self-isolation regarding COVID-19. Patients receive education, monitoring, and consultation [29]. In the COVID-19 pandemic, tele-healthcare service is needed for the reduction of patient movement and thus the reduction of infection. A tele-medical laboratory service was proposed based on IoT and the cloud. Specifically, physicians, nurses, and other medical staff from various hospitals worked together using their federated hospital clouds, created a virtual health team, and completed a healthcare workflow with security [30].

6. Cyber security based on blockchain technology

Blockchain technology offers immutable and distributed ledgers with auditable records, which is ideal for tracking every asset in supply chain management. It depends on a distributed, privacy-

preserving, secure, and immutable record-keeping framework [13]. Governments and hospitals can identify COVID-19 suspected cases, locations related to reported cases, and infected areas with high risks using blockchain. Blockchain has also been utilized to guarantee healthcare data security [10]. During the COVID-19 pandemic, it is significant to track patients and analyze their symptoms or reactions to the disease. Blockchain is a helpful platform in many countries affected by COVID-19, particularly in healthcare [31].

Insufficient data for risk assessment for catching or transmitting COVID-19 caused the quick spread of COVID-19 in general. Many patients were asymptomatic and the transmission mechanism for COVID-19 was not well understood until around May 2020. When cyber-attacks lead to information block, a permissioned blockchain offers two advantages: 1) anybody in the medical consortium can check when and how transactions and information occur; 2) blocking the information will change the hash. Therefore, patients can transmit personal records without any tampering risks [32]. For SARSCoV-2 (causes COVID-19) sequences, a closed hub was created that controls access and prohibits redistribution. Commercial aspirations can delay data sharing because patent incentives hinder open dissemination. Blockchain enables proof of the existence of specific data objects and their content [33]. COVID-19 data from the Centers for Disease Control and Prevention (CDC) in the United States include data and metadata. Blockchain helps manage medical data, identify patterns of symptoms, track supply chains of medical supplies and medicines, and increase diagnostic accuracy and effectiveness of treatment [3].

'Social Internet of Things' (SIoT) integrates people and smart devices interacting within a social structure of IoT, which is often through IoT platforms. Cloud IoT ecosystems are disruptive, but with many issues regarding security and privacy. SIoT has the same risks. Malware aims at people working at home and healthcare organizations. Blockchain can enhance the security and privacy of digital health systems [34]. A system based on blockchain was proposed to offer the secure management of home quarantine [17].

A novel blockchain-based framework was proposed to integrate intercountry for COVID-19 and track infected or tested patients globally. The framework is being developed as a new system with two components: access point and a single decentralized Ethereum-enabled virtual machine [35]. Blockchain is utilized to bridge the supply chain visibility gap because of its security features such as tamper-resistant, hash proof, and immutability. COVID-19 has disrupted many global supply chains. Rapid Supplier Connect, an IBM blockchain-based network, has been developed to help strengthen medical supply chain during the COVID-19 pandemic [36].

The coupling of AI with blockchain for self-testing and tracking systems has been proposed for the surveillance of COVID-19. Not only can such a system of self-testing achieve a higher testing rate, but it also allows for risk stratification of suspect cases [37]. Blockchain is also effective in data sharing between groups [38]. The applications of blockchain and AI in healthcare can be summarized as follows: health data analytics, remote patient monitoring, drugs and pharmaceutical supply chain management, management of electronic medical records (EMRs), etc. [39].

The management of electronic health records (EHR) with blockchain can reduce clinical bias [40]. The problem of interoperability among various EHR systems may be fixed through utilizing separate blockchain systems [38]. Table 9 shows the SWOT analysis of the utilization of a blockchain-based model in healthcare.

