Internet of Things, Ad Hoc and Sensor Networks Technical Committee Newsletter (**IoT-AHSN TCN**)

https://ahsn.committees.comsoc.org/newsletter/

CONTENTS

PREFACE

The IEEE ComSoc Ad Hoc and Sensor Networks Technical Committee (IoT-AHSN TC) sponsors papers, discussions, and standards on all aspects of IoT, ad hoc and sensor networks. It provides a forum for members to exchange ideas, techniques, and applications, and share experience among researchers. Its areas of interest include systems and algorithmic aspects of sensor and ad hoc networks, networking protocols and architecture, embedded systems, middle-ware and information management, novel applications, flow control and admission control algorithms, network security, reliability, and management. In an attempt to make all the TC members as well as the IoT-AHSN worldwide community aware of what is going on within our main areas of concerns, this newsletter had been set up. The newsletter aims at inviting the authors of successful research projects and experts from all around the world with large vision about IoT-AHSN-related research activities to share their experience and knowledge by contributing in short news. So, the thirteenth issue of the IoT-AHSN TC Newsletter features three high quality news items related to projects, initiatives and recent results on "IoT and AHSN for combating COVID-19 pandemic" gently provided by: (i) Jeffrey Jiarui Chen (St. Mark's School of Texas, USA), Rui Chen (University of Houston, USA), Xinyue Zhang (University of Houston, USA), Liang Li (Xidian University, China), Yanmin Gong (University of Texas at San Antonio, USA), Yuanxiong Guo (University of Texas at San Antonio, USA), Lan Ni (University of Houston, USA) and Miao Pan (University of Houston, USA) with a contribution entitled "*Location Privacy-Preserving COVID-19 Symptom Map Construction via Mobile Crowdsourcing for Proactive Constrained Resource Allocation*", (ii) Shaik Shakeel Ahamad (Majmaah University, KSA) and Al-Sakib Khan Pathan (Independent University, Bangladesh) with a contribution entitled "*Security and Privacy-aware Mobile Healthcare Framework During COVID-19-like Pandemic*", and (iii) Burak Kantarci (University of Ottawa, Canada) with a contribution entitled "*AI-Backed Decision Support for COVID-19 Mobile Assessments and Supply Services*". We thank them as well as all the previous contributors for their effort to make this newsletter successful towards fulfilling its objectives.

Newsletter Co-editors

Sidi-Mohammed Senouci, University of Burgundy, France (EiC)
Yacine Ghamri Doudane, University of La Rochelle, France (EiC)

TC OFFICERS AND NEWSLETTER EDITORS

TC Officers

Names	Affiliation	E-mail
Soumaya Cherkaoui	Université de Sherbrooke, Sherbrooke (QC), Canada	soumaya.cherkaoui@usherbrooke.ca
Jiajia Liu	Xidian University, Xi'an, Shaanxi, China	liujiajia@xidian.edu.cn
Sharief Oteafy	DePaul University, Chicago, IL, USA	soteafy@depaul.edu

Editors-in-Chief

Names	Affiliation	E-mail
Sidi-Mohammed Senouci	University of Burgundy, France	Sidi-Mohammed.Senouci@u-bourgogne.fr
Yacine Ghamri Doudane	University of La Rochelle, France	yacine.ghamri@univ-lr.fr

NEWS RELATED TO IOT-AHSN TC

Special Issue on "IoT and AHSN for combating COVID-19 pandemic"

Location Privacy-Preserving COVID-19 Symptom Map Construction via Mobile Crowdsourcing for Proactive Constrained Resource Allocation

Jeffrey Jiarui Chen[1], Rui Chen[2], Xinyue Zhang[2], Liang Li[3], Yanmin Gong[4], Yuanxiong Guo[5], Lan Ni[6] and Miao Pan[2]

[1]St. Mark's School of Texas, 10600 Preston Rd, Dallas, TX 75230
[2]Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77204
[3]School of Cyber Engineering, Xidian University, Xi'an, China 710071
[4]Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249
[5]Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249
[6]Valenti School of Communication, University of Houston, Houston, TX 77204

Abstract

The COVID-19 pandemic has caused a global public health crisis in the US and many other countries in the world. To combat the coronavirus, many countries have been using mobile phone tools and data sources for COVID-19 surveillance, such as tracking infections, monitoring community spread, and identifying populated areas at risk. However, the use of mobile devices as part of this effort has raised concerns around privacy, specifically location privacy. Our project uses a mobile crowdsourcing-based symptom report to develop a fine-grained COVID-19 vulnerability map. The vulnerability map tracks the number of people with COVID-like symptoms, so that the potential outbreak communities can be identified. This allows valuable healthcare resources to be proactively and dynamically allocated. To address the users' privacy concern, we proposed to make a COVID-19 vulnerability map without disclosing the participants' actual location. To protect the user's privacy, we used a semi-honest crowdsourcing aggregator. Based on the differentially private geo-indistinguishability, the mobile participants were able to locally perturb their geographic data. With the users' geographic location masked, we employ a best linear unbiased prediction estimator (BLIP) with spatial smoothing to obtain reliable vulnerability estimates in the areas of interest and construct the map. Furthermore, a federated learning framework that enables multiple crowdsourcing mobile apps to collaboratively derive the vulnerability prediction and construct the fine-grained VMP is developed. The FL-based fine-grained vulnerability map construction leverages a large amount of survey data while at the same time circumventing data privacy regulations that prevent user information from multiple apps to be shared with each other. Simulation results of the proposed FL framework with a long short-term memory (LSTM) neural-network model show a 6% improvement in prediction accuracy over the widely used FedAvg algorithm while at the same time providing user privacy.

1. Introduction

The COVID-19 pandemic has caused an unprecedented global crisis. Internet of Things (IoT) technology has been playing an important role in mitigating the crisis. Data collected from various mobile devices can be utilized to monitor the pandemic and to perform statistical analysis. COVID-19 heatmaps that show the locations of people with a high risk of being infected can help the public understand COVID-19 transmission in communities and facilitate healthcare organizations to proactively allocate scarce healthcare resources.

The COVID-19 vulnerability map construction relies on comprehensive COVID-19 data to be successful and accurate. The maps are normally generated based on infection information from local governments or the Centers for Disease Control and Prevention (CDC). However, the existing COVID-19 tracking maps only show confirmed cases at the county level. They don't provide fine-grained levels of vulnerability and also face a lack of adequate coverage of asymptomatic people. Consequently, there has been an increase in the number of various mobile and self-reporting web apps that allow users to send in crowd-sourced symptom data. These crowd-sourcing apps collect a tremendous amount of data that are tagged with specific geographic information. This information makes it possible to construct a fine-grained vulnerability map to reliably predict COVID-19 vulnerability [1].

The benefits of using mobile phone data to track and monitor the pandemic, however, are also accompanied by potential privacy concerns. There are risks to collecting sensitive data that show personal health and geographic location. People might worry about who will receive the data, how those recipients might use the data, how the data might be shared with other entities, and what measures will be taken to safeguard the data from theft or abuse. The possibility that one's privacy might be violated may dissuade people from sharing information.

Machine learning (ML) models have been recently used to predict the future trend of the coronavirus. However, this approach raises new challenges. Crowdsourced symptom-related data contains sensitive information and transferring this information is regulated by the government. This regulation prevents data from multiple crowdsourcing apps to be shared with each other. Another issue is that the crowdsourcing data may not distribute uniformly among devices, which can occur when the users of an app are from a particular community and thus represent a similar demographic. This could lead to misrepresentation of certain groups, potentially generating an inaccurate map. Last but not least, in some rural areas, there may be not enough crowdsourcing data collected and the small dataset can cause the overfitting problem in the ML model.

