electronics

MDPI

Article

A Public Platform for Virtual IoT-Based Monitoring and Tracking of COVID-19

Younchan Jung * and Ronnel Agulto

School of Information, Communications and Electronics Engineering, The Catholic University of Korea, 43 Jibong-ro, Bucheon-si 14662, Gyeonggi-do, Korea; ronnelagulto@catholic.ac.kr
* Correspondence: ycjung@catholic.ac.kr; Tel.: +82-2-2164-4364

Abstract: The world is developing an app that alerts my smartphone when a COVID-19 (COrona VIrus Disease 19) confirmed case comes near me. However, regardless of what will be put to practical use first, the COVID-19 tracking system should satisfy the issues of legalization of location tracking and scalability as a public platform used by the world. Additional problems need solutions related to real-time authentication for information gathering, blind naming and privacy of tracked persons, and quality of service on the Query/Reply procedure. This paper proposes the Software-Defined Networking Controller-centric global public platform to monitor and track information for the COVID-19 relevant people and provide real-time information disclosure services to world-wide Centers for Disease Control and Prevention (CDCs) and regular users. The CDC manages a list of people who needs to be monitored related to the COVID-19 and forcibly installs COVID-19 virtual Internet of Things (vIoT) nodes in the form of applications on their smartphones. In addition to these nodes, the vIoT support nodes also engage as information providers to improve the quality of information services. The design of our platform aims to ensure confidentiality and authentication services giving individually different secret keys. In addition, our platform meets system scalability and reduces Query/Reply latency, where the platform accommodates a large number of world-wide CDCs and persons in control per CDC.

Keywords: COVID-19; tracking; public platform; virtual IoT; CDC

Citation: Jung, Y.; Agulto, R. A Public Platform for Virtual IoT-Based Monitoring and Tracking of COVID-19. *Electronics* **2021**, *10*, 12. https://dx.doi.org/

Received: 20 November 2020
Accepted: 16 December 2020
Published: 23 December 2020

1. Introduction

The world is now developing an app that alerts my smartphone when a COVID-19 (COrona VIrus Disease 19) confirmed case comes within 5 m of me. This application can use the technology of either the distributed method or the centralized method.

It is not difficult to participate in a distributed warning network. First, let us look at the distributed method. Placing this decentralized application on my smartphone means that I am participating as a member of the distributed warning network as a node. Download one of the distributed warning network software packages via the web, install the program, find and connect to at least one other node belonging to this network group, and become a member node of the group. Suppose that my smartphone has joined as a configuration node of the distributed warning network as node A. To see if there are any COVID-19 confirmed cases around me, hit the "corona" keyword, and my current location and corona keyword information. Then, Node A sends the "Query" message to the nearest neighbor node. Upon receiving this message, the neighbor node first searches through the information it is holding, then informs Node A of the corresponding one, if any, and then sends the "Query" request to another node. This "Query" message spreads as the wave spreads by repeating the same process for the node receiving this. As a result, only one "Query" message can quickly spread to thousands of smartphones, Any node that receives the replied information about the presence of a COVID-19 confirmed case informs Node A of this information. Then, anyone can use the information that other people know

and store as my information when I need it. The key here is how to handle the source of information. A person who is a COVID-19 confirmed case who informs himself of his location has a problem participating in this distributed warning network and acting as a source information provider [1,2].

On the other hand, the operation of the centralized application is smooth [3,4]. In particular, it is easy for the government to manage. A large computer in the center keeps track of all COVID-19 confirmed cases and their current location. If a person wants it, the central computer is ready to provide the information in the form of a client-server type of web service. It has the advantage for the centralized application to establish a database dealing with the centrally forced COVID-19 confirmed case list and their current location information. However, privacy concerns link to the bigger problem. The centralized approach has to solve the privacy problem.

Apple (AAPL) and Google (GOOGL) are jointly developing this app, which seems to prefer a distributed method [5].

Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) is said to have already developed a centralized approach [6]. We will see what will be put to practical use first.

This paper places a point on the following seven issues to develop the world-wide public service system of the COVID-19 relevant information that the ordinary users, as well as Center for Disease Control and Prevention (CDC) institutions, use together.

- Legalization of location tracking: South Korea's large-scale diagnosis of COVID-19 suspects and the unveiling of a full moving line of COVID-19 confirmed cases surprised world health experts [7,8]. In 2015, after the Mers (Middle east respiratory syndrome) crisis, South Korea institutionalized tracking the path of the infected [9]. Since then, it is now possible for health authorities to use location information without their consent, if necessary, for preventing infection. It is essential to establish a location tracking system based on the safety plates to track the suspected legally. This paper is based on the following legal aspects: the Center for Disease Control and Prevention (CDC) manages a list of people who needs to be monitored related to the COVID-19 and forcibly installs virtual Internet of Things (vIoT) nodes in the form of applications on their smartphones.
- Public platforms used by the world: In the unpredictable circumstances of COVID-19's cause and development, organizations operating under secret central control, which hides some information, have exposed instability and failed to help overcome the COVID-19 crisis. Secrecy and authoritarianism may be useful in preventing the explosive distribution of false information, but they cannot contribute to the spread of viruses effectively. Therefore, transparent and open CDCs should manage infected suspects. However, they still make their tracking information public locally and individually. Consequently, it is necessary to build a global public platform that can capture them.
- Real-time authentication and reliability of information: Even though Singapore and Hong Kong announced fewer than 100 COVID-19 confirmed cases, there was civil unrest. However, there have been no such situations in South Korea despite a surge in confirmed numbers. South Korea had maintained stable social functions even when the number of infected people reached their peak. The reason for this is that South Korea's Director of Disease Control and Health Authorities have given them a detailed and transparent briefing on the information, giving them confidence that they are in control of the situation. However, they gave intelligence briefings once every 24 h as frequently as they can. The background of releasing information every 24 h is the product of the era of offline newspapers. Information should be collected immediately on an online basis. When ordinary users request the information they need, they should receive the disclosure service of that information as fast as possible. For these services to be successful, the information collection and this authentication should occur at the same time. In addition, the reliability of the newly collected information must be able to be proven in real-time.

- Blind naming of infected persons: The real-time tracking of confirmed cases and suspected infections is possible now because everyone has a smartphone connected to the Internet. However, their personal information should be protected thoroughly. A different approach to naming is necessary [10,11]. The authority responsible for tracking them can give each of them a different conceptual identifier that is the same as a number assigned to the Internet of Things device. This blind id enables one to prevent hackers from inferring the identity information corresponding to this number, even if they secretly obtain this identifier number.
- Confidentiality: The privacy information of the confirmed cases, person suspected of infection, or person in need of management should be encrypted and stored using a secret key that is granted separately for each individual. With a large number of CDCs distributed around the world and enough people to manage per CDC, the platform should provide a security management service that allows individuals to use different secret keys for each individual [1,12–14].
- Scalability: The platform should provide real-time disclosure services for the COVID-19-related tracking information to any CDC and anyone in the world in the same way as a DNS (Domain Name System) provides name-address conversion services in HTTP communications in real-time. It is a prerequisite that the platform should be able to accommodate enough people to manage per CDC as well as a large number of CDCs distributed around the world. So, the data structure that the platform handles must be concise and straightforward so that the scalability of the system can be satisfied [15].
- Latency: Currently, the person gets to figure global COVID-19 cases out based on data provided by the World Health Organization (WHO). In addition, they usually get to know Global COVID-19 case trends based on WHO data. However, it takes time for the WHO to gather reliable, comprehensive data. It should also go beyond the official statistical data presentation method. It is necessary to send a query on an individual basis and receive a reply to the information service in real-time. The time it takes to complete the Query/Reply process in a global public service must be faster to satisfy the Quality of Service to the users [16].

This paper proposes the SDNC (Software-Defined Networking Controller)-centric global public platform to monitor and track information for the COVID-19 relevant people who are infected and suspected and provide real-time information disclosure services to world-wide CDCs and regular users. The design of our platform aims to ensure confidentiality and authentication services using individually different Diffie–Hellman (DH) secret keys for real-time information delivery. This paper argues that the world must use the same platform. This paper also seeks to satisfy system scalability and reduce Query/Reply latency where the platform accommodates a large number of world-wide CDCs and persons in control per CDC.

The rest of this paper is organized as follows. Section 2 introduces related works. Section 3 explains the proposed platform architecture with vIoTs, CDCs, and SDNC. In Section 4, this paper explains SDNC-centric tracking and real-time information services which the platform provides. Section 5 discusses how the proposed platform satisfies the seven issues addressed in the introduction section. This paper concludes in Section 6.

