big data and cognitive computing

MDPI

Article

Security and Privacy Threats and Requirements for the Centralized Contact Tracing System in Korea

Sungchae Park and Heung-Youl Youm *

Department of Information Security Engineering, Soonchunhyang University, Asan-si 31538, Republic of Korea
* Correspondence: hyyoum@sch.ac.kr

Abstract: As COVID-19 became a pandemic worldwide, contact tracing technologies and information systems were developed for quick control of infectious diseases in both the private and public sectors. This study aims to strengthen the data subject's security, privacy, and rights in a centralized contact tracing system adopted for a quick response to the spread of infectious diseases due to climate change, increasing cross-border movement, etc. There are several types of contact tracing systems: centralized, decentralized, and hybrid models. This study demonstrates the privacy model for a centralized contact tracing system, focusing on the case in Korea. Hence, we define security and privacy threats to the centralized contact tracing system. The threat analysis involved mapping the threats in ITU-T X.1121; in order to validate the defined threats, we used LIDDUN and STRIDE to map the threats. In addition, this study provides security requirements for each threat defined for more secure utilization of the centralized contact tracing system.

Keywords: centralized contact tracing system; Korea COVID-19 smart management system (SMS); privacy model; security threats; privacy threats; security and privacy requirements

Citation: Park, S.; Youm, H.-Y. Security and Privacy Threats and Requirements for the Centralized Contact Tracing System in Korea. *Big Data Cogn. Comput.* **2022**, *6*, 143. https://doi.org/10.3390/bdcc6040143

Academic Editors: Peter R.J. Trim and Yang-Im Lee

Received: 5 August 2022
Accepted: 7 October 2022
Published: 28 November 2022

1. Introduction

As COVID-19 became a pandemic worldwide, contact tracing technologies and information systems were developed for the quick control of infectious diseases in both the private and public sectors. The systems were implemented to collect and process various data to monitor the COVID-19 pandemic, and the pandemic was managed through contact tracing systems that can identify contacts and prevent the spread of infectious diseases.

There are several types of contact tracing systems; apart from centralized and decentralized models, a hybrid way has been approached. In centralized contact-tracing, mobiles share their anonymous IDs to a central server maintaining a centralized database, and the server uses this database to perform contact tracing, risk analysis, and alert notifications to the users [1]. The ROBERT (ROBust and privacy-presERving proximity Tracing) protocol is an example of the centralized contact tracing system adopted by France and Europe. ROBERT is a joint contribution in the framework of the PEPP-PT (Pan European Privacy-Preserving Proximity Tracing) initiative, which aims to enable the development of interoperable contact tracing solutions that comply with European data protection, privacy, and security standards as part of a more comprehensive response to the pandemic [2]. De-centralized contact tracing, on the other hand, does not send any PII data to the centralized server but stores all PII data in the user's mobile phone and notifies them when they come into contact with a confirmed case. In addition, each user's mobile phone acts as a local server that shares only the infected individual's data to the centralized server, and then mobile phones will fetch this data periodically from the server and do contact matching locally [1]. An example of a decentralized contact tracing system is DP-3T: a decentralized, privacy-preserving proximity tracing system. DP-3T aims to minimize privacy and security risks for individuals and communities and guarantees the highest level of data protection [3]. A hybrid architecture may have a component of both approaches,

with some information handled on individual devices with a central server analyzing data and sending notifications [4]. PIVOT (Private and Effective Contact Tracing) and DESIRE(a novel exposure notification system that leverages the best of centralized and decentralized systems) have been known as representative examples of the hybrid approach for contact tracing systems [5,6].

Each system has different priorities in terms of a quick response to confirmed cases and privacy. A major advantage of a centralized contact tracing system is that health authorities enable an infectious diseases situation to be controlled more effectively, such as COVID-19. However, a centralized system requires the extensive collection of personal data within the centralized server or systems. In addition, it may cause higher risks of security and privacy issues compared to decentralized and hybrid systems.

