Project Proposal
Toward Securing Contact-tracing apps related to Covid-19

Nitin Gupta, Mayank Dhiman, Ujjawal Gupta, Yashwant Kumar
Department of CSE
National Institute of Technology
Hamirpur, Himachal Pradesh, India

Abstract: *From the emergence of Covid-19, the primary focus of governments across the world is contact tracing of the effected person. To achieve this, most of the governments use smartphone data to track where people go and with whom they interact. In this regard, Government of India is also using 'Arogya Setu App' successfully. These so-called contact-tracing apps help public health officials get ahead of the spread of Covid-19. However, the downside is the inherent loss of privacy. If abused, raw location data of a person could reveal sensitive information related to that person using the app. Therefore, this work proposes to develop a lightweight cryptographic algorithm such that sensitive location data can be securely transferred to the destination without being compromised.*

Introduction: Coronavirus disease (COVID-19) is an infectious disease caused by a new virus SARS-COV-2. The disease causes respiratory illness (like the flu) with symptoms such as a cough, fever, and in more severe cases, difficulty breathing [1]. To date more than 42,00,000 people from all over the world have been infected while the disease has taken more than 2,84,000 lives till now [2]. These numbers go on increasing day-by-day. Apart from this, the COVID-19 coronavirus pandemic has plunged the system into a deep crisis. The stock markets are plummeting, a recession seems inevitable. The outbreak of this pandemic is unpredictable in terms of global consequences. From the emergence of Covid-19, the primary focus of governments across the world is contact tracing of the effected person. To achieve this, most of the governments use smartphone data to track where people go and with whom they interact. In this regard, Government of India is also using 'Arogya Setu App' successfully [3]. These so-called contact-tracing apps help public health officials get ahead of the spread of Covid-19. However, the downside is the inherent loss of privacy. If abused, raw location data of a person could reveal sensitive information related to that person using the app [4]. Therefore, this work proposes to develop a lightweight cryptographic algorithm such that sensitive location data can be securely transferred to the destination without being compromised.

Overview of Project: To overcome the above mentioned problem, an Android app has been developed by our team tha similar to the Arogya Setu app helps in collecting the location data of a user, as at this stage code for Arogya Setu is not available. Next, we will develop a lightweight encryption algorithm which can be transferred to the server safely. We will install a server at the remote place and send the encrypted data to the server. Further, recently it is also mentioned that data store in the server may also be leaked like Aadhaar card data [5]. To overcome this issue, data in encrypted form only be stored in the server and can only be retrieved by the authorized person.

The project is expected to overcome the problem of security issues in the location aware apps used for Covid-19.

Keywords: Covid-19, Location data, Arogya Setu App, Cryptography.

Expected Outcome: Light weight cryptographic algorithm to secure location data which can preferably work with 'Arogya Setu App.'

Expected Timeline: 6-8 Weeks

Budget Requirements: NIL.

References

[1] Y.-Y. Zheng, Y.-T. Ma, J.-Y. Zhang, and X. Xie, "Covid-19 and the cardiovascular system," *Nature Reviews Cardiology*, vol. 17, no. 5, pp. 259–260, 2020.

[2] "Worldometer," http://www.worldometers.info/, 2008, [Online; accessed 11-May-2020].

[3] NIC, "mygov," http://www.mygov.in/aarogya-setu-app/, 2020, [Online; accessed 29-April-2020].

[4] T. Week, "Security issue found in Aarogya Setu app," http://www.theweek.in/news/india/2020/05/05/security-issue-found-in-arogya\ \-setu-app-rahul-gandhi-was-right-cybersecurity-expert.html, 2020, [Online; accessed 05-May-2020].

[5] T. Hindu, "Hacker 'sees' security flaws in Aarogya Setu," http://https://www.thehindu.com/news/national/ethical-hacker-robert-baptiste-elliot\ \-alderson-sees-security-flaws-in-aarogya-setu/article31515292.ece, 2020, [Online; accessed 06-May-2020].