2. Related Works

Knowledge of the quantity and quality of apps related to coronavirus disease (COVID-19) is lacking. [17] performed an observational, cross-sectional, descriptive study of all smartphone apps associated with COVID-19. Between 27 April and 2 May 2020, they searched the App Store (iOS) and Google Play Store (Android) for COVID-19 apps. The searched data were classified into the following categories: news, general information, self-diagnosis, contact tracing, notices to contacts, notification of close cases, awareness, helplines, monitoring of clinical parameters, recording of symptoms and treatment, and messaging with health care professionals. They concluded that the apps' most common purposes are providing information on the numbers of infected, recovered, and deceased

patients, recording symptoms, and contacting tracing rather than real-time tracking and monitoring COVID-19 cases.

Center for health security at Johns Hopkins announced a national plan to save lives, reduce COVID-19's burden on our healthcare system, ease strict social distancing measures, and confidently make progress toward returning to work and school [18]. They suggested that the United States must implement a robust and comprehensive system to identify all COVID-19 cases and trace all close contacts of each identified case. According to their estimation, if one person spreads the virus to three others, that first positive case can turn into more than 59,000 cases in 10 rounds of infections. COVID-19 is already spreading through communities across the United States. Therefore, a case-based intervention approach will be impossible to achieve for COVID-19 without a new national initiative that combines a massive expansion of rapid diagnostic tests with the adoption of new technologies to case identification and contact tracing in each state. To manage COVID-19 epidemics from now on, communities in the United States need:

- Rapid diagnostic tests for all symptomatic cases or those with reasonable suspicion of COVID-19 exposure.
- The ability to trace all contacts of reported cases.

To accomplish this goal requires actions that the federal, state, and local governments and other organizations must take to stand up for these capabilities as quickly as possible. Moreover, the second solution to monitoring and tracking issue is urgent.

Countries have been employing a variety of means to enable contact tracing. In Israel, legislation was passed to allow the government to track people's mobile-phone data with suspected infection [19]. In South Korea, the government has maintained a public database of known patients, including information about their age, gender, occupation, and travel routes [20]. In Taiwan, medical institutions were given access to patients' travel histories [21], and authorities track phone location data for anyone under quarantine [22]. Furthermore, on 20 March 2020, the Singaporean government released a mobile phone app, TraceTogether, designed to help health officials track down exposures after an infected individual is identified. However, there are important privacy implications of the existence of such tracking apps. While Singapore's TraceTogether app protects users' privacy from each other, it has serious privacy concerns concerning the government's access to the data. This document discusses these privacy issues [23]:

- Appropriate privacy tradeoffs can be obtained so that people can be willing to endure for the sake of public health.
- With sufficient computational resources and the use of cryptographic protocols, app-based contact tracing can be accomplished without completely sacrificing privacy.

This application's use is limited because it relies on direct contact tracing using Bluetooth proximity networks without using any location data. Even though they begin to use private messaging systems, increasing privacy remains as future work. They agree that there is a long way to adopt a contact tracing app globally. For example, the scalability of the data structures used in the servers may become a major issue when the number of infected individuals and public users rises.

The tracking system can use blockchain-based Ethereum smart contracts and oracles to track reported data related to the number of new cases, deaths, and recovered cases obtained from trusted sources [24]. Numbers such as positive and negative tests, patients hospitalized, deaths, hospital beds occupied, ventilator shortfalls, etc. allow the officials and public to track the progress of COVID-19 in real-time. However, these numbers pose a major problem as decisions based on such data are often imperfect and incomplete. Thus, tracking apps' introduction becomes necessary and valuable to prevent the spread of this virus and maintain data quality and integrity. Furthermore, tracking valid data is vital to monitor the progress of the pandemic. Tech giants, researchers, and healthcare officials started using contact-tracing mobile apps that use Bluetooth-based proximity tracing or geolocation tracking functionality to track COVID-19 cases [25,26]. However, data

available online may not be perfect as it is susceptible to data manipulation. They argue that blockchain technology can revolutionize the way to track COVID-19 cases. They focus on the benefits of implementing a blockchain-based solution over a traditional centralized solution in various aspects, including data handling, quality assurance, fault tolerance, etc. It introduces immutability and data provenance while removing a single point of failure in the system. Even though blockchain has great potential in combating the COVID-19 outbreak, a critical challenge must be considered. The tracking data traffic becomes bulky as the number of transactions increases every day. Every node on the blockchain has to store all validated transactions, and this becomes an obstacle as there is a restriction on the block size and time interval used to create a new block. Current blockchain platforms process only a few transactions per second, which becomes problematic as millions of transactions are needed to be processed in real-time. Since the block size is limited, this causes some transactions to be delayed so much. As a result, this latency issue makes the blockchain-based tracking platform not suitable from the viewpoints of scalability and latency.

The latency issue makes it difficult to realize the blockchain-based tracking platform. In addition, blockchains demand high bandwidth and expensive computational power. Therefore, blockchains are not completely suitable for most resource-constrained IoT devices meant for smart cities. However, a blockchain-based solution has been tried to solve the security and privacy problems of medical data. A modified blockchain model was proposed suitable for IoT devices to rely on its distributed nature and other additional privacy and security properties of the blockchain network [27]. That solution makes IoT application data and transactions more secure and anonymous over a blockchain-based network. Blockchain can help create a single database to collect data during clinical trials and allow patients' data security. In [28], they combine the Internet of Medical Devices (IoMT) applications and blockchain technology in healthcare for patients' data analysis and research about adequate medication. A remote patient monitoring system using IoT devices has been proposed [29]. The paper presents the benefits and practical obstacles to blockchain-based security approaches focused on IoT and remote patient monitoring.

In [30], they present a holistic vision of IoT-enabled smart communities utilizing various IoT devices, applications, and relevant technologies, which have the potential to be a breakthrough in efforts to control and fight against the current pandemic situation. IoT is an emerging field of research, along with the ubiquitous availability of smart technologies, as well as increased risks of infectious disease spread through the globalization and interconnection of the world necessitates its use for predicting, From the perspective of monitoring and tracking to prevent COVID-19, their design is limited to implement a Remote Patient Monitoring (RPM) use case within the E-Health domain very relevant to COVID-19 patients in home isolation and enforcing the quarantine. It is expected that smart cities and Intelligent Transportation System (ITS) technology will host a range of data-driven services together with deployed sensors to assist in the early detection of such COVID-19 outbreaks [31]. This article focuses on proposing a novel architecture and several use-cases that can be developed to create a smart city and ITS inspired data-driven system, which can be used to effectively and timely enforce social distancing community measures and optimize the use of resources in critical situations.

Compared to several existing approaches to using technology to control the spread of COVID-19, this paper's scope is as follows.

- We design a global platform focusing on monitoring and tracking to prevent COVID-19.
- A virtual Internet of Things (vIoT) node can be a confirmed case or a suspected infection.
- CDC forcibly installs virtual vIoT nodes in the form of applications on their smartphones.
- CDC controls the vIoT nodes for a list of people who need monitoring and tracking in its control range.

- SDNC is a centralized center that collects location-related information sent from vIoT nodes under all the distributed CDCs' control.
- Each vIoT node is responsible for updating location-related information into SDNC.
- An individual vIoT's secret key is created and provided by its CDC.
- Each vIoT node uses the secret key to update location-related information to SDNC.
- SDNC generates and uses the secret key in real-time when it receives the update message.
- CDC can monitor the location-related information about the vIoT nodes under its control.
- Unlike vIoT nodes, the ordinary user can obtain limited information from the SNDC without a secret key.
- An ordinary user can reach SDNC and obtain necessary information except for privacy-related data even though the user does not maintain any security associations

3. Platform Architecture with vIoTs, CDCs and SDNC

One of the key ideas of this paper is to solve how all COVID-19 information providers operate with different secret keys. The platform participants are vIoT, CDC, SDNC, and information consumers (ordinary users). This platform consists of vIoT participating as an information provider, the CDC assisting in maintaining a link between VIoT and SDNC, and the SDNC, which provides means to allow information consumers to receive information provided by the information provider in real-time.

3.1. Basics of the Proposed Security Management

Privacy of personal information is an essential factor in the public platform. An individual vIoT's secret key is created and provided by its CDC. Each vIoT node uses the secret key to update location-related information to SDNC. Then, SDNC generates and uses the secret key in real time whenever it receives this update. The SDNC has security association information for each CDC to create a volume of DH keys requested by the CDC. Therefore, the CDC can monitor the RR information about the vIoT nodes under its control. Unlike vIoT nodes, the ordinary user can obtain limited information from the SNDC without a secret key.