This study analyzes a privacy model and the security and privacy threats of a centralized contact tracing system, based on Korea's COVID-19 smart management system. We also identify relevant security and–privacy requirements, which should be taken into account at each processing of data.

2. Related Works

Contact tracing is an effective method to control emerging infectious diseases. Since the 1980s, modelers have been developing a consistent theory for contact tracing, with the aims to find effective and efficient implementations and to assess the effects of contact tracing on the spread of an infectious disease. Contact tracing is a more focused method: once an infected individual is diagnosed and isolated, contact persons are identified, who potentially had infectious interactions with that index case [7].

This section summarizes the previous literature with regards to contact tracing technology, which is an effective method to control emerging infectious diseases and compares the features of this paper with the related literature.

2.1. Case Study of Contact Tracing for COVID-19 in Korea

In April 2021, the *Journal of the American Medical Association* (JAMA) published research regarding the information-technology-based tracing strategy in response to COVID-19 in South Korea and the related privacy controversies, as studied by Seoul National University (SNU)'s Haksoo Ko. This research covers legal and policy responses of contact tracing related to COVID-19 in South Korea. It explains that South Korea extensively utilized the country's advanced information technology (IT) system for tracing individuals suspected to be infected or who had been in contact with an infected person. In addition, this research emphasizes that there is a need for a balance between privacy issues and the effects of epidemiological investigations brought about by the extensive tracing of infected people and disclosure of collected information [8].

2.2. Case Study on COVID-19 Contact Tracing in Taiwan

Inspired by the lessons learned from the Ebola outbreak in West Africa, the Taiwan Center for Disease Control (TCDC) developed a national contact tracing platform named TRACE in 2017, to link other data systems, monitor the health status of contacts, and support the management of contacts by compiling the daily descriptive analysis and relevant performance indicators. The modules in TRACE were applicable for all notifiable diseases in Taiwan, and they have been implemented for contact tracing in diseases such as measles and rubella and for health monitoring of individuals exposed to animals with avian influenza. For the COVID-19 outbreak response, Taiwan's government developed a COVID-19 module in mid-January 2020 to support contact tracing. To ensure confidentiality, the database that contained contacts' personally identifiable information(PII) would be deleted in six months and could not be used for other purposes [9].

There is another study on contact tracing in Taiwan. The purpose of this study was to measure the high national acceptance for COVID-19 contact tracing technologies in Taiwan. The study is regarding that the effectiveness of government policies in the control

of the spread of COVID-19 and the acceptance of such government policies among people are different. In addition, it shows acceptance increased with the perceived technology benefits; trust in the providers' intent, data security, and privacy measures; the level of ongoing control; and one's level of education. Acceptance decreased with data sensitivity perceptions and perceived low policy compliance by others in the general public [10].

2.3. Analysis and Comparison of Privacy in Contact Tracing Apps

When people first started using contact tracing applications, privacy issues for the people who are infected with COVID-19 occurred. In addition, there was resistance to the use of contact tracing apps and discrimination against patients with coronavirus disease. A study based on this situation modeled specific privacy threats to explain the detailed analysis results of COVID-19 tracing apps and the main differences between privacy protection and security performance among various contact tracing apps. This study described different national cultures that tend to select centralized and decentralized contact tracking applications. Furthermore, this study emphasized that it is undeniable that privacy has been violated to some extent no matter what application is used in the context of prevention and control. In order to protect personal data, privacy threat analysis of various contact tracing technologies and a comparison of the results of contact tracing apps for COVID-19 suggest that infectious disease prevention, control, and privacy can be effectively protected [11].

2.4. Case Study of COVID-19 Contact Tracing Mobile Application in Singapore

The Singaporean government released a mobile phone app, TraceTogether, which is designed to assist health officials in tracking down exposures after an infected individual is identified. However, there are important privacy implications of the existence of such tracking apps. A related study analyzes some of those implications and proposes ways of ameliorating privacy concerns without decreasing the usefulness to public health [12].