In this context, this project aims to build a privacy-preserving mobile crowdsourcing platform and a federated learning framework that leverages multiple crowdsourcing mobile and web apps for COVID-19 vulnerability prediction and fine-grained vulnerability map construction. Participants can report their symptoms in real-time to help track specific locations where COVID-19 is spreading. The data collected is then used to predict the coronavirus infection dynamics. To address the mobile crowdsourcing participants' privacy concerns, a location privacy-preserving feature leveraging geo-indistinguishability is developed. Furthermore, a federated learning framework that enables multiple self-reporting apps to collaboratively achieve a reliable vulnerability prediction and VMP construction is created. The potentially imbalanced datasets from each individual self-reporting app are addressed by an adaptive worker selection algorithm that ensures the aggregated age distribution correctly represents the age distribution in the fine-grained map area. To protect the user's privacy, a distributed differential privacy (DDP) scheme is employed on the age distribution. The FL-based fine-grained COVID-19 vulnerability map is promising in its ability to reliably identify the potential outbreak areas while preserving the participants' privacy.

2. Privacy-Preserving Crowdsourcing COVID-19 Prediction and VMP Construction

The goal of the project is to develop a privacy-preserving mobile crowdsourcing framework that predicts COVID-19 spread and vulnerability. A fine-grained and periodically updated vulnerability prediction map is constructed by collecting COVID-19 symptoms data through a mobile crowdsourcing platform, as depicted in Fig. 1. The system consists of four components: a mobile survey app that takes in symptoms, a cloud-based aggregator, a COVID-19 vulnerability analyzer, and an interactive mobile map app. The aggregator in the mobile crowdsourcing platform launches an online survey that asks users to input which COVID-like symptoms they have. The participants anonymously report their answers to the survey along with their location information to the

aggregator. By using a semi-honest crowdsourcing platform, a geo-indistinguishability scheme [2] is employed to protect the participants' location privacy in the survey. More specifically, the participants' location data is perturbed before uploading, which ensures differential privacy [3]. To estimate the vulnerability level in a fine-grained map, the analyzer first determines the individual vulnerability level based on the symptom self-reporting. Then, given the obfuscated locations, it utilizes a spatial best linear unbiased prediction (SBLUP) estimator [4] with a spatial smoothing technique to reduce the estimation bias induced by the use of the privacy protection scheme. The analyzer further predicts the trend of the coronavirus by utilizing a susceptible-exposed-infected-removed (SEIR) model [5]. Finally, an interactive mobile map app displaying the vulnerability levels and the trend of COVID-19 is implemented using Google Maps.

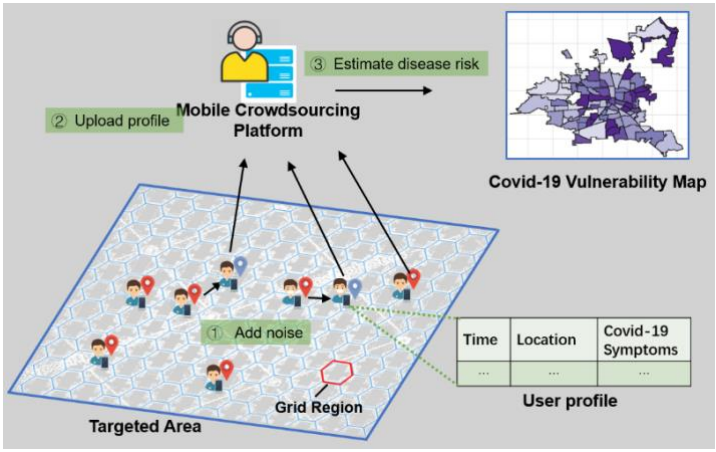

Figure 1. Vulnerability map construction via mobile crowdsourcing.

Since the location information is closely related to either the participant's home or work address in the fine-grained map, the crowd-sourcing platform provides a masked address instead of the true location. The masked location is generated based on geo-indistinguishability and it has a personalized privacy budget included. A two-dimensional Laplace distribution is applied to randomly produce the location noise. In the design, the probability of generating an obfuscated location is decreased exponentially with the distance from the actual location.

In order to achieve a fine-grained vulnerability prediction, the targeted map area is divided into several non-overlapping cells. The spatial unit is set to the street or township area. Each cell is tagged with a certain vulnerability prediction level. Given the users' reported symptoms and their obfuscated locations, the crowdsourcing analyzer predicts the vulnerability level for each cell and generates the vulnerability map in the targeted area. The map construction contains two steps. The first step is calculating the individual risk assessment. The vulnerability score of each participant is evaluated as the number of reported symptoms divided by the total number of predefined symptoms related to COVID-19, such as cough, fever with body temperature, chest pain and shortness of breath, etc. The second step is to determine the cell-level estimation. By associating users with grid cells based on locations, the analyzer estimates the cell-level vulnerability by obtaining the averaged individual risk assessments. Since the true location of a user may be perturbed to a location that belongs to a different grid cell, the sample size of the grid cell of interest could be affected. Additionally, small geographical regions may not have sufficient survey data to be statistically reliable. To adjust the estimates and account for the problems listed above, the SBLUP technique, a widely used approach in small area estimation, is utilized. The technique considers the vulnerability levels of neighboring grids as well as the spatial correlation in the target area.

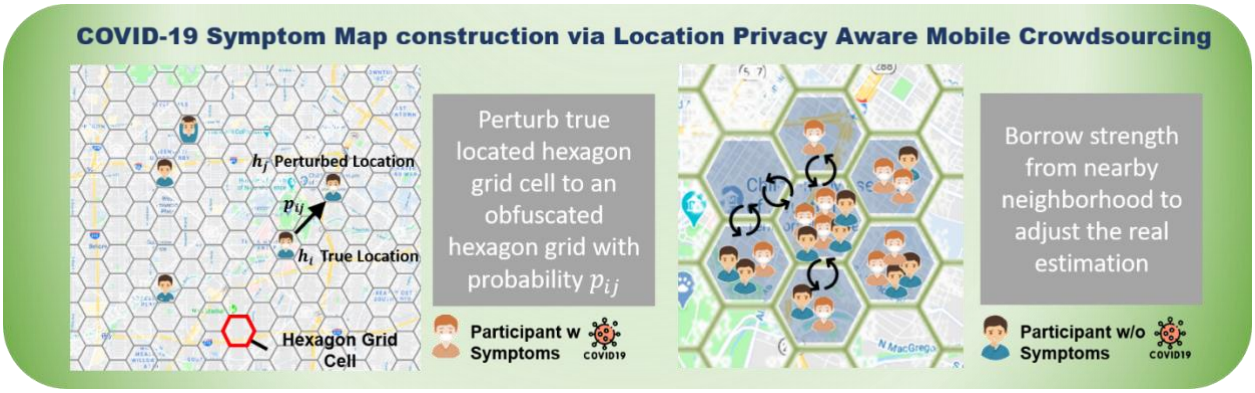

Figure 2. COVID-19 symptom survey and prediction with location privacy protection.

To predict the possible risk trend of a specific cell, the analyzer leverages the ensemble results of the number of infected individuals from two learning models: the SEIR model and the LSTM model. The SEIR model is a commonly used mathematical algorithm to describe the diffusion of an epidemic disease. It computes the number of infected individuals based on the number of contacts, probability of COVID-19 transmission, incubation and infectious periods, and the disease fatality rate. In the SEIR model, the total population is divided into four groups: Susceptible, Exposed, Infected, and Removed. Susceptible people are those who are not yet infected but are at risk of being infected. Exposed people are those who have mild symptoms or are asymptomatic but have not been confirmed as infected. Infected people are those who have been confirmed to be infectious. Removed people are those who have been cured or died from the disease. The COVID-19 vulnerability analyzer empirically estimates the parameters in the SEIR model based on the observed confirmed cases. The long-short term memory network is an extension of the recurrent neural network (RNN), which is a widely used time series prediction model. RNNs contain hidden states distributed across time, and this allows them to store information about the past. However, one limitation of RNN is the vanishing gradient or exploding gradient problem. Thus, it can be difficult to train standard RNNs to solve problems that require learning long-term temporal dependencies. LSTM models overcome the disadvantages of traditional RNN models by introducing a memory cell that can store information for long periods of time. A set of gates is used to control when information enters the memory, when it is outputted, and when it is forgotten. The COVID-19 vulnerability analyzer utilizes the LSTM model to observe the long-term dependencies in the history of COVID-19 cases. The analyzer combines the decisions from both SEIR and LSTM models to collaboratively predict the temporal evolution of the COVID-19's spread. The ensemble results improve the prediction accuracy and reduce causes of error in learning models due to noise, bias, and variance.

