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

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.

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

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.

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

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.

Author Bio:
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.

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.

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. doi: 10.1038/s41569-020-0360-5

[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. doi: 10.1038/s41591-020-0824-5

[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. doi: 10.1109/ACCESS.2020.2992341

[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. doi: 10.1007/s10916-020-01577-8