2.5. Differences and Contributions of This Paper

In addition to the studies described above, there are various meaningful studies on infectious disease contact tracing techniques or systems such as those for COVID-19. There have been a lot of papers, research, studies, etc., in terms of infectious disease control and security, including a comparison of centralized and decentralized contact tracing systems. These published studies revealed the positive effects of the IT technologies reflecting each government's policy, enabling a rapid response to global infectious diseases such as the COVID-19 pandemic. A comparison of this paper and the abovementioned related works is displayed in Table 1. In this Table 1, ○ means that relevance issue in column 1 is addressed and ✕ is not addressed.

Table 1. A comparison of this paper and the related works.

Contents of This Paper	This Paper	2.1	2.2	2.3	2.4
Privacy modeling of contact tracing system	○	✕	✕	✕	✕
Security and privacy threats analysis	○	✕	✕	○	○
Security and privacy requirements mapping	○	✕	✕	○	○
Contact tracing technology based method	QR code Credit card	Not mentioned	Bluetooth	Bluetooth GPS	Bluetooth
Comparison of a centralized and decentralized model	✕	✕	○	○	✕

○ means that relevance issue in column 1 is addressed and ✕ is not addressed.

Table 2 provides some contact tracing systems or applications developed by many countries including Korea as well as companies.

Table 2. The examples of contact tracing systems/applications by countries/authors.

Country or Authors	Examples of Contact Tracing Systems or Applications	Approach
Korea	Korea COVID-19 smart management system	Centralized
UK	NHS contact tracing app [13]	Centralized
China	Health Code [14]	Centralized
Singapore	TraceTogether (OpenTrace/BlueTrace) [12,15]	Centralized
EU	PEPP-PP [16]	Centralized
EU	DP-3T [17]	Decentralized
TCN Coalition	TCN [18]	Decentralized
Google/Apple	Google–Apple Exposure Notification application programming interface (API) [19]	Decentralized
Norway	Smittestopp [20]	Centralized Decentralized
Mahabir Prasad Jhanwar, Sumanta Sarkar	PHyCT (Privacy preserving Hybrid Contact Tracing) [21]	Hybrid
Giuseppe Garofalo, Tim Van hamme, et al.	PIVOT (PrIVate and effective cOntact Tracing) [6]	Hybrid
Claude Castelluccia, Nataliia Bielova, et al.	DESIRE (a novel exposure notification system that leverages the best of centralized and decentralized systems) [5]	Hybrid

The NHS COVID-19 app uses Bluetooth Low Energy (BLE) to understand the distance, over time, between app users and send an exposure notification to someone who has had close contact [13]. The Chinese government relies on Health Code, developed by Alipay and WeChat, for identifying people potentially exposed to COVID-19 [14]. TraceTogether is the first national deployment of a Bluetooth-based contact tracing system in the world. It was developed by the Singaporean government's Technology Agency and Ministry of Health to help the country better respond to epidemics [15]. The purpose of the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) approach is to provide a common basis for management systems that can be integrated into national public health responses to the COVID-19 pandemic. The PEPP-PT approach has been created by a multinational European team [16]. DP-3T determines who has been in close physical proximity to a COVID-19-positive person without revealing that person's identity or where the contact occurred, requiring a centralized database or server [17]. TCN is a protocol developed by the TCN Coalition, which has jointly developed a common protocol between their apps [18]. The Google–Apple Exposure Notification application programming interface (API) is the most representative example of a decentralized contact tracing system based on Bluetooth. This exposure notification app generates a random ID for a mobile phone without tracking a person's location [19]. Norway released two types of contact tracing applications, based on the centralized approach for the first version and the decentralized approach for the second version. The decentralized approach is based on the protocol for exposure notification by Apple and Google [20]. In addition, a hybrid model may have a component of both approaches, with some information handled on individual devices with a central server analyzing data and sending notifications [4].