Suppose the CDC and SDNC wish to exchange a group of keys. Here, the total number of secret keys is equal to the number of people the CDC needs to manage. CDC selects N random integers, that is, Secret Value Table (SVT) $[X_{D,1}, X_{D,2}, X_{D,2}, \cdots, X_{D,N}]$ and computes N corresponding blind values, that is, Blind Value Table (BVT) $[Y_{D,1}, Y_{D,2}, Y_{D,2}, \cdots, Y_{D,N}]$ where $Y_{D,i} = \alpha^{X_{D,i}} \ mod \ q, i = 1, 2, 3, \cdots, N$. In the DH cryptography system, a set of global public elements includes a large prime number of q and α integer, which is the primitive root of q. Each CDC uses a set of different global parameters for the DH key exchange. The secret key can be any value within the range $[1, q-1]$. Assuming that Advanced Encryption Standard (AES) is used for the symmetric encryption algorithm, the size of the prime number q needs to be as much as 128 bits. Similarly, the SDNC independently selects N random integers, that is, SVT $[X_{S,1}, X_{S,2}, S_{D,2}, \cdots, X_{S,N}]$ and computes N corresponding blind values, that is, BVT $[Y_{S,1}, Y_{S,2}, Y_{S,2}, \cdots, Y_{S,N}]$ where $Y_{S,i} = \alpha^{X_{S,i}} \ mod \ q, i = 1, 2, 3, \cdots, N$. Each side keeps the SVT private and makes the BVT available publicly to the other side. After the mutual exchange of BVTs, the CDC computes the ith DH key as $K_{D,i} = {Y_{S,i}}^{X_{D,i}} \ mod \ q$ and the SDN computes the ith DH key as $K_{S,i} = {Y_{D,i}}^{X_{S,i}} \ mod \ q$. These two calculations produce identical results. All sensitive personal information handled by the SDN platform is encrypted with a DH secret key for the individual. For the ith person who the CDC manage, CDC and vIoT node of the person use $K_{D,i}$ while SDNC uses $K_{S,i}$ for that person. For privacy purposes, both CDC and SDN platform manage COVID-19 relevant persons with the identifier of the CDC-side blind value, that is, $Y_{D,i}$ for the ith person.

3.2. Platform Structure Based on Software-Defined Networking Controller

The CDC manages a list of people who needs to be monitored related to the COVID-19 and forcibly installs vIoT nodes in the form of applications on their smartphones. Then, a vIoT node can be a confirmed case or a suspected infection. Regardless of privacy, this is a social obligation to those who are controlled by the CDC. A large number of CDCs can exist worldwide, and each CDC controls the vIoT nodes for a list of people who need monitoring and tracking in its control range. As shown in Figure 1, for a vIoT node, its wallet maintains two types of records: SA (Security Association) and RR (Resource Record). The SA record, which the CDC provides via offline transmission, contains the same content as the corresponding entry stored in the CDC's SADB. So, the size of the CDC's SADB comes to the total number of people in its control. The RR in the vIoT wallet, which is always up to date, maintains consistency with the corresponding entry stored in the SDNC's RRDB. Then, SDNC is a centralized center that collects RR information from distributed information providers (vIoT nodes) under all the distributed CDCs' control. While each vIoT node is responsible for updating an RR in RRDB at SDNC, an ordinary user can reach the RRDB at SDNC and obtain necessary RRs except for the privacy-related data even though the user does not maintain any security associations.

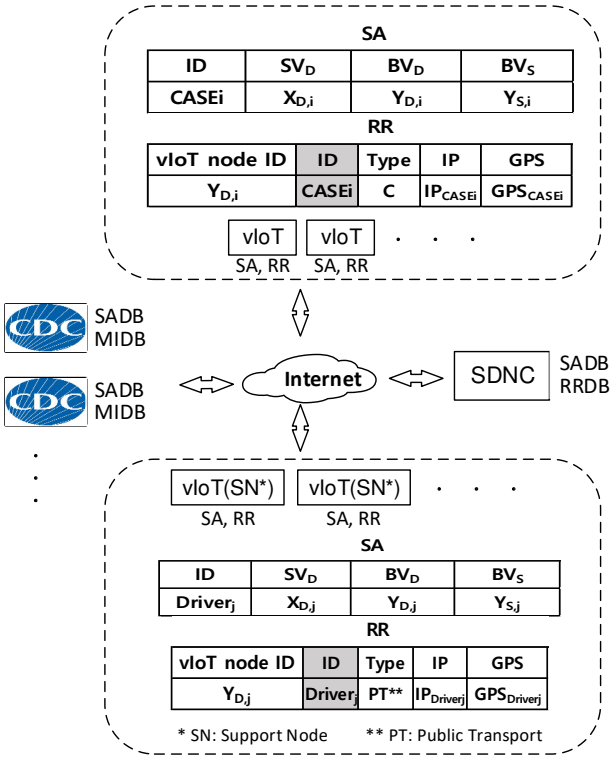

Figure 1. Two different vIoTs as COVID-related nodes and support nodes.

vIoT may operate differently for support purposes. For example, one can take advantage of the VIoT support node in the area of public transport. The CDC requires public transport bus drivers to mount vIoT nodes on the driver's smartphones and establish security relationships in the same way as COVID-related vIoT nodes. At this time, the Type field value of the RR data is PT (Public Transport). Then, whenever the driver drives the bus and changes its location, his location information is reported to the SDNC. If a passenger traveling by bus wants to know whether the COVID-related person is on the bus he or she is riding, they send the query to the SDNC. If there is a COVID person on the bus, SDNC will let the passenger know about this. If no COVID person is on board, the SDNC will also respond to the situation. Of course, suppose the SDNC can search for RR entries

that change in the same pattern as the driver's position information. In that case, it will allow the passenger to see in real-time the COVID-related situation in the moving vehicle.

The tasks performed by the vIoT wallet software usually include:

- Get an SA from its CDC and install it. The CDC is responsible for its revocation.
- Track its location-related status such as current IP address and GPS data when it moves.
- Renew its RR based on the changed location-related status.
- Register the renewed RR to the SDNC immediately in any change of the current RR.

The CDC is usually a national center for disease control and prevention. As indicated in Figure 2, CDC maintains two types of databases: SADB (SA Database) and MIDB (Medical Information Database). The one is for security management, and the other is for managing medical information. In SADB, each entry is an SA containing security variables that enable both CDC and SNDC to compute the same secret key for a certain vIoT. The tasks performed by the CDC software usually include:

- Request to generate all SADB entries at a time to the SDNC. An SA contains Diffie–Hellman (DH) parameters necessary to determine the resultant DH key. The key is applied to encrypt sensitive information in RRs. The field value of "vIoT node ID" identifies each SA.
- Maintain SADB entries that tell which SA to use to apply to decipher an encrypted part of a given RR. An SA specifies the same DH key applied between the CDC and SDNC as well as vIoT and SDNC. The field value of "vIoT node ID" indicates a specific SA among SADB entries.
- Maintain MIDB entries. The field value of "vIoT node ID" identifies the medical status information related to a specific person in need of care. The CDC gives him (or her) a unique management number ("ID") and classes it according to its severity. Each can belong to one of a confirmed case group (C), self-isolation group (S), those who need observation (O). The field of "Type" classifies a specific group. This field also includes PT (Public Transportation) to specify the vIoT support node. People with COVID-19 can experience mild to severe respiratory illness. The field of "Medical information " (*** in Figure 2) can explain COVID-19-related symptoms or combinations of symptoms.
- Query the RRDB in the SDNC and analyze the dynamical behaviors of the people under monitoring.

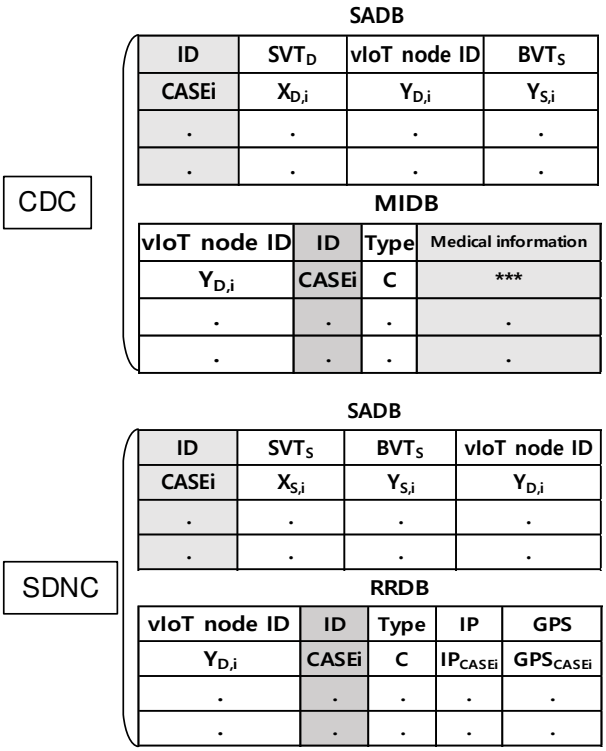

Figure 2. Databases handled by CDC and SDNC.