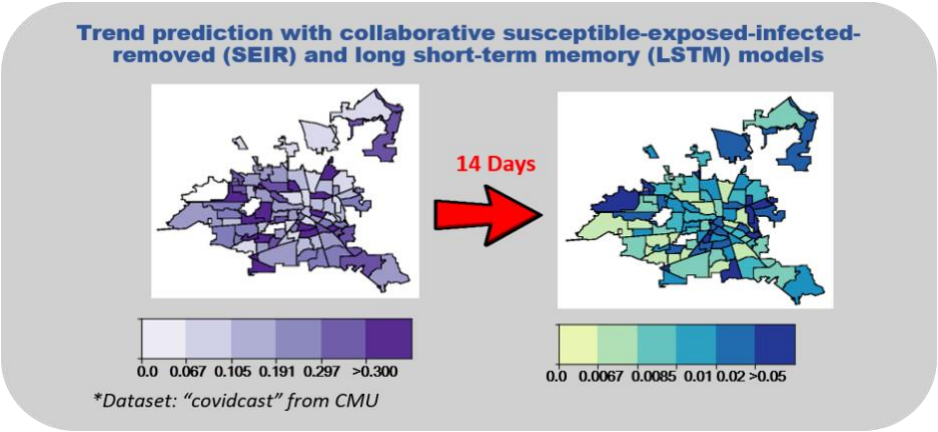

Figure 3. Covid-19 trend prediction with collaborative SEIR and LSTM learning models.

3. Privacy-Preserving Federated Learning for Reliable COVID-19 Vulnerability Prediction

To take advantage of the large amount of COVID-19 survey data available from public-domain mobile and web apps, a privacy-preserving federated learning framework that enables multiple self-reporting apps to cooperate with each other is developed. FL is a state-of-the-art ML approach that seeks to address the problems of data governance and privacy by training algorithms collaboratively without exchanging raw input data [6]. Most recently, several approaches utilizing FL have been developed for COVID-19 applications, such as using X-ray image analysis to detect lung infections. To the best of our knowledge, our approach using the FL method to construct a reliable and accurate COVID-19 vulnerability map is unique.

The proposed FL framework for the coronavirus vulnerability prediction and VMP construction is shown in Fig. 4. In the VPM, the targeted area is divided into non-overlapping cells. Each cell is set to street or township level, such as a zip code. The framework contains a central server and many app providers. The central server creates a broker for each cell and manages the broker operations. In each cell, a broker is responsible for performing an area vulnerability prediction via FL. The central server supervises the crowdsourcing apps as they join the framework. An app is allowed to join the framework if it contains user reported COVID-19 symptoms data and provides the central server with a list of its workers. A worker is defined as an individual crowdsourcing app provider which collects and stores self-reporting data. It provides CPU and memory resources to be used in the model training process. The workers can be from different apps. The central server sends the workers' IDs to the corresponding broker. Each broker coordinates the workers in the cell to jointly train the FL model. A broker server selects a set of workers from the total available workers in the cell for training. The broker server starts a model training process with a preset of model parameter weights. Each worker downloads the primary model with the weights and hyperparameters from the broker server such as the batch size, the local epochs, and the model learning rate. The workers train the new model locally using their own data and upload the generated weights to the broker. The broker gathers the locally trained models and aggregates them to obtain a shared global model. The broker repeats the training process until a preset epoch number, or an accuracy condition is reached. In the FL framework, the broker does not need to know about the user information since the data is stored locally on each worker and will not be shared with the broker during training. After training, the broker sends the prediction results to the central server to construct the vulnerability map. The potentially imbalanced or biased datasets from each individual self-reporting app are addressed by an adaptive worker selection algorithm to find additional workers from each cell's neighboring workers to ensure the aggregated age distribution correctly represents the age distribution in the fine-grained area. A dataset pre-processing mechanism is also employed to mitigate the potential small dataset problem. To protect user's privacy, a DDP scheme is applied to the age distribution parameter.

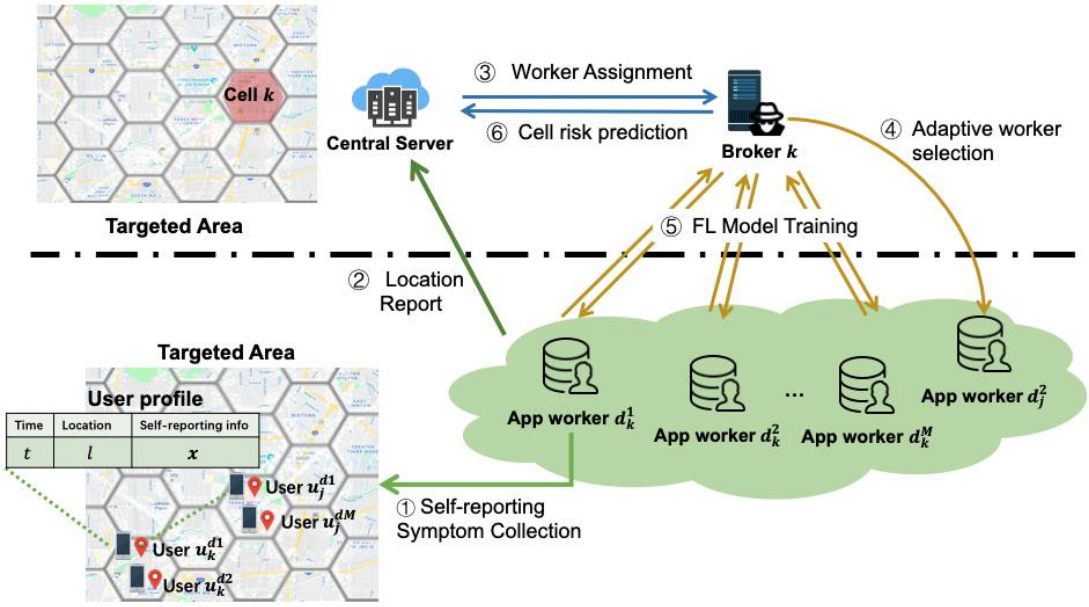

Figure 4. Federated learning framework for COVID-19 vulnerability map construction.

We now examine the performance of the proposed framework for the construction of the privacy-preserving vulnerability map. The software used for performance evaluation is Python. We regard the City of Houston as the target area for estimating the risk level at each super neighborhood. Houston's government has divided the city into 88 super neighborhoods. Each neighborhood has the attributes of a grid ID and boundary GPS coordinates. Each neighborhood's age distribution is utilized in the adaptive worker selection algorithm. The simulation results are based on the publicly available Demystata COVID-19 dataset [7] that includes COVID-19 cases within the US aggregated by zip code. We estimate the super neighborhood COVID-19 cases based on the percentage of the population in the zip code. We simulate the user symptom data by using the number of COVID-19 cases in each age group reported by Harris County Public Health [8]. Figure 5 shows the prediction accuracy improvement in one area. The blue line is the vulnerability level from the testing data and the green line is our proposed approach and the red line represents the widely used FedAvg results. Our results are much closer to the testing results. The root mean square error (RMSE) was reduced from 0.372×10^4 to 0.125×10^4. On average there is a 6% improvement in prediction accuracy compared with the FedAvg FL method. Not only were our predictions accurate, but we also protected the user's privacy throughout the machine learning process.