In Europe and North America, a decentralized contact tracing system has been mainly preferred, but, in Asia, a centralized contact tracing system has been used more. Hybrid contact tracing systems have been introduced in journals and some technical reports. Not all the contact tracing systems or applications in the table above have been used or adopted successfully. Table 2 lists some representative examples of contact tracing systems or applications used during the COVID-19 pandemic. This study describes a privacy perspective model for a centralized infectious disease contact tracking system and a life cycle for processing collection information, focusing on Korean cases. Moreover, our work analyzes the security and privacy threats affecting the privacy model of a centralized contact tracing system on a QR code basis and aims to validate it; we present the mapping result of the security and–privacy requirements against each threat.

3. Data Processing Model for a Centralized Contact Tracing System

3.1. Korea's COVID-19 Smart Management System (SMS) [22]

The Korean government defines basic activities that need to be accomplished to prevent the spread of COVID-19, per 'Infectious Disease Control and Prevention Act' as an 'epidemiological investigation' [23], and has developed a centralized system to control the spread of COVID-19, which is called the COVID-19 smart management system. This system enables the automation of the epidemiological investigation, as specified in 'Infectious Disease Control and Prevention Act', and it has developed the application of smart city technologies to collect, process, and analyze a huge volume of urban data.

Through this system, it is possible to secure epidemiological investigation results within 10 min by the real-time analysis of the movements of confirmed patients and large-scale outbreak areas, by using big data linked to 28 institutions through the cooperation of government agencies. The use of the personal information from confirmed cases in this system is based on the regulations of the 'Infectious Disease Control and Prevention Act' that allow for the public to use some personal information that would be sensitive for accurate epidemiological investigations in infectious disease crisis situations [23]. This policy was put in place to conduct accurate epidemiological investigations, with the legal change occurring after the Middle East Respiratory Syndrome (MERS) outbreak in 2015. This law allows for the use of personal information in exceptional cases for the prevention of infectious diseases such as COVID-19, through the cooperation and approval of relevant agencies. Korea's COVID-19 smart management system collects minimal data and applies a strict data collection process for the use and safe management of PII [24].

Korea's government has developed a centralized infectious disease contact tracing system, as shown in Figure 1. When a confirmed case of COVID-19 occurs, the data collection method for tracking the movement of the confirmed person is as follows:

- QR-code-based electronic access list used when entering specific facilities;
- Handwritten list;
- Collected mobile phone numbers recorded by people calling with phone numbers issued by local governments when entering specific facilities.

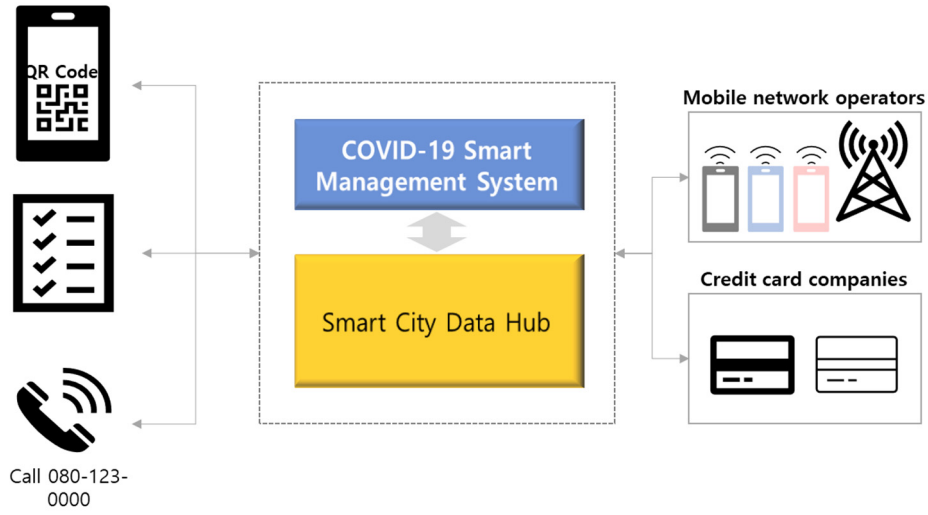

Figure 1. Korea's COVID-19 smart management system (SMS).

