Chapter 17
Privacy and Security Challenges in the Era of the COVID-19 Pandemic

Vishal Sharma
M.M. College of Pharmacy, M. M. (Deemed) University, Mullana, India

Renu Saharan
M.M. College of Pharmacy, M. M. (Deemed) University, Mullana, India

Kashish Wilson
M.M. College of Pharmacy, M. M. (Deemed) University, Mullana, India

Diksha Sharma
Institute of Pharmaceutical Sciences, Kurukshetra University, Kurukshetra, India

Suresh Beniwal
Bharat Institute of Pharmacy, Kurukshetra, India

Chander Parkash Dora
Chitkara College of Pharmacy, Chitkara University, Rajpura, India

ABSTRACT

The outbreak of the COVID-19 pandemic has resulted in social, economic, and healthcare disruption unprecedently worldwide. It has brought practically everything to a halt. Moreover, it has dramatically accelerated the adoption of digital technology resulting in a growing number of incidences of cybercrime, including social engineering to access sensitive information. Furthermore, with the reduced amount of common physical labor, some digital surveillance and security systems were proposed for keeping the trace of transmission. Nevertheless, various automatic associated tracking implementations and the lack of smartphone usage among people bring privacy and security concerns. So, this chapter mainly discusses digital security and privacy violations with their protection measures and the recently developed digital surveillance systems after COVID-19. Furthermore, this chapter will pave the way to understand the futuristic tools and aspects that could be worthwhile in tackling digital privacy and security challenges in managing such infectious diseases.

DOI: 10.4018/978-1-6684-5741-2.ch017

INTRODUCTION

Coronavirus (COVID-19) is a fatal ill-health disease problem that has tremendously trembled the whole world in shock and is called an emergency for the public's health worldwide (Hoops et al., 2020). WHO announced COVID-19 as a pandemic as a disorder of respiratory problems due to SARS COVID-2 in March 2020 (Zhu et al., 2020). This pandemic leads to an increased threat for various businesses in various fields. It produces vast challenges in the medical infrastructure in developed as well as developing countries all around the globe. Different countries have adopted methods to reduce the spread of pandemics, such as lockdown and social distancing in the corporate world, education field, and political arena (Yu et al., 2020). These educational and business hubs tend to adopt new ideas such as work from home, distance learning, and online school work, which shows maximum dependency on the internet, laptop, computer, high pixel camera, and tedious software that pose various challenges. High-level audits and meetings in the corporate sector require conferences through videos (Gaffar et al., 2020). Initially, Digital Surveillance System(DSS) was adopted by the various health care workers and technical experts to monitor the movement of the population on a digital platform as this is not possible to be performed on a manual basis. DSS can be classified into ACT(Automated Contact Tracing) and DSS(Drone Based Monitoring System) in operation fulfillment, but it imposed various challenges. ACT helps in data collection of the person who recently contacted the Covid-19 affected patient through a trained team and multiple applications on smartphones, which is not in every case. The ACT system also tends to diminish the individual's privacy and significant issues arising from security such as mismanagement of the individual data, jamming of the network, and camera hacking the professionals (Altawy & Youssef 2016). Drone Based System(DSS) employs an Unnamed Aerial Vehicle controlled by the leading operator that tends to generate the location and images of the respective person not following the lock down guidelines.

The images can be downloaded in JPEG format, which may get caught in imprecise custody. Further, the other challenges associated with this drone system are hijacking and internet GPS signal issues, along with information distribution and various wireless connections (Gloe, 2012). Cybercrime tends to increase at a fatal rate due to a large amount of internet use in work from home and online schooling because the maximum dependency of the people comes on the internet (Khan et al., 2020). Many cyber security threats are email spam, virus accumulation such as malware and Trojan, spiteful domains, ransom extortion, email regarding business terms and agreements, and malign social media advertisements (Meghisan-Toma & Nicula 2020). During COVID-19, social distancing and close contact among people are employed, leading to Radio Frequency Identification (RFID), which utilizes the indications through high pulsation radio waves. These RFID helps in purchasing arrangements and security with good provision of reduction in theft issues (Gupte et al., 2020). Various corporate sectors have imposed teleworking at home to keep their employee safe. Still, the configuration services at home are indigent compared to IT technology at the office, leading to significant cyberattack changes in the COVID-19 crisis. These Cybercriminals often take charge of the unbarred internet routers, modems and network devices that are unsuccessfully configured at home for official use. Furthermore, Cybercrime was very much uplifted in this COVID-19 time which produces ill-legal operations in education and any corporate meeting. Thus, to avoid these cybercrimes and high-tech broad and inclusive cyber security system is used by the government (Aldawood & Skinner 2019).