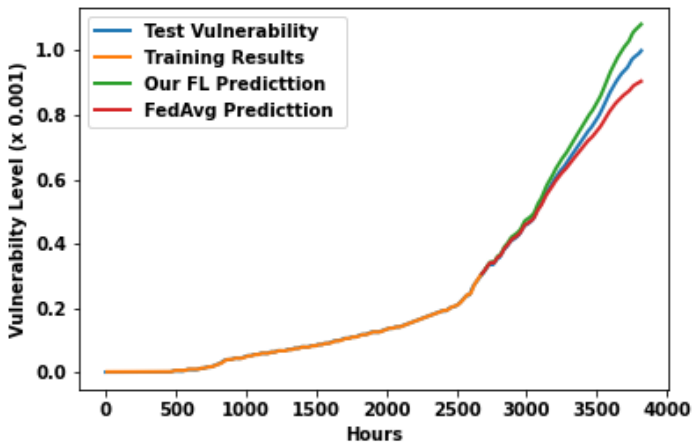

Figure 5. Vulnerability prediction performance.

4. System Implementation

The privacy-preserved mobile survey app and the interactive mobile map app were developed using Android Studio and Google Maps. The privacy-preserved mobile survey app allows participants to anonymously report their symptoms, as shown in Figs. 6(a) and (b). The aggregator uses the Google Firebase database to store users' information, as illustrated in Fig. 6(c). The COVID-19 vulnerability analyzer is developed in Python. It acquires the newly obtained user information from the Google Firebase database and constructs the vulnerability map and uploads both maps into Google Firebase storage space. The interactive mobile map app downloads the vulnerability and trend maps from Google Firebase and displays them on Google maps, as shown in Figs. 6(d) and (e).

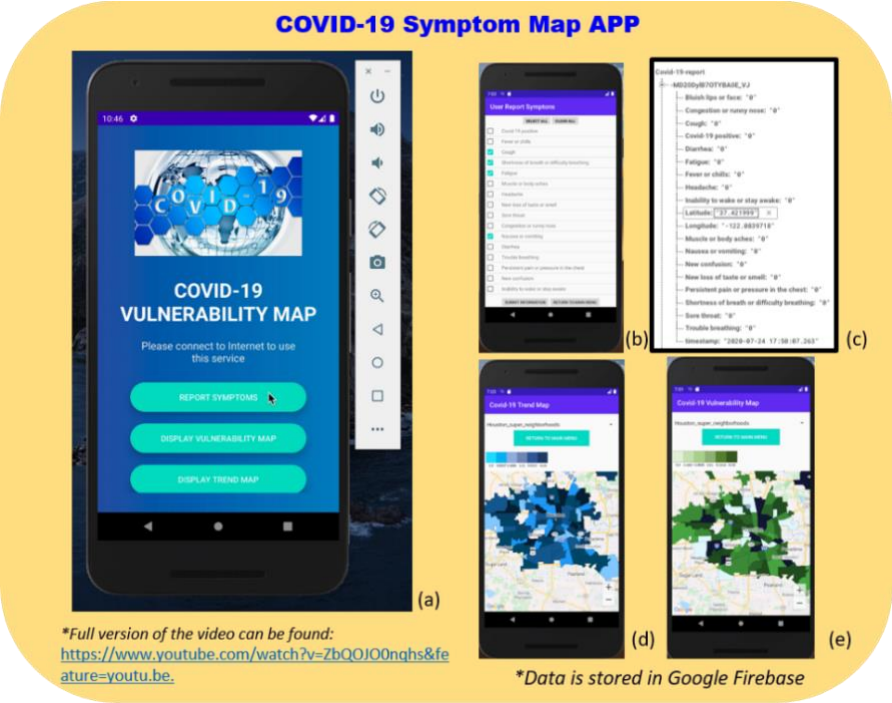

Figure 6. COVID-19 Mobile survey and vulnerability and trend map apps development.

5. Conclusion

We have developed a privacy-preserving mobile crowdsourcing platform and a federated learning framework that leverages multiple crowdsourcing mobile and web apps to predict COVID-19 vulnerability and construct a fine-grained map. The geo-indistinguishability approach has been applied to protect users' sensitive geographic profiles. The spatial estimators have been leveraged to resolve the problem of an unreliable risk estimation due to location uncertainty. Further, a federated learning framework has been developed for reliable COVID-19 future trend prediction by utilizing the large amount of survey data available from multiple crowdsourcing apps while at the same time providing a privacy guarantee. The mobile survey app and an interactive COVID-19 vulnerability and trend mobile map app were developed using Android Studio and Google Maps.

References

[1] R. Chen, L. Li, J. Chen, R. Hou, Y. Gong, Y. Guo, and M. Pan, "Covid-19 vulnerability map construction via location privacy preserving mobile crowdsourcing," in IEEE Global Communications Confer- ence (GLOBECOM'20), Taipei, Taiwan, December 2020.
[2] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," arXiv preprint arXiv:1212.1984, 2012.
[3] C. Dwork, "Differential privacy: A survey of results," in International Conference on Theory and Applications of Models of Computation, Xi'an, China, April 2008.
[4] J. K. Rao, "Small area estimation," Wiley StatsRef: Statistics Reference Online, 2014.
[5] Z. Yang, Z. Zeng, K. Wang, S.-S. Wong, W. Liang, M. Zanin, P. Liu, X. Cao, Z. Gao, Z. Mai, J. Liang, X. Liu, S. Li, Y. Li, F. Ye, W. Guan, Y. Yang, F. Li, S. Luo, Y. Xie, B. Liu, Z. Wang, S. Zhang, Y. Wang, N. Zhong, and J. He, "Modified SEIR

and AI prediction of the epidemics trend of COVID-19 in China under public health interventions," Journal of Thoracic Disease, vol. 12, no. 3, 2020.
[6] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019.
[7] "Demystdata: Covid-19," https://www.snowflake.com/datasets/demystdata-covid-19, Accessed October, 2020.
[8] "Harris county houston COVID-19 cases," https://publichealth.harriscountytx.gov/Resources/2019-Novel-Coronavirus, Accessed October, 2020.

Security and Privacy-aware Mobile Healthcare Framework During COVID-19-like Pandemic

Shaik Shakeel Ahamad[1] and Al-Sakib Khan Pathan[2]
[1] College of Computer and Information Sciences, Majmaah University, Al Majmaah, Kingdom of Saudi Arabia
[2] Department of Computer Science and Engineering, Independent University, Dhaka, Bangladesh
[1] s.ahamad@mu.edu.sa , [1] ahamadss786@gmail.com , and [2] sakib.pathan@gmail.com

Abstract
Existing schemes in the realm of mobile healthcare (also, e-Healthcare) based on cloud and IoMT (Internet of Medical Things) do not ensure end-to-end security and are not compliant with HIPAA (Health Insurance Portability and Accountability Act). It is also very difficult often for these schemes to obtain evidence from the cloud in case of security breaches. In addition to these issues, mobile healthcare applications are prone to various types of attacks and formal proof is often unavailable. In this work, we propose a framework in community cloud in an IoMT setting that ensures end-to-end security and circumvents many of the existing negative aspects using Trusted Platform Module (TPM). For this project, we would provide necessary proofs using BAN logic and Scyther tool. Also, we would show that the energy consumption and the costs of communication and computation for our proposed protocol are far less than that of the existing protocols. The protocol has been implemented using Kotlin language in Android Studio ensuring all the security properties.

1. Introduction
The exponential growth of IoT-enabled (Internet of Things-enabled) wearable devices such as smart medical sensors and healthcare management software has led to the revolution of collecting and storing healthcare data. Nowadays, we see a trend of increased use of IT (Information Technology) facilities and cyberspace. As one of the prominent technologies today, cloud computing also plays a vital role in some mobile healthcare systems. There is an expectation that this trend would grow fast in the coming days contributing to the field of IoMT in general. In fact, during recent outbreak of COVID-19 pandemic [1], the necessity of IoMT for remote healthcare services has significantly been realized.

As part of IoMT [2], cloud computing is linked with the healthcare system; stored data could be sent to the hospitals and the doctors quickly from external storage. While using cloud can reduce the burden of a hospital to possess its own data storage facility and strong IT infrastructure, in such a setting, ensuring security and privacy of data would be quite difficult given the nature of cloud (as a third-party facility) and the overall communication and networking settings of IoMT. Security is basically considered a major challenge for wide-spread adoption of cloud technology or IoMT technology [3] for mobile- or e-healthcare.