SDNC (Software-Defined Networking Controller) provides a platform for vIoT nodes, CDCs, and smartphone users. SDNC handles two types of databases: SADB and RRDB. Because SADB in SDNC is associated with that in the CDC, two calculations to generate DH keys in CDC and SDNC produce identical results. It is RR in RRDB that tracks the movement status of each person under monitoring. The field of "ID" keeps encrypted in RRDB with a DH secret key for the individual. The tasks performed by the SDNC software usually include:

- Maintain SADB entries generated as results of BVT exchange procedures initiated by the CDC.
- Calculate the DH key using the SA, which the field value of "vIoT node ID" points out, to encrypt sensitive information in RRs.
- Maintain RRDB entries and updates them when the "Update RR" messages arrive from vIoT nodes.
- Send the corresponding RRs matched after receiving queries from the CDC and normal users, in response.

4. SDNC-Centric Tracking and Real-Time Information Services

The proposed platform is using a centralized approach based on the SDNC. However, from the CDC perspective, it is a decentralized method. This section first offers a way of linking the SADB settings between the CDC and SDNC and how the centralized SDNC collects information from distributed information providers around the world. In addition, it proposes a way to receive information from the information consumer perspective in real-time.

4.1. Associating SADBs between CDC and SDNC

This paper uses a 128-bit DH key to give each CDC up to 2^{128} keys under its management. Considering the possible total number of keys where each CDC uses a different set

of global parameters for the DH key exchange, scalability in the space of the key can be guaranteed, covering enough number of world-wide CDCs as well as a large number of people managed by each CDC. If a CDC controls N vIoT nodes, the CDC needs to associate N DH keys with SDNC. However, these DH key exchanges do not happen at the same time. In addition, each DH key exchange between CDC and SDNC does not require a real-time process.

As shown in Figure 3, CDC and SDNC wish to exchange a group of keys. Here, the total number of secret keys, that is, N, is equal to the number of people the CDC needs to manage. First, CDC selects N random integers to make Secret Value Table of CDC (SVT_D) of $[X_{D,1}, X_{D,2}, X_{D,2}, \cdots, X_{D,N}]$ and computes N corresponding blind values to make Blind Value Table of CDC (BVT_D) of $[Y_{D,1}, Y_{D,2}, Y_{D,2}, \cdots, Y_{D,N}]$ where $Y_{D,i} = a^{X_{D,i}} \ mod \ q, i = 1, 2, 3, \cdots, N$. Then, CDC sends Association Request with the information of the identifiers ($CASAE_1, CASAE_2, CASAE_2, \cdots, CASAE_N$) to SDNC. Receiving this request, SDNC selects N random integers to make Secret Value Table of SDNC (SVT_S) of $[X_{S,1}, X_{S,2}, X_{S,2}, \cdots, X_{S,N}]$ and computes N corresponding blind values to make Blind Value Table of SDNC (BVT_S) of $[Y_{S,1}, Y_{S,2}, Y_{S,2}, \cdots, Y_{S,N}]$ where $Y_{S,i} = a^{X_{S,i}} \ mod \ q, i = 1, 2, 3, \cdots, N$. After the association process is complete between CDC and SDNC, they exchange their BVTs. As a result, CDC and SDNC maintain their own SADBs. Each SADB entry (in this paper, this is called "SA") is identified by the CDC-side blind value, that is, the field value of "vIoT node ID".

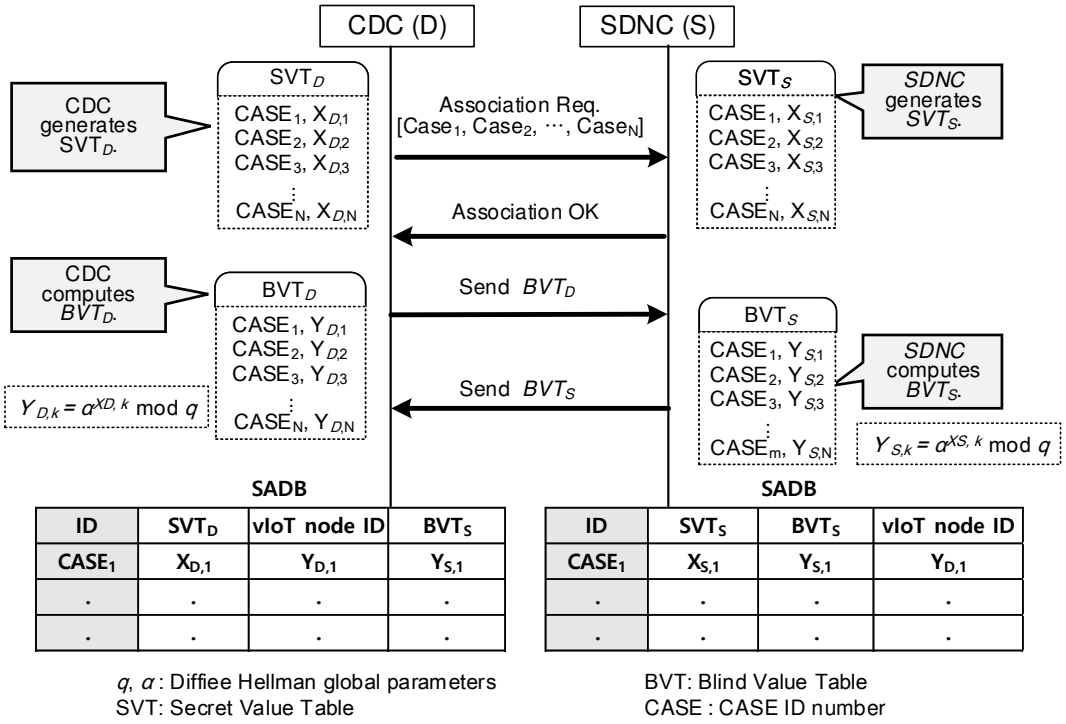

Figure 3. Associating Diffie–Hellman parameters between CDC and SDNC.

4.2. Updating an RR in RRDB at SDNC

If CDC considers that it is necessary to track a particular person, it assigns personal three integers, which include [Identifier of the person in care ($CASE_i$), CDC-side secret value ($X_{D,i}$), SDNC-side blind value ($Y_{S,i}$)], to the vIoT node that belongs to that person. When the vIoT node receives this information, it computes its identifier, that is, its CDC-side blind value, by using the equation of $Y_{D,i} = a^{X_{D,i}} \ mod \ q$. Now, the vIoT node begins to maintain its SA record. Note that the person's identifier, that is, $CASE_i$, is independent of

that of the vIoT node. Then, the vIoT node computes its key as $K_{D,i} = Y_{S,i}{}^{X_{D,i}} \ mod \ q$. This key is used to encrypt the "ID" field of its RR as well as the Update RR message to SDNC. Main role of the vIoT node includes track i) its location-related status such as current IP address (IP_{CASE_i}) and ii) GPS data when it moves (GPS_{CASE_i}). As a result, vIoT RR is always up to date because a person moves with his (or her) smartphone.

Each vIoT node is responsible for sending an Update RR message to the SDNC when there is any change in its RR. When the SDNC receives the Update RR message from a certain vIoT node, a real-time DH key computation is necessary to compute the corresponding DH key. As shown in Figure 4, when any change in vIoT RR occurs, the vIoT node sends the Update RR message to SDNC. This message contains the safe part encrypted with the CDC-side key of $K_{D,i}$, that is, $E^{AES}{}_{K_{D,i}}(Y_{D,i}, CASE_i, IP_{CASE_i}, GPS_{CASE_i})$ as well as its blind value of $Y_{D,i}$ in a clear form. So, the attackers cannot decipher the Update RR message. In addition, the blind value of $Y_{D,i}$ in that message has no relation with the person who owns this blind value. Receiving the Update RR message, SDNC first searches SDNC-side secret value ($X_{S,i}$) corresponding to the blind value of $Y_{D,i}$ from its SADB. Then, the SDNC computes the DH key as $K_{S,i} = Y_{D,i}{}^{X_{S,i}} mod q$ and carries out the AES-decryption process of $D^{AES}{}_{K_{S,i}}(E^{AES}{}_{K_{D,i}}(Y_{D,i}, CASE_i, IP_{CASE_i}, GPS_{CASE_i}))$ using the SDNC-side key of $K_{S,i}$. The SDNC authenticates the sender of the Update RR message by checking if the decrypted value of $Y_{D,i}$ equals to the blind value of $Y_{D,i}$ in the message. Now, SDNC updates $Y_{D,i}$-indexed entry in its RRDB.