The records of subjects' facility visits are stored on the management server of the Korea Social Security Information Service (SSIS), and the PII of the QR code is encrypted and stored on the server of each company that issued the QR code. In addition, when data are required, in the case of the occurrence and tracing of confirmed COVID-19 cases, the distributed data that were stored on differently located servers are called by the COVID-19 smart management system, which combines the required data for tracing.

In the case of Korea's contact tracing system, it is not simply limited to the mobile app as a system. Korea's contact tracing system, the COVID-19 Smart Management System (SMS), operates by leveraging the central data hub platform of the Korean government, taking into account both the pre-confirmation status and the confirmed status [22].

The KCDC shares data and cooperates with central, municipal, or local governments; national health insurance agencies; and health care professionals and their associations, as depicted in Figure 2. This system enabled the prompt delivery of data pertaining to the confirmed cases to relevant agencies. Furthermore, the MOHW must release information such as the path and means of transportation of infected persons, etc., on the Internet or through a press release [8].

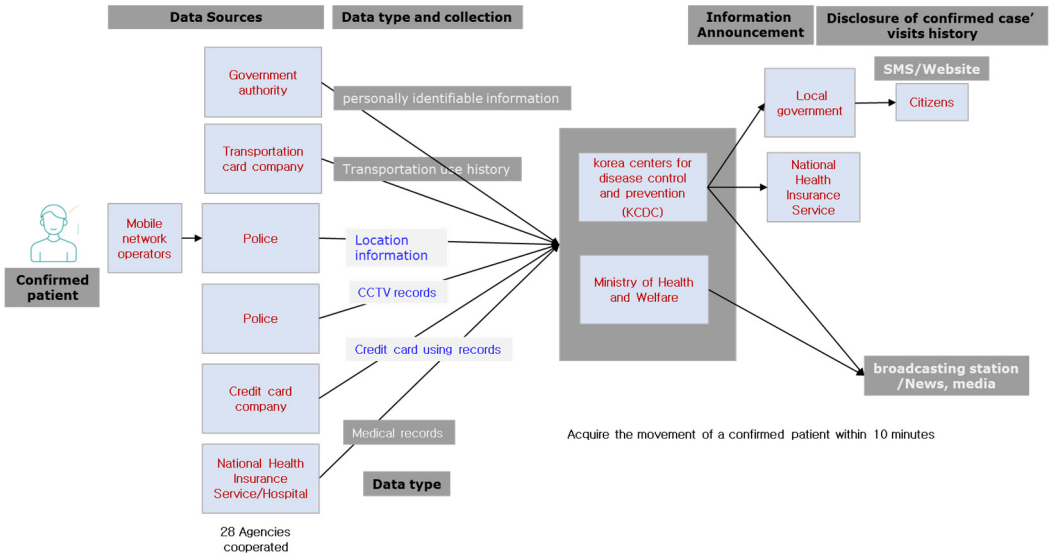

Figure 2. An example of the overall structure of the Korean contact tracing system [25].

An example of the overall structure of the Korean contact tracing system is shown in Figure 2.

3.2. Data Processing Model

This paper suggests a privacy model for a centralized contact tracing system based on the case study of the Korean system for the prevention and control of infectious diseases. In the Korean system, a third party, the Korea Centers for Disease Control and Prevention (KCDC), works as a centralized server that mainly processes the health information and infection status, analyzing that to identifying patients and contactors and collaborating with other third parties to quarantine patients and publish infection information to the public [24]. In a centralized privacy model, third parties takes a significant role in the response and control of infectious diseases.