Medical data are often very sensitive and need to be protected maintaining some standard. For instance, to regulate healthcare industry, the US government introduced Health Insurance Portability and Accountability Act (HIPAA) (HIPAA, 2020). This was enacted to set some storage regulations and ensure sensitive medical data privacy to protect individuals covered by health insurance. While some legislated standards can ensure personal data privacy, often new technologies attract people, and when those are tried or tested (for practical implementation), there could be possibilities of violating standard terms. Many healthcare industries are not prepared for the new cyber age (Healthcare, 2020). Fraud and identity theft in the healthcare sector have been on the exponential rise [4], just like in many other systems that take advantage of IT and cyber technologies today. ABI Research report [4] states that it is evident that the healthcare industry is adopting cloud technologies very swiftly and by the end of 2020, 80% of healthcare data might be stored at the cloud. Hence, in addition to its existing security challenges, healthcare industry has to cope with the security challenges of the cloud. At a minimum, the mobile healthcare industry should comply with HIPAA standards that regulate data privacy for personal healthcare information.

2. Novelty and Contribution of the Project

The novelty and contribution of this work are as follows:

a) Our mobile healthcare framework ensures end-to-end security and overcomes the flaws in the existing literature.
b) The mobile healthcare framework complies with HIPAA regulations.
c) We are the first to propose a secure mobile healthcare framework using a community cloud and capable of collecting and preserving evidence (in case of security breaches) using the transaction log, counters, forensics method, and cryptographic audit log techniques.
d) We are the first to implement our protocol in real-time using *Kotlin* language in Android Studio.
e) Formal verification of our mobile healthcare protocol was successful using BAN logic [5], [6], and Scyther tool [7].
a) Finally, our proposed protocol's energy consumption, communication, and computation costs are far less than that of the existing protocols.

We name our mechanism, Security and Privacy-aware Mobile Healthcare Framework (SPMHF). Following sections elaborate the project's various aspects.

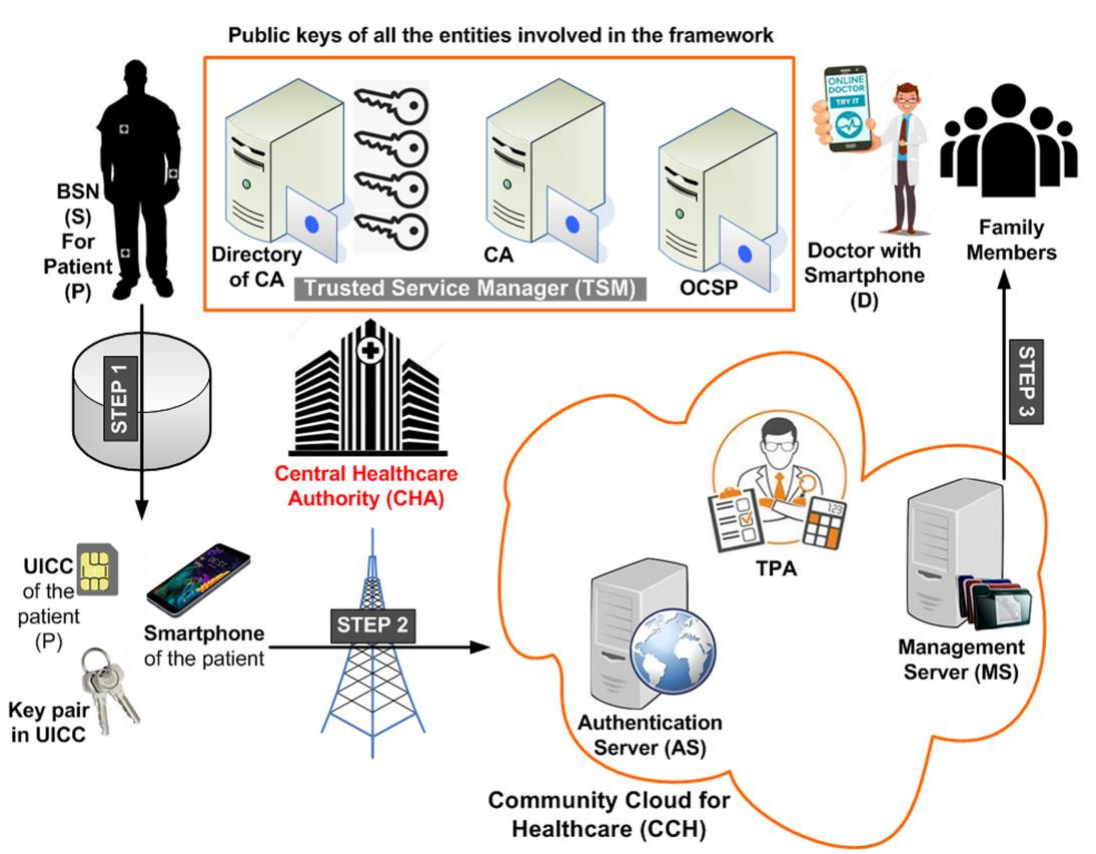

Figure 1. Security and Privacy-aware Mobile Healthcare Framework (SPMHF).

3. SPMHF for COVID-19-like Pandemic Situation

Following are the major entities involved:

- Body Area Sensor Network (BSN). Here is the Sensor (S).
- Healthcare Application in BSN.
- Universal Integrated Circuit Card (UICC) in Smartphone.
- Healthcare Application in UICC.
- Central Healthcare Authority (CHA).
- Certifying Authority Cloud (CAC).
- Doctor (D).
- Patient (P) and Family (individuals).
- Community Cloud for Healthcare (CCH).

As reported in various reliable sources from the medical community, due to the nature of the COVID-19, it is classified as *highly contagious*. In such case or similar disease condition, when a patient needs emergency treatment or in the ICU (Intensive Care Unit), various types of bodily conditions need to be

measured like low oxygen level in blood or hypoxia, high temperature, irregular pulse or heart rate, and so on. A key requirement is as less physical contact with the patient as possible. Here, BSN could be very useful.

In our setting (see Figure 1), the BSN contains a Secure Element (SE), SE contains a healthcare application which collects the health information (e.g., heart rate, temperature). This BSN healthcare application shares a symmetric key with the Mobile Healthcare Application (MHA) in UICC [8] of the patient's smartphone. Again, this MHA and CCH share symmetric key between them. Both the Patient (P) and Doctor (D) possess mobile phones with UICCs as SEs and they communicate using 4G/5G through Mobile Network Operator (MNO). The MNO also enables Over-The-Air (OTA) connectivity. CCH provides healthcare services to the patients by bringing all hospitals or medical centers in the same cloud. The country's central government would manage CCH and it hosts a Trusted Platform Module (TPM) of all the hospitals (the respective hospitals personalize TPM).

CCH and patients are connected via 4G/5G ensuring communication security using Transport Layer Security (TLS) protocol. Application security is ensured using AES (Advanced Encryption Standard) and ECDSA (Elliptic Curve Digital Signature Algorithm). Certifying Authority (CA) serves as a Trusted Service Manager (TSM) [9] in addition to its usual functions. Community Cloud here is controlled and shared by multiple organizations. Several owners can have some common interest and hence, it could be managed by a committee of owners or a third party - even can be located at a distant place. The legitimate members of the community would be given access to the data in the cloud. Wireless Public Key Infrastructure (WPKI) is implemented in this framework. Healthcare applications in BSN and UICC are personalized by the CCH using OTA. CCH updates the firmware in the SE of BSN and MNO updates the firmware in the UICC.

3.1 Certifying Authority Cloud (CAC)

CA has a cloud with usual functions like issuing certificates, providing directory services, Online Certificate Status Protocol (OCSP), and Certificate Revocation List (CRL).

Registration Authority (RA): CA infrastructure contains this authority for checking the credentials of patients.