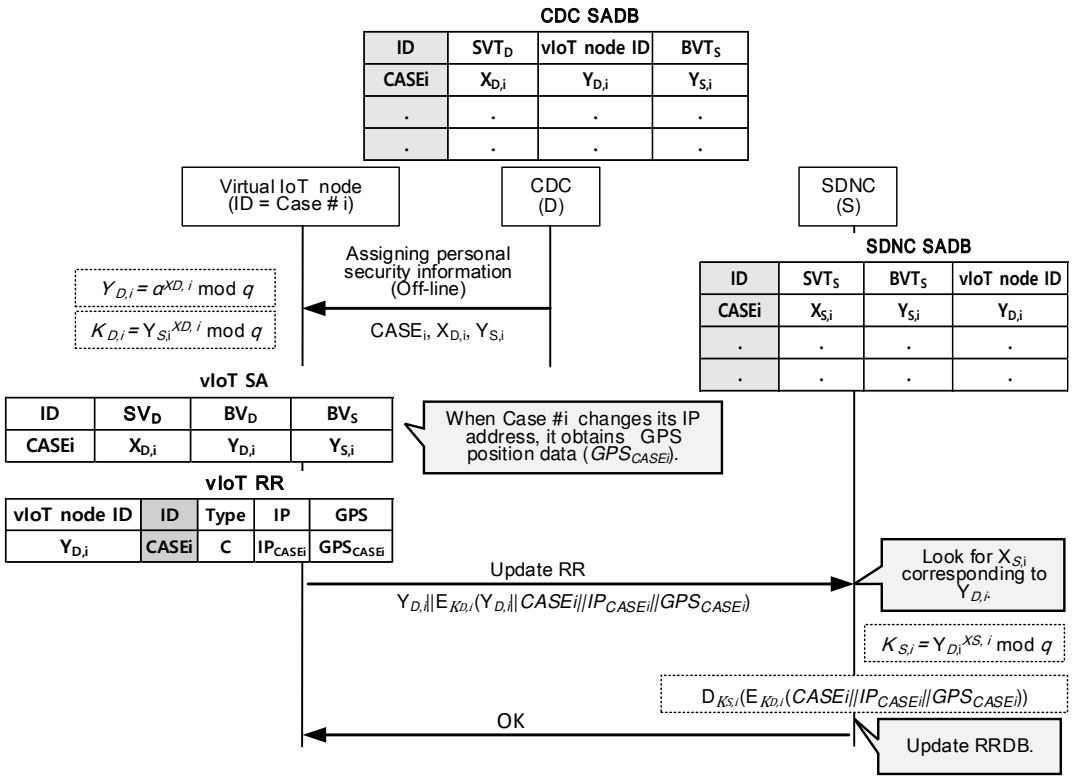

Figure 4. Updating an RR in RRDB at SDNC.

4.3. Querying RRs Matched with the Index List

CDC obtains the necessary RR data from RRDB at SDNC via the Query/Reply mechanism like the DNS. When CDC sends the Query message to SDNC, it uses the "Index List" that stands for a combined list of words such as the location information and the types of the person CDC wants to observe. When the Query message arrives at SDNC, it searches to find the RRs related to the requested index list. Figure 5 shows the example

case that "Query" matches two RRs: $Y_{D,i}$-indexed RR and $Y_{D,k}$-indexed RR. SDNC sends these two RRs to CDC as the Reply message. Here, SDNC finds the information CDC is looking for from RRDB and answers it without processing it. No processing significantly reduces SDNC's computing load to handle queries and replies and also reduces the amount of time spent on one time Query/Reply try from CDC viewpoints. When CDC receives the Reply message, it first calculates the relevant keys ($K_{D,i}$, $K_{D,k}$). Using these keys, the CDC can decrypt the encrypted fields in the received RRs. Now, CDC analyzes the replied information.

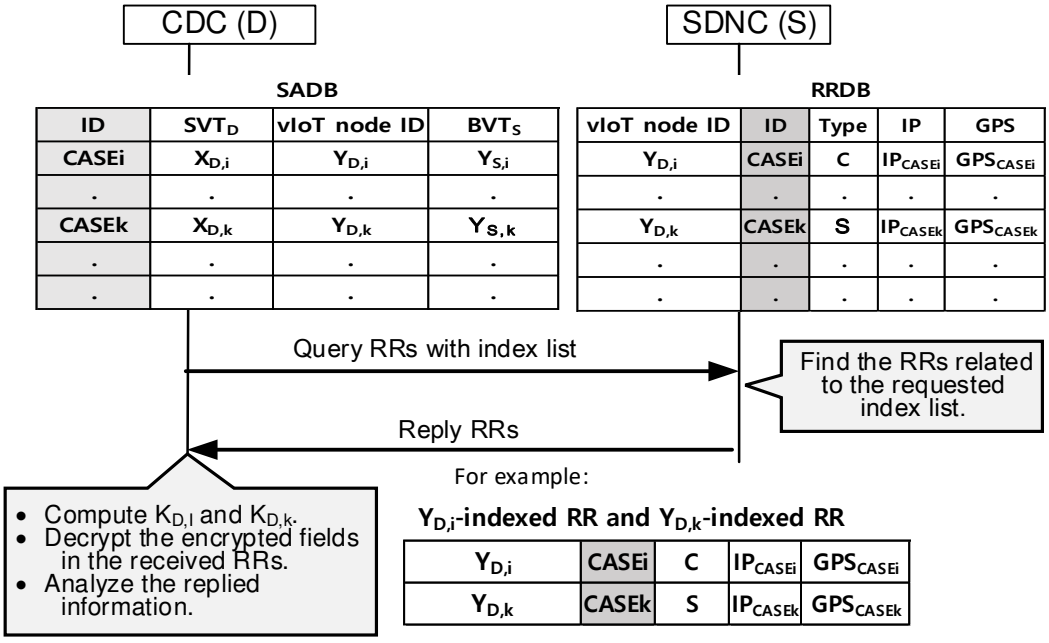

Figure 5. Querying RRs matched with the index list.

4.4. Accessing RRDB from Normal Users Having No Security Associations

Ordinary users do not maintain any security associations. However, they can access necessary RRs from RRDB at SDNC. Those users send the Query message to SDNC with the "Index List" containing the location information and the types of the person he (or she) wants to observe. When the Query message arrives at SDNC, it searches to find the RRs related to the requested index list. Here, SDNC replies in the same way without discriminating CDCs and ordinary users as Query senders. Figure 6 shows the example case that "Query" matches two RRs: $Y_{D,m}$-indexed RR and $Y_{D,k}$-indexed RR. Here, SDNC finds the information the user is looking for from RRDB and answers it without processing it at all. SDNC sends these two RRs to the user as the Reply message. Receiving the RRs, the Query sender neglects the encrypted fields in the received RRs. Now, it starts to analyze the contents in all the cleared areas in the RRs.

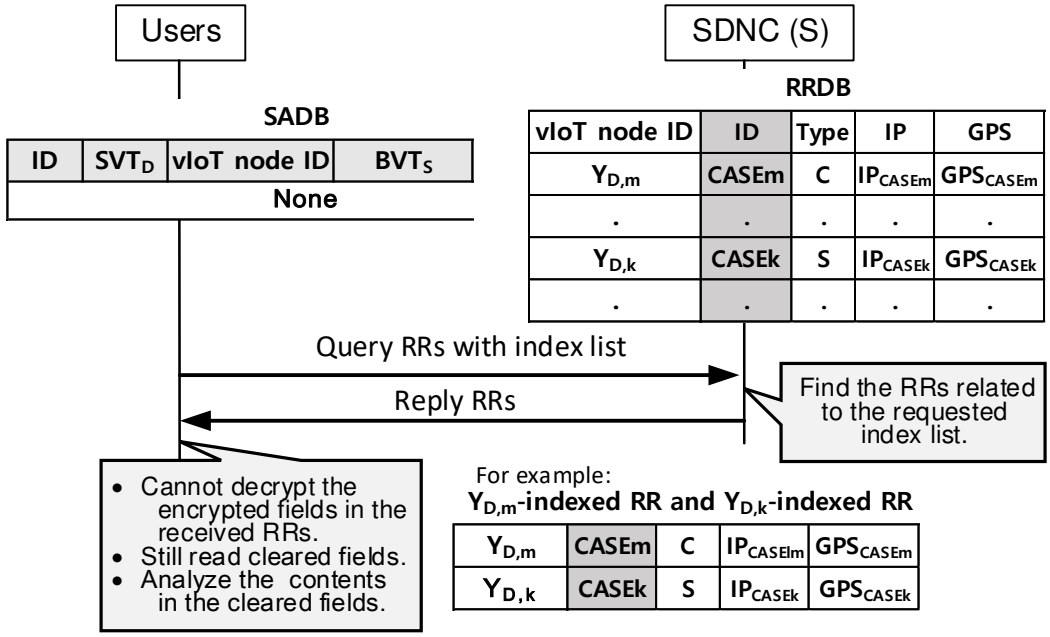

Figure 6. Accessing RRDB from ordinary users having no security associations.