Table 9. SWOT of using a blockchain-based model in healthcare [38]

	Positive	Negative
Internal	***Strengths*** • Transparency • Trust • Immutability • Privacy • Disintermediation and automation	***Weaknesses*** • Lack of flexibility • Creation of possible forks • Operation costs • Need of greater capability of data storage on local servers
External	***Opportunities*** • Increase in technology awareness and new expertise development • Greater collaboration among operators in the healthcare system	***Threats*** • Lack of expertise • Resistance to change • Lack of trust in the application of a new technology by healthcare workers

7. Discussion

During the COVID-19 pandemic, there have been many cyber security issues. However, because there were so many infections and deaths, the pandemic became more news than cyber security vents. Overall, more people are working at home now and using their own security systems and modems. While this adds some layers of protection against cyber security events, it is not generally strong enough to protect the work environment from cyber security casualties. Therefore, the extent of cyber security in the pandemic era means that more stringent levels are layers of cyber security are necessary and should be developed overall while working at home. There needs to be more cyber security options, for example, during the pandemic we should have had a better option for work at home individuals who needed that added layer of security and protection. Most people who worked from home during the pandemic did not have specific training in IT or cyber security; therefore, better training procedures and more efficient programs that provide that extra layer of protection needs to be developed by engineering so that in the future should we have another situation like the COVID-19 pandemic we can provide security for ourselves when we work at home.

Associated with the human conduct aspect of cybersecurity is the undertaking of risky behaviors. Cybersecurity breaches are relevant to both technical implementation and the routine processing of confidential electronic information. Many cybersecurity breaches result from human errors. There should be further research on cybersecurity in relation to human behaviors based on human error-related -related incidents [41]. The data protection and cybersecurity authorities of the European Union (EU) have identified encryption as a significant tool that can contribute to the confidentiality, privacy, data integrity, and data availability of communications and personal data. It has been agreed to enhance the ability of the EU in protecting itself against cyber threats and providing a secure communication environment, especially through quantum encryption [42].

Smartphones and their ability to keep track of their locations (e.g., via GPS and Wi-Fi), along with their built-in Bluetooth interfaces (permitting communication and proximity detection with nearby smartphones), make themselves useful devices for contact tracing. Smartphone contact tracing apps help trace all recent contacts of newly identified individuals with COVID-19 infection, but tracing apps face challenges, including proximity estimation, attack vulnerability, the management of user data, and the privacy and security of the apps [43]. For future research, contact tracing or tracing based on

quantum computing [44] will be exponentially powerful. It may include artificial learning algorithms and advanced Monte-Carlo or particle filter type tracking solutions. Quantum sensing [45] utilizes hypersensitivity embedded in quantum entanglements as an approach to improved timing, network synchronization, location accuracy, and accelerometer accuracy. It is very useful in contact tracing and can maximize the efficacy and overall performance. Quantum communications [46] is one of advanced quantum applications. One of its major impacts on tracing applications will probably be improved cybersecurity in communications and enhanced privacy protection [43].

8. Conclusion

During the COVID-19 pandemic, there are many cyber risks due to people's action as well as failures in systems and technology. Telework and IoT-based applications are vulnerable to cyber-attacks. Telehealth provides an opportunity to protect patients, physicians, nurses, etc. from the COVID-19 infection. However, telehealth creates cyber security and privacy risks. Blockchain helps pandemic management and improves the privacy and security of digital health systems. The combination of blockchain and AI facilitates health data analytics, remote patient monitoring, management of EMR, drugs and pharmaceutical supply chain management, etc.

COVID-19 has issued in a new age of cyber awareness as companies now send their employees to work from home with limited security. Virtual private networks (VPNs) and servers will play a significant role in cyber security of the future. Not only are many companies across the world going to work from home models, thousands of work-from-home companies are now springing up and are facing similar problems. Cyber criminals are all too aware of the limited security that individuals can provide at home. New challenges for the work-at-home individuals include finding simple yet secure solutions for cyber security.

Acknowledgments

Authors thank Technology & Healthcare Solutions, Mississippi, USA for support.

Conflict of interest

Authors declare no conflict of interest.