Signing Services and Certificate Repository (SSCR): This entity is responsible for generating and signing the certificates.

OCSP: OCSP maintains X.509 certificates; this entity helps verify certificate validity.

TSA: Time Stamping Authority is for timestamping services.

CRL: It maintains the list of revoked certificates.

3.2 Central Healthcare Authority (CHA)

This entity monitors the functions of the hospitals. It also ensures the implementation of HIPAA in hospitals. CHA and CA employ Trusted Party Auditor (TPA) for monitoring the functions of CCH. CHA acts as an adjudicator and TSM. CCH is a subsidiary of CHA and CHA controls TPA.

3.3 Community Cloud for Healthcare (CCH)

The following entities are involved in CCH:

Communication Manager (CM): Information about CCH services, standards of communications, and interfaces used for different devices is kept in it. For encrypted communication, IPSec VPN (Internet Protocol Security Virtual Private Network) is placed at the forefront of medical gateways. To engage in HTTPS (Hypertext Transfer Protocol Secure) communication, SSL (Secure Sockets Layer) protocol is applied for servers at the medical gateways (for web servers).

TPA: This entity is employed by TSM (i.e., CA) and CHA in our framework which monitors the functions of CCH.

WPKI Manager: This is responsible for the lifecycle of stakeholder's certificates, and it takes care of the certificate status and directly contacts with the CA. This entity closely works with PM (Personalization Manager) and CA.

Logging and Monitoring Control Manager (LMCM): It performs anomaly detection using statistical and machine learning (ML) algorithms and identifies traffic variances against pre-defined conditions. Any deviation of a system from standard access control policies could be monitored. Also, various authentication attempts (either passed or failed), management of users, rights management, and so on can be recorded using logs. The items in a log can be:

- User IDs (identities).
- Exact timestamp (date-time) for logging in and logging off.
- Device location that uses the LAN (Local Area Network), ID of access point, or ID of remote-access system.

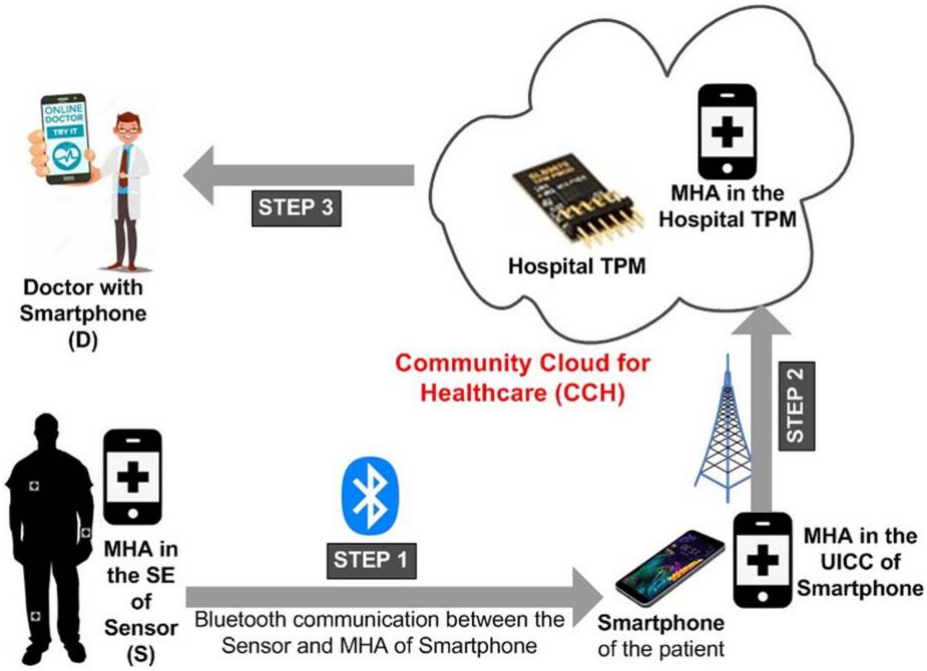

Figure 2. Steps in the Health Monitoring Mechanism.

The hospital TPM contains:

(a) Identity and Access Management (IAM): This entity authenticates IoT devices, IoT Medical Applications (IMA) and Doctor (D) credentials which are issued by TSM, i.e., CA and issues a token which is used to carry out transactions.

(b) Time Stamping Authority (TSA): It offers timestamping services for CCH generated messages.

(c) Personalization Manager (PM): PM is responsible for provisioning and personalizing of the IoT device, IMA, and UICC of the doctor. UICC is the SE in doctor's smartphone.

(d) Evidence Manager (EM): It collects evidences using various audit log techniques. When any dispute arises among the stakeholders, this entity can provide proofs to the court of law.

(e) Patch Management and System Hardening: Applications and OSs are often targeted by various types of attacks on a daily basis. Effective "*Patch Management*" can successfully reduce the risk of compromising systems. *System hardening* process ensures relatively less attack surface of various types of networking devices and applications.

The mechanism has the following phases:

- Doctor Registration Phase
- Customization of Sensor (BSN) Phase
- Healthcare Data Upload Phase
- Customization of Patient's Secure Element Phase
- Customization of MHA Phase

Figure 2 shows the steps in the health monitoring mechanism in this framework.

4. Performance Issues and Implementation

For security analysis we consider the following issues and aspects:

- Accountability
- Personalization of MHA
- Key agreement
- Key freshness
- Repackaging attack
- Security of Keys
- Denial of Service (DoS) attack

- Multi-protocol attack
- Man-In-The-Middle (MITM) attack
- Replay attack
- Impersonation attack
- Parallel Session attack
- Auditing issues
- HIPAA compliance
- Application security
- Physically stolen medical sensor or Node Capture attack
- Key computation
- Privileged Insider attack
- Stolen Verifier attack
- Defense-in-Depth

For performance analysis in terms of computation and communication costs, we would consider some of the representative classical or most recent or the latest alternatives in this arena. As remote healthcare is considered, as noted, by the work's own strength, HIPAA compatibility is a plus point that could put it ahead of other similar works.

We have already implemented a part of our Mobile Healthcare Application (MHA). Our implementation related information and *Kotlin* code can be found at: https://webmah.com/security/mobile-healthcare.zip

5. Conclusion

SPMHF is designed in compliance with HIPAA standard. Given various practical circumstances of COVID-19 pandemic or any other similar situation that may appear in the future, it is a requirement to ensure appropriate level security and privacy for patient's data as well as to develop a mechanism of minimum-contact based remote health monitoring of critical-stage patients. Our framework and protocol could be very effective in this scenario.

References

[1] A.-S.K. Pathan, "Access to information vs blocking of information during COVID-19 pandemic: a governance dilemma in the era of crowdsourcing based on ICT," *International Journal of Computers and Applications*, Taylor & Francis, 2020, DOI: 10.1080/1206212X.2020.1767396.

[2] P. Parthasarathy, and S. Vivekanandan, "A typical IoT architecture-based regular monitoring of arthritis disease using time wrapping algorithm," *International Journal of Computers and Applications*, Taylor & Francis, Volume 42, Issue 3, 2020, pp. 222-232.

[3] R.A. Khan and A.-S.K. Pathan, "The State of the Art Wireless Body Area Sensor Networks – A Survey," *International Journal of Distributed Sensor Networks*, SAGE pub., 14(4), 2018, DOI: 10.1177/1550147718768994.

[4] O. Bay, "Healthcare Cybersecurity a Massive Concern as Spending Set to Reach Only US$10 Billion by 2020," 2015, Retrieved 26 May 2020, from https://www.abiresearch.com/press/healthcare-cybersecurity-a-massive-concern-as-spen/

[5] M. Burrows, M. Abadi, and R. Needham, "A logic of Authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, 1990, pp. 18–36.

[6] M. Abadi, M. Burrows, C. Kaufman, and B. Lampson, "Authentication and delegation with smart-cards," *Science of Computer Programming*, Volume 21, Issue 2, 1993 pp. 93-113.