5. Discussions

To monitor the movement situation of targets, who are likely to spread COVID-19 infection in real-time, is a prerequisite condition to prevent the spread of COVID-19. In addition, identifying their movements should be done globally, not limited to specific regions. From this perspective, it is explained below how the paper meets the seven issues mentioned in the introduction explaining the merits of the proposed public platform for COVID-19 tracking. It also suggests the need for further research.

5.1. Benefits of the Proposed Platform

5.1.1. Authentication

CDC and SDNC are all trusted institutions. At the security association stage between CDC and SDNC, it is possible to ensure mutual authentication because the DH variables switch between two trusted institutions. Usually, CDC legally requires vIoT nodes to take compulsory measures such as reporting their location information. Besides, when the CDC provides variables related to security to vIoT nodes, it is made offline. Therefore, there is no need to worry about problems such as mutual authentication on an online basis. The Update RR message contains the value of the vIoT node ID in an AES-encrypted form and that in a transparent way. Receiving the Update RR message, SDNC first searches SDNC-side secret value corresponding to the value of the vIoT node ID in a transparent way. Then, the SDNC computes its DH key with which it decrypts the AES-encrypted part in the message. Then, SDNC can authenticate the vIoT node, which sent the Update RR message by checking whether the encrypted value of the vIoT node ID and that in a clear form is the same.

5.1.2. Confidentiality

Though anyone can access RRDB, authorized users with the relevant secret keys can decipher the critical fields in the RRs because each RR is encrypted with its unique secret key and then stored. So, all RRDB entries are secure as long as their corresponding DH keys are safe. In addition, all data is registered, retrieved, and sent using the identifier of the vIoT node ID. So even if a hacker uses a traffic analysis attack to find the identifier, it

is hard to conclude that this is someone's identity. In this respect, there is no need to be exposed to personal identity.

5.1.3. Scalability

N and P are the numbers of persons tracked by the CDC and CDCs in the world. As both N and P increase, Quality of service still needs to be ensured. The 128-bit space of the DH key in this paper enables each CDC to accommodate 2^{128} essentials under its management. In addition, the same group members, which belong to a specific CDC, use the unique set of global parameters. This set consists of a large prime number of q and α integer that is the primitive root of q. Considering that P CDCs use different sets of global parameters for their DH key exchanges, that is, q_i, α_i where $i = 1, 2, 3, \cdots, P$, the global public platform can guarantee scalability in spite of the increase of P. That means the proposed SDNC works with $N \times P$ different secret keys where N is the number less than 2^{128}. This paper argues that the world must use this type of platform capable of creating this many secret keys in time.

5.1.4. Quality of Service on Latency

DH algorithm uses the computation of modular exponentiation, that is the only reason to cause a latency problem from the viewpoints of security management. To generate BVT, CDC and SDNC each needs N times time required to compute the unit modular exponentiation. However, completing BVT does not require real-time operation, so the computing load of this degree is not a problem in the latency aspect of the DH key exchange. As long as the authentication check goes completed, "Update RR" messages from the vIoT nodes are registered as new entries into the RRDB or updated as the changed entry contents without any processing. Therefore, even if the amount of $N \times P$ increases, SDNC-side latency that occurs to process the RRDB content is not a problem. When SDNC receives a "Query RRs" message, it searches the relevant RRs that match with the index list requested and acknowledges the matched RRs without any processing such as encryption and decryption. So, even if the amount of $N \times P$ increases, SDNC-side latency that occurs to handle world-wide Query/Reply tries is not a problem. For CDCs and ordinary users who receive "Reply RRs" messages, the time it takes to complete the Query/Reply procedure can decrease considerably because of the same reasons as mentioned above.

We built a testbed to obtain latency data that explain how long it takes to complete the Update RR procedure and compute the shared DH keys in a real environment. In our testbed shown in Figure 7, the SDNC's subnet link operates over Wi-Fi with a data rate of 72 Mbps. The Update RR procedure takes time to completion of the DH key agreement between peers. So this latency consists of the round trip network delay and DH key computation time. While the round trip network delay relies on the network traffic condition, the DH key computation time mainly depends on the DH key size. In addition, the DH key computation time varies depending on the Update RR request rates. As shown in Table 1, this paper considers two conditions: CPU conditions of I and II:

- CPU condition I assumes that the smartphone's CPU power is almost free when the Update RR request arrives.
- CPU condition II assumes that the smartphone's CPU power is already occupied by other Update RR requests by 35% when the Update RR request arrives.

Our testbed runs a web's application where the VioT node sends an HTTP request. it contains the safe part encrypted with the CDC-side key of $K_{D,i}$, that is, $E^{AES}{}_{K_{D,i}}(Y_{D,i}, CASE_i, IP_{CASE_i}, GPS_{CASE_i})$ as well as its blind value of $Y_{D,i}$ in a clear form. As SDNC receives the HTTP request, it first searches SDNC-side secret value ($X_{S,i}$) corresponding to the blind value of $Y_{D,i}$ from its SADB. Then, the SDNC computes the DH key as $K_{S,i} = {Y_{D,i}}^{X_{S,i}} mod q$ and carries out the AES-decryption process of $D^{AES}{}_{K_{S,i}}(E^{AES}{}_{K_{D,i}}(Y_{D,i}, CASE_i, IP_{CASE_i}, GPS_{CASE_i}))$ using the SDNC-side key of $K_{S,i}$. The SDNC authenticates the Update RR message by checking if the decrypted value of $Y_{D,i}$ equals to the blind value of $Y_{D,i}$ in the message. Then, SDNC updates $Y_{D,i}$-indexed entry in its RRDB and sends Update OK

message to the vIoT node. The SDNC-playing server computes the DH key. We deal with four different keys: 512-bit DH key, 1024-bit DH key, 2048-bit DH key, and 3072-bit DH key. The vIoT node uses a CPU core clock of 1.2 GHz and Android version 5.0.2. The SDNC-playing web server operates with a CPU core of 2.90 GHz. We repeat HTTP sessions 20 times for each DH key to obtain the latency data and DH key computation time. So, the delay from the departure of the Update RR request to the Update OK's arrival includes network delay and DH key computation time.

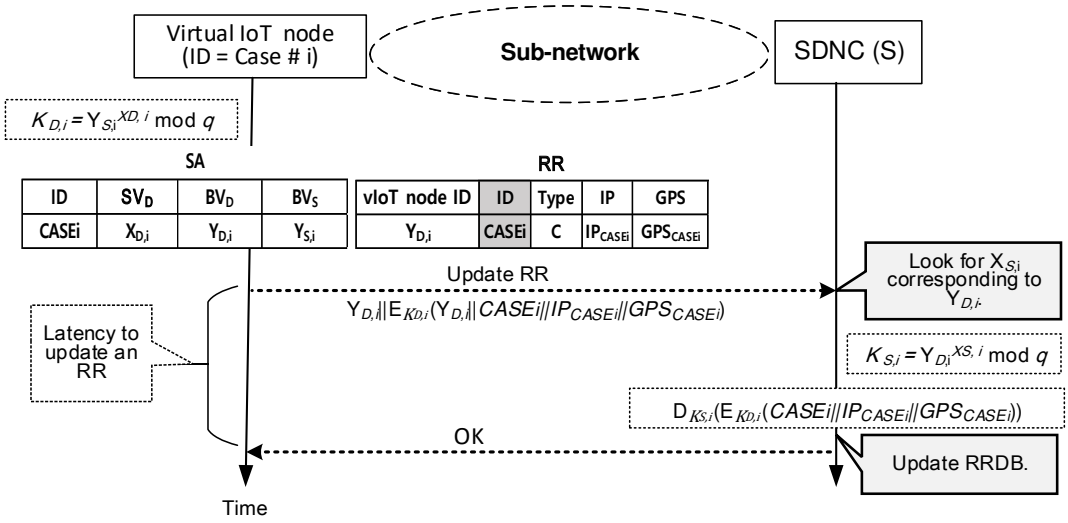

Figure 7. Testbed to obtain experimental data that complete the Update RR procedure in a real environment.

Figure 8 shows the experimental data that explains how long it takes for the vIoT node to complete the Update RR procedure. The measured latency includes the two main factors of the network delay and DH key computation delay. It is shown that latency results differ a lot, depending on the DH key size. If the DH key size increases to 1024 bits, latency reaches around one second. For the DH key size of 3072 bits, it approaches 10 s. As shown in the lower graph, latency variation increases as the key size become large. Considering that our virtual IoT-based monitoring platform uses the 128-bit DH key, latency requirement for the DH key agreement can be satisfied enough.