References

1. Hoops K, Johnson T, Grossman ER, et al. (2020) Stay-at-home orders and firearms in the United States during the COVID-19 pandemic. *Prev med* 141: 106281.
2. Marient M (2020) COVID-19, Human Security, and Global Leadership. *Cadmus* 4: 49–52.
3. Manalu EP, Muditomo A, Adriana D, et al. (2020) Role of Information Technology for Successful Responses to Covid-19 Pandemic. *In 2020 International Conference on Information Management and Technology (ICIMTech)*, IEEE, 415–420.
4. Gaffar B, Alhumaid J, Alhareky M, et al. (2020) Dental Facilities During the New Corona Outbreak: A SWOT Analysis. *Risk Manag Healthc P* 13: 1343.
5. Wijayanto H, Prabowo IA (2020) Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi dan Komputer)* 9: 395–399.
6. Khan NA, Brohi SN, Zaman N (2020) Ten deadly cyber security threats amid COVID-19 pandemic. *TechRxiv* Powered by IEEE: 394-399.

7. Khan NA, Brohi SN, Jhanjhi NZ (2020) UAV's applications, architecture, security issues and attack scenarios: a survey. *InIntelligent Computing and Innovation on Data Science 2020*, Springer, Singapore, 753–760.
8. Meghisan-Toma GM, Nicula VC (2020) ICT Security Measures for the Companies within European Union Member States–Perspectives in COVID-19 Context. In *Proceedings of the International Conference on Business Excellence* 14: 362–370.
9. Gupte R, Rege S, Hawa S, et al. (2020) Automated Shopping Cart Using RFID with a Collaborative Clustering Driven Recommendation System. *In 2020 Second International Conference on Inventive Research in Computing Applications* (ICIRCA), IEEE, 400–404.
10. Hossain MS, Muhammad G, Guizani N (2020) Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics. *IEEE Network* 34: 126–132.
11. Mastaneh Z, Mouseli A (2020). Technology and its Solutions in the Era of COVID-19 Crisis: A Review of Literature. *Evidence Based Health Policy, Management and Economics* 4: 138–149.
12. Tan H, Kim P, Chung I (2020) Practical Homomorphic Authentication in Cloud-Assisted VANETs with Blockchain-Based Healthcare Monitoring for Pandemic Control. *Electronics* 9: 1683.
13. Khurshid A (2020) Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic. *JMIR medical informatics* 8: e20477.
14. Badawy SM, Radovic A (2020) Digital approaches to remote pediatric health care delivery during the COVID-19 pandemic: existing evidence and a call for further research. *JMIR pediatrics and parenting* 3: e20049.
15. Sardi A, Rizzi A, Sorano E, et al. (2020) Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability* 12: 7002.
16. D'Arcy J, Adjerid I, Angst CM, et al. (2020) Too Good to Be True: Firm Social Performance and the Risk of Data Breach. *Information Systems Research* 31: 1200–1223.
17. Zhang J, Wu M (2020) Blockchain Use in IoT for Privacy-Preserving Anti-Pandemic Home Quarantine. *Electronics* 9: 1746.
18. Yallop AC, Aliasghar O (2020) No business as usual: a case for data ethics and data governance in the age of coronavirus. *Online Inform Rev* 44: 1217–1221.
19. Naidoo R (2020) A multi-level influence model of COVID-19 themed cybercrime. *Eu J Inform Syst* 29: 306–321.
20. Burrell DN (2020) Understanding the Talent Management Intricacies of Remote Cybersecurity Teams in Covid-19 Induced Telework Organizational Ecosystems. *Land Forces Academy Review* 25: 232–244.
21. Rub í JN, Gondim PR (2020) Interoperable internet of medical things platform for e-health applications. *Int J Distrib Sens N* 16: 1550147719889591.
22. Kelly JT, Campbell KL, Gong E, et al. (2020) The Internet of Things: Impact and Implications for Health Care Delivery. *J Med Internet Res* 22: e20135.
23. Akhbarifar S, Javadi HH, Rahmani AM, et al. (2020) A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. *Pers Ubiquit Comput* 16: 1–17.
24. Hoffman DA (2020) Increasing access to care: telehealth during COVID-19. *J Law Biosci* 7: 1–15.
25. Kim DW, Choi JY, Han KH (2020) Risk management-based security evaluation model for telemedicine systems. *BMC Med Inform Decis* 20: 1–14.
26. Camara C, Peris-Lopez P, Tapiador JE (2015) Security and privacy issues in implantable medical devices: A comprehensive survey. *J Biomed Inform* 55: 272–289.
27. Bao SD, Poon CC, Zhang YT, et al. (2008) Using the timing information of heartbeats as an entity identifier to secure body sensor network. *IEEE T Inf Technol B* 12: 772–779.