[7] C.J.F. Cremers, "Scyther - Semantics and Verification of Security Protocols," Ph.D. dissertation, Eindhoven University of Technology, 2006.

[8] S.S. Ahamad, V.N. Sastry, and S.K. Udgata, "Secure mobile payment framework based on UICC with formal verification," *Intl Jrnl of Computational Science and Engineering*, 9(4), Inderscience, 2014, pp. 355-370.

[9] S.S. Ahamad and A.-S.K. Pathan, "Trusted Service Manager (TSM) based Privacy Preserving and Secure Mobile Commerce Framework with Formal Verification," *Complex Adaptive Systems Modeling*, 7:3, Springer Open, 2019.

AI-Backed Decision Support for COVID-19 Mobile Assessments and Supply Services*

Burak Kantarci
University of Ottawa, Canada

Abstract
This project aims at improving response and preparedness against COVID-19 with the following unique, feasible and transformative research objectives: 1) Designing realistic predictive models of community spread through mobility behavior of communities, 2) Development of an AI-empowered preparedness and planning framework against pandemic outbreak on vulnerable regions, 3) Development of AI-backed decision support systems for supply services during the pandemic. The results have been enabling monitoring, modeling and AI-based projections for the deployment of assessment centres alongside the required supply services. Providing AI-empowered digital services to decision makers will enable different levels of governments to make proactive strategies so to facilitate management and logistics.

1. Introduction
Recent pandemic crisis due to COVID-19 outbreak has uncovered two facts: 1) Fragility of supply chains, 2) Vitality of effective strategies for rapid assessments against the outbreak as it is not possible to test the entire population. The project outcomes aim to provide AI-backed software services to maximize the assessed population at risk in the shortest possible time based upon the risk maps and with limited resources. In a situation where citizens are encouraged to self-isolate and minimize their social interactions, the agility of supply chains become vital to provide the medical and essential supplies with optimal strategies. Given these challenges, this project will contribute to COVID-19 research through the field of applied machine learning research by developing innovative methods to predict risk scores of multiple zones. Furthermore, through its industry partnerships with the aforementioned companies, the project is aiming to enable filling in the missing piece required to fully automated the real-time modelling of supply services during the pandemic. Therefore, once completed successfully, the project will contribute to the resolution of COVID-19 crisis through: 1) improved ability to model community spread, 2) fast maximization of the tested (suspected) population, 3) effective use of available assessment equipment, and 4) AI-backed decision support for supply services.

The severity of the newly identified COVID-19 is denoted by its reproduction number (R0), which is between 1.5-2.5 [1]. Thus, an infected individual can infect up to 2.5 other individuals on the average. This makes manageability a major implication of this pandemic as hospital surge capacities are expected to be hit by the disease [2] while supply chains become extremely fragile [3]. As forecast by multiple authorities, the earliest time with the most optimistic assumptions to be able to immunize the World's entire population against COVID-19 will be in Spring 2021. Besides the medical practice for treatment and immunization, it is vital to have a thorough understanding of the community spread phenomena as related research reports 17.9%-30.8% confirmed cases to remain asymptomatic. Therefore, an effective assessment strategy is vital to maximize tested population in a short amount of time, and strategists call for preventive and proactive strategies to cope with COVID-19.

* *This newsletter article reports the ongoing project titled is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) under the Alliance Program under Grant Number ALLRP 552696-2020. Principal Investigator: Burak Kantarci. Partner Organizations, Gnowit Inc., Lytica Inc.*

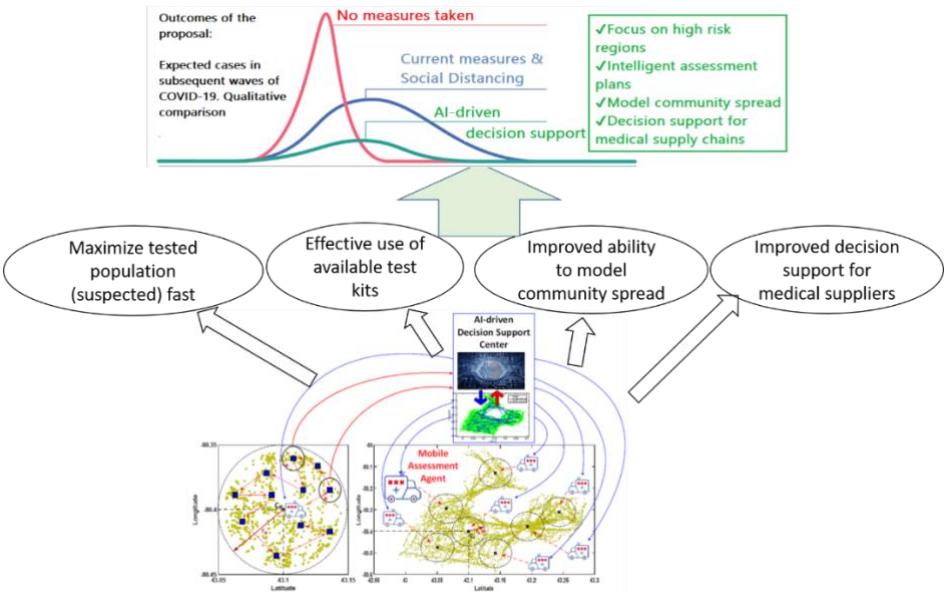

Figure 1. Minimalist illustration of the project and expected outcomes

As illustrated in Figure 1, the project incorporates predictive models for the outbreak based on behavioral patterns obtained from sensory data so to obtain vulnerability and risk scores of the monitored regions. The outcomes will enable monitoring, modeling and AI-based projections for the deployment of assessment centres alongside the required medical supplies.

2. Background and State of the Art

Existing studies and related research uses AI to address problems concerning public health and well being. For instance, diagnosis of infectious diseases, as well as response to treatment is modeled by using AI techniques [4]. Another problem where researchers employ AI techniques is the modeling of epidemics with high precision through neural networks [5]. The closest research to this proposal contains two efforts: modeling the social contact network in Delhi with the objective of planning public sector and health resources under pandemic [6], and a machine learning-based model to optimize the use of public resources with high precision in an upcoming influenza pandemic [7]. However, even the closest research remains reactive and relies on the data obtained from the previous pandemic. Thus, the project is introducing a globally unique approach through an AI-backed proactive strategy to suppress the curve based on the current modeling of communities whereas the existing research relies on data obtained from assessed cases on symptomatic patients in former epidemic/pandemic cases.

Existing strategies for public preparedness are based on massive assessment plans [8], and these plans translate into cost benefits [9]. Indeed, preparedness entails many aspects, from modelling of outbreaks to decisions concerning logistics and mobilization.

3. Latest contributions of the project

Since some of the infected individuals can be asymptomatic which means up to 30% positive-tested cases for Covid-19 are not realized without testing [10] collecting mobility patterns of individuals in certain regions should be considered as critical for monitoring the community spread of Covid-19 like pandemics and taking effective actions against them. Earlier in May, we used mobile Crowdsensing data for early detection of Covid-19 cases through a self organizing feature map (SOFM) [11]. In that study, once mobile assessment centers had been assigned to the selected region; each stop of each mobile assessment center were planned by SOFM. More specifically, the worst-case scenario was considered for early detection of infected cases in the region. The general framework of Artificial Intelligence (AI)-based deployment and route planning decision for mobile assessment center consists of two steps. The first step is self organizing feature map (SOFM)-based region selection and the second step is SOFM-based mobility decision. Under the worst-case scenario, the research has proven that the minimum number of neurons (i.e., stops) for SOFM (mobile assessment agents) can be achieved on the 15th day following the occurrence of the first confirmed case to be able to detect and isolate all infected

individuals whereas the random deployment under the same number of stops over multiple districts fail to detect all cases and leads to non-assessed population remain quadruplicated.

Following upon this work, the project has tackled the problem of community risk mapping via MCS data in [12]. The project presented an MCS-driven community risk modeling solution against a pandemic supported by mobile smart device users, who opt-in to crowdsensing campaigns and grant access to their mobile device's built-in sensors (including GPS). The MCS platform keeps track of the mobility patterns of the participants and utilizes unsupervised machine learning (ML) algorithms. Fig.2 presents the building blocks of this community risk mapping scheme in four pieces.