Figure 9 shows the experimental data that explains the DH key computation time under CPU condition I. DH key computation delays differ a lot, depending on the DH key size. For the DH key size of 3072 bits, the key computation delay approaches 10 s where the component of network delay has no effects. As shown in the lower graph, latency variation increases as the key size become large. Considering that the DH key computation delay decreases below 100 ms for the 512-bit DH key, our virtual IoT-based monitoring platform, which uses the 128-bit DH key, satisfies the requirements DH key computation latency.

Figure 10 shows how the DH key computation time differs as the Update RR request rates vary. It is shown that the DH key computation latency difference between CPU conditions of I and II becomes more considerable as the key size increases. However, the difference can be negligible for the case of the 512-bit DH key. So, it can be concluded that our virtual IoT-based monitoring platform, which uses the 128-bit DH key, satisfies the requirements DH key computation latency even under the condition that the computing power of 35% is occupied with handling the massive Update RR requests.

Table 1: Two different conditions related to the degree of Update RR request rates.

Operational Conditions	CPU	Background CPU Utilization
CPU condition I	Intel i7-10700 2.90 GHz	2 %
CPU condition II	Intel i7-10700 2.90 GHz	35 %

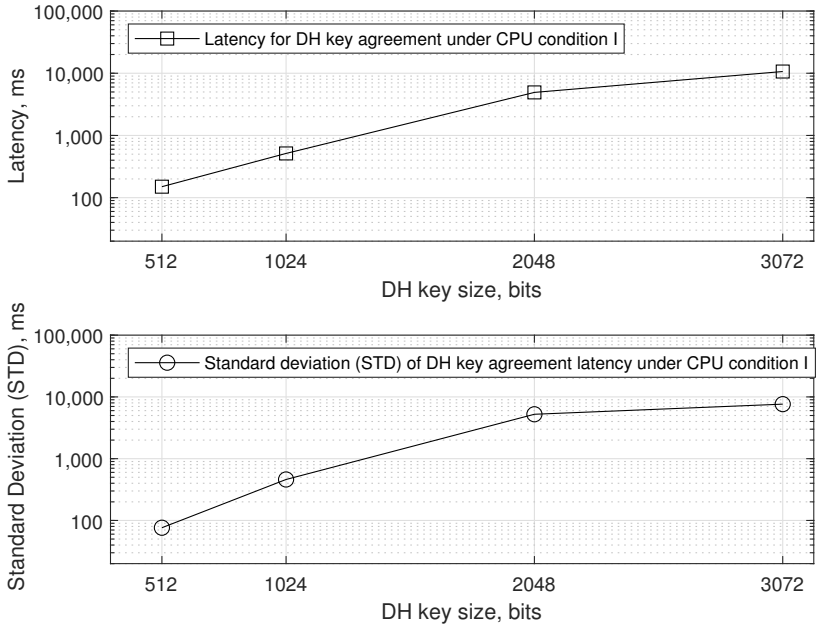

Figure 8. Update RR latency to completion of the DH key agreement between peers.

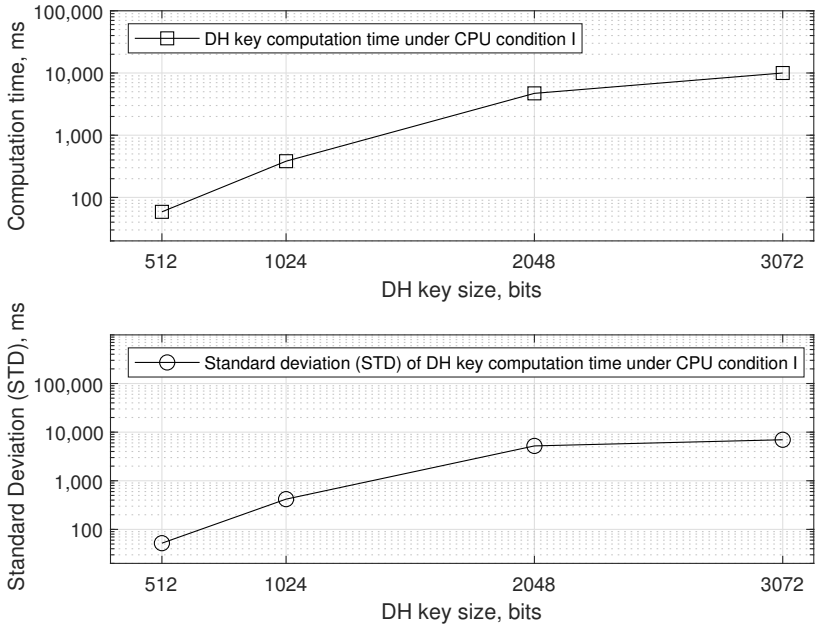

Figure 9. Latency to compute shared DH keys under CPU condition I.

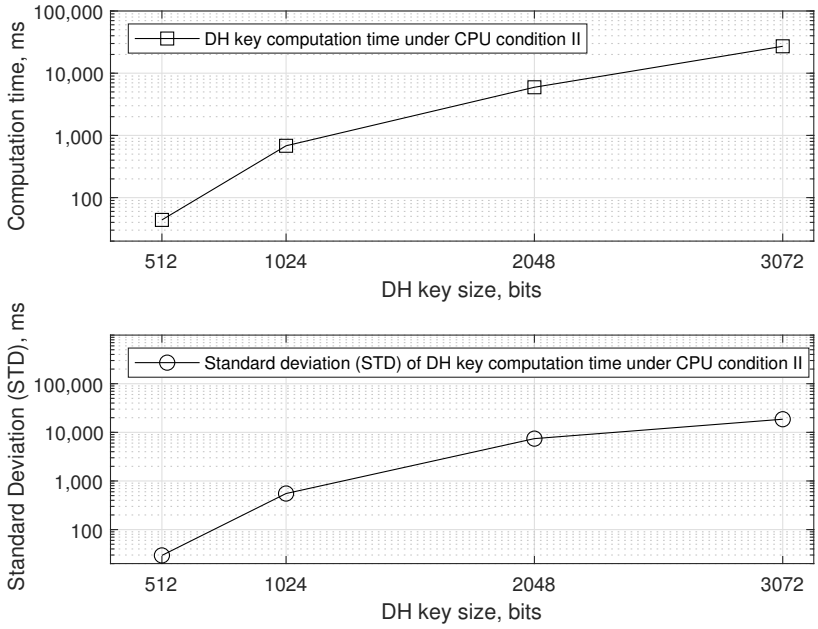

Figure 10. Latency to compute shared DH keys under CPU condition II.

5.2. Further Study Area

5.2.1. Expansion of Information Providers

Even in athletic stadiums and rallies, CDC can assign the "Type" field values to the event organizers and rally organizers. The attractive Type field is PT (Public Transport). If a passenger traveling by bus wants to know whether the corona related person is on the bus he or she is riding, sending the query to SDNC is enough to obtain the information whether there is a COVID person on the bus. Therefore, follow-up research is needed to establish the roles and obligations of the vIoT support nodes, engage them as information providers of the platform, and analyze the limits that the platform can afford to accept various "Type" fields.

5.2.2. Intelligent Searching Algorithm

To receive COVID status information for passengers traveling in the same vehicle, SDN requires high-quality RRDB search capability. For example, if an ordinary user is traveling by bus, the user will send a Query with his (her) location and means of transportation to SDNC. Then, the SNDC must find the bus driver's RR data, which changes in the same pattern as this passenger and return searched RRDB entries for the COVID vIoT nodes in the vehicle changing the position along with the same road as the bus driver. So, future work includes an intelligent search algorithm to improve accuracy in such searches.

5.2.3. CDC Rating Algorithm

It is necessary to verify the reliability of the RRDB contents. For example, in the various world-wide CDCs, their operating levels are quite different. Therefore, it is essential to evaluate the rating of the RRDB provided by a particular CDC. That is why the SDNC should have a CDC rating algorithm using AI technology.