28. Partala J, Keränen N, Särestöniemi M, et al. (2013) Security threats against the transmission chain of a medical health monitoring system. *In 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, 243–248.
29. Snell R (2020) How Is COVID-19 Impacting Compliance Professionals across the Country? *Journal of Health Care Compliance*, 33–38.
30. Celesti A, Ruggeri A, Fazio M, et al. (2020) Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds. *Sensors* 20: 2590.
31. Ahir S, Telavane D, Thomas R (2020) The impact of Artificial Intelligence, Blockchain, Big Data and evolving technologies in Coronavirus Disease-2019 (COVID-19) curtailment. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, IEEE, 113–120.
32. Radanliev P, De Roure D, Walton R, et al. (2020) COVID-19 what have we learned? The rise of social machines and connected devices in pandemic management following the concepts of predictive, preventive and personalized medicine. *EPMA Journal* 30: 1–22.
33. van der Waal MB, Ribeiro CD, Ma M, et al. (2020) Blockchain-facilitated sharing to advance outbreak R&D. *Science* 368: 719–721.
34. Radanliev P, De Roure D, Walton R, et al. (2020) COVID-19 what have we learned? The rise of social machines and connected devices in pandemic management following the concepts of predictive, preventive and personalized medicine. *EPMA Journal* 30: 1–22.
35. Rimsan M, Mahmood AK, Umair M, et al. (2020) COVID-19: A Novel Framework to Globally Track Coronavirus Infected Patients using Blockchain. In *2020 International Conference on Computational Intelligence (ICCI)*, 70–74.
36. Sangeetha AS, Shunmugan S, Murugan G (2020) Blockchain for IoT Enabled Supply Chain Management-A Systematic Review. *In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 48–52.
37. Chen J, See KC (2020) Artificial Intelligence for COVID-19: Rapid Review. *J Med Internet Res* 22: e21476.
38. Fusco A, Dicuonzo G, Dell'Atti V, et al. (2020) Blockchain in healthcare: Insights on COVID-19. *Int J Env Res Pub He* 17: 7167
39. Mashamba-Thompson TP (2020) Crayton ED. Blockchain and artificial intelligence technology for novel coronavirus disease-19 self-testing. *Diagnostics* 10: 1–4.
40. Angeles R (2019) Blockchain-based healthcare: Three successful proof-of-Concept pilots worth considering. *Journal of International Technology and Information Management* 27: 47–83.
41. Evans M, Maglaras LA, He Y, et al. (2016) Human behaviour as an aspect of cybersecurity assurance. *Secur Commun Netw* 9: 4667–4679.
42. Council of the European Union (2020) Council Resolution on Encryption – Security through encryption and security despite encryption. White Paper, 13084/1/20 REV 1, Brussels, November 24, 2020.
43. Ahmed N, Michelin RA, Xue W, et al. (2020) A survey of covid-19 contact tracing apps. *IEEE Access* 8: 134577–134601.
44. Slussarenko S, Pryde GJ (2019) Photonic quantum information processing: A concise review. *Appl Phys Rev* 6: 041303.
45. Degen CL, Reinhard F, Cappellaro P (2017) Quantum sensing. *Rev Mod Phys* 89: 035002.
46. Manzalini A (2020) Quantum communications in future networks and services. *Quantum Reports* 2: 221–232

AIMS Press