The first building block denotes a standard data acquisition procedure in an MCS campaign. The second step involves dimensionality reduction to enable intuitive visualization of mobility patterns on a 2D-plot. The reduced dimensions are fed into an unsupervised machine learning algorithm to detect clusters within the acquired data where each cluster stands for a community in the monitored region. In the third step, spatio-temporal behavior of MCS participants reveal changes in their geo-coordinates in time so to reveal clusters (i.e., communities) such that the estimated risk of community spread in each cluster can be computed via predicted future coordinates of the users.

Through numerical results from simulating a metropolitan area (e.g., Paris), it is shown that communities' COVID-19 risk scores at the end of a set of MCS campaign has been shown to be predicted 20% ahead of time (i.e., upon completion of 80% of the MCS time commitments) with a dependability score up to 0.96 and an average of 0.93. Further tests with a larger population of participants show that community risk scores can be predicted 20% ahead of time with a dependability score up to 0.99 and an average of 0.98.

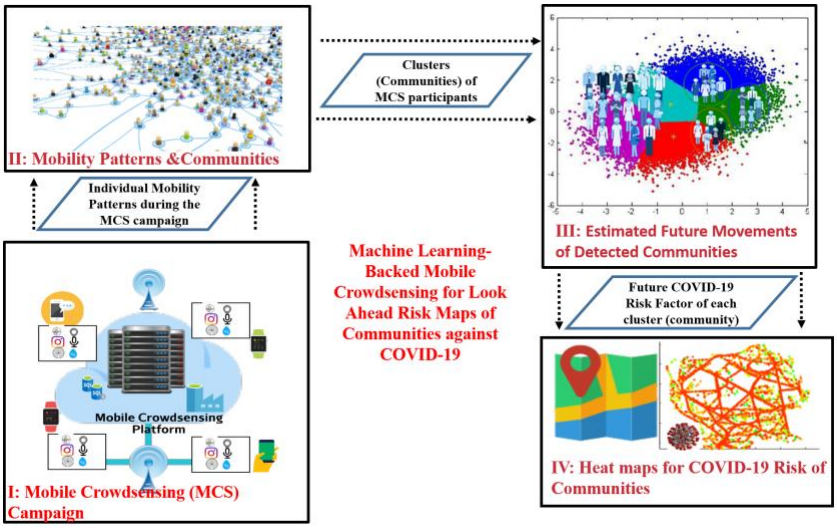

Figure 2. Minimalist illustration of the proposed COVID-19 community risk mapping via MCS [12]

4. Concluding remarks, ongoing Research, open issues and challenges

Recent pandemic crisis due to COVID-19 outbreak has uncovered two facts: 1) Fragility of supply chains, 2) Vitality of effective strategies for rapid assessments against the outbreak as it is not possible to test the entire population. According to Public Health data in Canada, 30 days after the state of emergency, 503,003 people were tested, and confirmed cases were 31,407. However, quoting public health officials, the numbers representing the positive cases are the "tip of the iceberg" as a large fraction of individuals are estimated to be infected, remain asymptomatic and causing to transmit the disease to healthy individuals. With this in mind, we have so far developed proactive mobile assessment strategies for potentially asymptomatic individuals. Furthermore, we have developed a mobile crowdsensing-based risk mapping for communities. Results of the projects are being updated on an ongoing basis on the Covid-19 section of the Next Generation Communications and Computing Networks (NEXTCON) Laboratory's web site (http://nextconlab.academy/covid19.html).

MCS-based COVID-19 risk mapping of communities builds on the assumption that MCS data can always be acquired ubiquitously. However, some MCS campaigns may not require a large pool of recruited participants for various reasons. Therefore, when data is scarce, the framework developed in this project is expected to augment MCS data with other data sources. City infrastructures host various types of dedicated sensors that can provide useful data, including images and traffic data, which can improve MCS-based community risk modeling accuracy. This approach will require the integration of sensor fusion with machine/deep-learning-based context recognition techniques.

The project has so far presented a look ahead community risk mapping based on the mobility behavior and distances between the members of detected communities. However, quantification of the COVID-19 risk can be made more precise by integrating the MCS-based risk maps with epidemic models.

Acknowledgements: This newsletter article has been prepared by compiling the most recent research results disseminated in peer-reviewed venues. Current research activities are continuing in collaboration with Murat Simsek (Research Assoc, Univ. of Ottawa), Azzedine Boukerche (Collaborator, Univ. of Ottawa), Damla Turgut (Collaborator, Univ. of Central Florida), Shahzad Khan (Gnowit Inc.), and Sedevizo Kielienyu (Grad. student, Univ. of Ottawa).

References

[1] Shim, E.; Tariq, A.; Choi, W.; Lee, Y.; Chowell, G. Transmission potential and severity of COVID-19 in South Korea. International Journal of Infectious Diseases 2020.

[2] Woodul, R.L.; Delamater, P.L.; Emch, M. Hospital surge capacity for an influenza pandemic in the triangle region of North Carolina. Spatial and Spatio-temporal Epidemiology 2019, 30, 100285.

[3] Ivanov, D. Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case. Transportation Research Part E: Logistics and Transportation Review 2020, 136, 101922.

[4] Agrebi, S.; Larbi, A. Chapter 18 - Use of artificial intelligence in infectious diseases. In Artificial Intelligence in Precision Health; Barh, D., Ed.; Academic Press, 2020; pp. 415 – 438.

[5] Jiang, D.; Hao, M.; Ding, F.; Fu, J.; Li, M. Mapping the transmission risk of Zika virus using machine learning models. Acta Tropica 2018, 185, 391 – 399.

[6] Xia, H.; Nagaraj, K.; Chen, J.; Marathe, M.V. Synthesis of a high resolution social contact network for Delhi with application to pandemic planning. Artificial Intelligence in Medicine 2015, 65, 113 – 130. Intelligent healthcare informatics in big data era.

[7] Nieto-Chaupis, H. Face To Face with Next Flu Pandemic with aWiener-Series-Based Machine Learning: Fast Decisions to Tackle Rapid Spread. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0654–0658.

[8] Hsih,W.H.; Cheng, M.Y.; Ho, M.W.; Chou, C.H.; Lin, P.C.; Chi, C.Y.; Liao,W.C.; Chen, C.Y.; Leong, L.Y.; Tien, N.; Lai, H.C.; Lai, Y.C.; Lu, M.C. Featuring COVID-19 cases via screening symptomatic patients with epidemiologic link during flu season in a medical center of central Taiwan. Journal of Microbiology, Immunology and Infection 2020.

[9] Panovska-Griffiths, J.; Grieco, L.; van Leeuwen, E.; Grove, P.; Utley, M. A method for evaluating the cost-benefit of different preparedness planning policies against pandemic influenza. MethodsX 2020, p. 100870.

[10] H. Nishiura, T. Kobayashi, A. Suzuki, S.-M. Jung, K. Hayashi, R. Kinoshita, Y. Yang, B. Yuan, A. R. Akhmetzhanov, N. M. Linton, and T. Miyama, "Estimation of the asymptomatic ratio of novel coronavirus infections (covid-19)," Int. Journal of Infectious Diseases, 2020.

[11] Simsek, M.; Kantarci, B. Artificial Intelligence-Empowered Mobilization of Assessments in COVID-19-like Pandemics: A Case Study for Early Flattening of the Curve. Int. J. Environ. Res. Public Health 2020, 17, 3437.

[12] Sedevizo Kielienyu, Burak Kantarci, Damla Turgut, and Shahzad Khan. 2020. Bridging Predictive Analytics and Mobile Crowdsensing for Future Risk Maps of Communities Against COVID-19. In Proceedings of the 18th ACM Symposium on Mobility Management and Wireless Access (MobiWac '20). Association for Computing Machinery, New York, NY, USA, 37–45.