6. Conclusions

Existing relevant contributions suggest a holistic vision of IoT-enabled smart communities utilizing various IoT devices. Compared to existing approaches, this paper aims to design a global platform for monitoring and tracking to prevent COVID-19. In this paper, a vIoT node is a confirmed case or a suspected infection. CDC forcibly installs a virtual IoT node in applications on the smartphone of a confirmed case or a suspected infection

that need monitoring and tracking in its control range. As a centralized center of the platform, SDNC collects location-related information from vIoT nodes belonging to all the distributed CDCs. Each vIoT node is responsible for updating this information to SDNC on a real-time basis. This updating procedure and maintaining relevant data in SDNC are secure because of shared secret keys between a specific vIoT node and SDNC. The CDC can monitor the complete information for monitoring and tracking the vIoT nodes under its control. Unlike vIoT nodes, an ordinary user can obtain the resource data of SDNC except for privacy-related data even though the user does not maintain any security associations. Our platform's design aims to ensure individual privacy to every vIoT node, while SDNC provides real-time information services to ordinary users as much as possible. In addition, our platform meets system scalability and reduces Update latency for a vIoT node and Query/Reply latency to normal users, where the platform accommodates a large number of world-wide CDCs and persons in control per CDC. Our analytical results proved that our virtual IoT-based monitoring platform, which uses the 128-bit DH key, satisfies the latency requirement for real-time Updates between vIoT and SDNC.

Author Contributions: Y.J.: Conceptualization; methodology; investigation; original; writing; supervision; funding acquisition. R.A.: Formal analysis; writing—editing; experiments. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2020R1A2B5B01001825). This study was also supported by the Research Fund, 2020 of The Catholic University of Korea.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sultan, A.; Mushtaq, M.A.; Abubakar, M. IOT Security Issues Via Blockchain: A Review Paper. In Proceedings of the 2019 International Conference on Blockchain Technology, Honolulu, HI, USA, 15 March 2019; pp. 60–65.
2. Bai, Z.; Gong, Y.; Tian, X.; Cao, Y.; Liu, W.; Li, J. *The Rapid Assessment and Early Warning Models for COVID-19*; Springer: Berlin, Germany, 2020; p. 1.
3. Ndiaye, M.; Oyewobi, S.S.; Abu-Mahfouz, A.M.; Hancke, G.P.; Kurien, A.M.; Djouani, K. IoT in the Wake of COVID-19: A Survey on Contributions, Challenges and Evolution. *IEEE Access* **2020**, *8*, 186821–186839, doi:10.1109/ACCESS.2020.3030090.
4. Ksentini, A.; Brik, B. An Edge-Based Social Distancing Detection Service to Mitigate COVID-19 Propagation. *IEEE Internet Things Mag.* **2020**, *3*, 35–39, doi:10.1109/IOTM.0001.2000138.
5. Exposure Notification Bluetooth Specification Preliminary—Subject to Modification and Extension. 2020; Volume 1.2. Available online: https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf (accessed on 23 June 2020).
6. Cooper, D.; Quathem, K.; Meneses, A. COVID-19 Apps and Websites–The "Pan-European Privacy Preserving Proximity Tracing Initiative" and Guidance by Supervisory Authorities. Available online: https://www.insideprivacy.com/covid-19/covid-19-apps-and-websites/ (accessed on 23 June 2020)
7. Kim, J.M.; Kim, H.M.; Lee, E.J.; Jo, H.J.; Yoon, Y.; Lee, N.J.; Son, J.; Lee, Y.-J.; Kim, M.S.; Lee, Y.-P.; et al. Detection and Isolation of SARS-CoV-2 in Serum, Urine, and Stool Specimens of COVID-19 Patients from the Republic of Korea. *Osong Public Health Res. Perspect.* **2020**, *11*, 112–117, doi:10.24171/j.phrp.2020.11.3.02.
8. Park, O.; Park, Y.J.; Park, S.Y.; Kim, Y.M.; Kim, J.; Lee, J.; Park, E.; Kim, D.; Jeon, B.H.; Ryu. B.; et al. Contact Transmission of COVID-19 in South Korea: Novel Investigation Techniques for Tracing Contacts. *Osong Public Health Res. Perspect.* **2020**, *11*, 60–63, doi:10.24171/j.phrp.2020.11.1.09.
9. Team, G.P.T.F. Global Health Security: The Lessons from the West African Ebola Virus Disease Epidemic and MERS Outbreak in the Republic of Korea. *Osong Public Health Res. Perspect.* **2015**, *6*, S25–S27, doi:10.1016/j.phrp.2015.12.006.
10. Jung, Y.; Peradilla, M.; Saini, A. Software-defined Naming, Discovery and Session Control for IoT Devices and Smart Phones in the Constraint Networks. *Procedia Comput. Sci.* **2017**, *110*, 290–296, doi:10.1016/j.procs.2017.06.097.
11. Nour, B.; Sharif, K.; Li, F.; Moungla, H.; Liu, Y. A unified hybrid information-centric naming scheme for IoT applications. *Comput. Commun.* **2020**, *150*, 103–114, doi:10.1016/j.comcom.2019.11.020.
12. Festijo, E.; Jung, Y.; Peradilla, M. Software-defined security controller-based group management and end-to-end security management. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 3365–3382, doi:10.1007/s12652-018-0678-6.
13. Jung, Y.; Agulto, R. Integrated Management of Network Address Translation, Mobility and Security on the Blockchain Control Plane. *Sensors* **2020**, *20*, 69.

14. Jung, Y.; Peradilla, M.; Agulto, R. Packet Key-Based End-to-End Security Management on a Blockchain Control Plane. *Sensors* **2019**, *19*, 2310, doi:10.3390/s19102310.
15. Choi, Y.J.; Kang, H.J.; Lee, I.G. Scalable and Secure Internet of Things Connectivity. *Electronics* **2019**, *8*, 752, doi:10.3390/electronics8070752.
16. Kaur, J.; Kaur, K. Internet of Things: A review on technologies, architecture, challenges, applications, future trends. *Int. J. Comput. Netw. Inf. Secur.* **2017**, *9*, 57.
17. Collado-Borrell, R.; Escudero-Vilaplana, V.; Villanueva-Bueno, C.; Herranz-Alonso, A.; Sanjurjo-Saez, M. Features and functionalities of smartphone apps related to COVID-19: systematic search in App stores and content analysis. *J. Med Internet Res.* **2020**, *22*, e20334.
18. Watson, C.; Cicero, A.; Blumenstock, J.S.; Fraser, M.R. *A National Plan to Enable Comprehensive COVID-19 Case Finding and Contact Tracing in the US*; Johns Hopkins Bloomberg School of Public Health, Center for Health Security: Baltimore, MD, USA, 2020.
19. Tidy, J. Coronavirus: Israel enables emergency spy powers. BBC News. 2020. Available online: https://www.bbc.com/news/technology-51930681 (accessed on 17 March 2020).
20. Kim, M.; Denyer, S. A 'travel log' of the times in South Korea: Mapping the movements of coronavirus carriers. The Washington Post. 2020. Available online: https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html (accessed on 13 March 2020).
21. Wang, C.J.; Ng, C.Y.; Brook, R.H. Response to COVID-19 in Taiwan: Big data analytics, new technology, and proactive testing. *JAMA* **2020**, *323*, 1341–1342.
22. Lee, Y. Taiwan's new'electronic fence'for quarantines leads wave of virus monitoring. Reuters Technology News. 2020. Available online: https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc-idUSKBN2170SK (accessed on 20 March 2020).
23. Cho, H.; Ippolito, D.; Yu, Y.W. Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv* **2020**, arXiv:2003.11511.
24. Marbouh, D.; Abbasi, T.; Maasmi, F.; Omar, I.A.; Debe, M.S.; Salah, K.; Jayaraman, R.; Ellahham, S. Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. *Arab. J. Sci. Eng.* **2020**, 1–17, doi:10.1007/s13369-020-04950-4.
25. Bischoff, P. COVID-19 App Tracker: Is Privacy Being Sacrificed in a Bid to Combat the Virus? 2020. Available online: https://www.comparitech.com/blog/vpn-privacy/coronavirus-apps/ (accessed on Day Month Year).
26. Warner, K.; Nowais, S. Coronavirus: Doctors urge public to help track Covid-19 cases with tracing app. The National. 2020. Available online: https://www.thenationalnews.com/uae/health/coronavirus-doctors-urge-public-to-help-track-covid-19-cases-with-tracing-app-1.1012267 (accessed on 28 April 2020)
27. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326.
28. Aileni, R.M.; Suciu, G. *IoMT: A Blockchain Perspective*; Springer: Cham, Switzerland, 2020; pp. 199–215.
29. G. Srivastava, J.C.; Dhar, S. A Light and Secure Healthcare Blockchain for IoT Medical Devices. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–5, doi:10.1109/CCECE.2019.8861593.
30. Gupta, D.; Bhatt, S.; Gupta, M.; Tosun, A.S. Future Smart Connected Communities to Fight COVID-19 Outbreak. *Internet Things* **2020**, 100342, doi:10.1016/j.iot.2020.100342.
31. Gupta, M.; Abdelsalam, M.; Mittal, S. Enabling and enforcing social distancing measures using smart city and ITS infrastructures. *arXiv* **2020**, arXiv:2004.09246.