The privacy model of a centralized contact tracing system is depicted in Figure 3 [1].

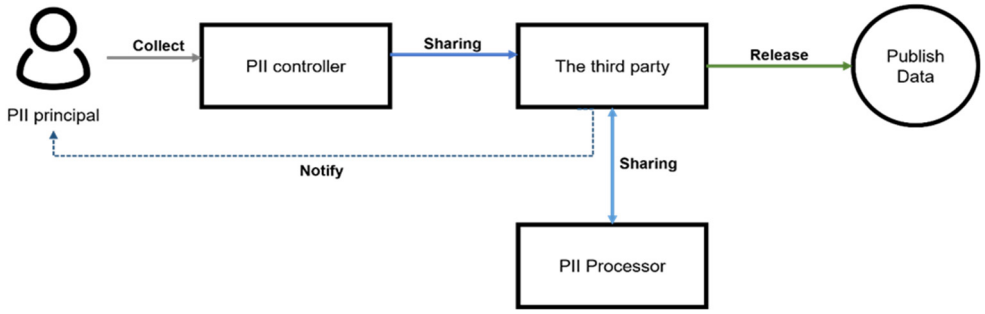

Figure 3. Privacy model of a centralized contact tracing system.

In this model, each party performs the following roles:

- PII: PII is data such as the phone number or credit card number of a data subject, the place where a credit card is used, and the location of the mobile base station.
- PII principal: A stakeholder who provides PII to classify whether they are a contact of an epidemic patient or is diagnosed as positive for an infectious disease. PII may include epidemic information and other information that could help to identify a recent contact including geological information. A PII principal could receive notification of exposure to an epidemic patient from the third party.
- PII controller: A stakeholder who collects PII and shares it to a third party. The collected information can be directly related to infection information such as diagnosis or other information to track a patient/contact path to identify other contacts [26], though a PII controller may need additional consent from a PII principal to use such data in this system. Medical institutions or private service providers related to geological/financial services can be PII controllers in this model.
- Third Party: A stakeholder receiving information from the PII controllers, who takes measures to prevent and manage epidemics and has an obligation to disclose information to share the status of outbreak and spread. Organizations could be a third party such as the Korea Centers for Disease Control and Prevention (KCDC), which oversees all health data processing, as well as local governments that carry out quarantine measures for infected persons/contacts [24].
- PII Processor: A stakeholder who processes data on behalf of a third party and can process data analysis, integration, and de-identification on behalf of a third party. If a third party operates a health information system by their own, a PII processor could help to establish or maintain such information systems [24]. PII processors include data service providers [24].

3.3. Data Processing Life Cycle

The data processing of the centralized contact tracing system may have six steps from collection to retention, as shown in Figure 4. The cycle includes the collection, sharing, processing, notification, release, and retention of data.

Figure 4. Data processing steps of the centralized contact tracing system.

- Data Collection

The data from a PII principal are collected by a PII controller [27]. The PII controller collects infection information and other contact data from infected persons to trace the

path and identify contact [24]. Collection from private PII controllers can only be practiced when it has permission from an authority to legally permit collection [24].

- Data Sharing

The data collected from PII controllers are shared to a third party to respond against epidemic diseases. If a PII principal is diagnosed as positive, the PII controller, such as epidemiological investigators or the medical institution that performed tests, reports the infection information to the third party and requests the third party to take quarantine measures [24]. The third party additionally receives data from PII controllers after permission is given by an authority such as a national police agency or credit association to further identify the contact, if necessary [24].

The third party should use the data provided by the PII controller only for the purpose of preventing, controlling, and treating infectious diseases. Such a process could include the aggregation of geological data to identify contact with an infected person or anonymization or de-identification to create the disease statistics to be used in a data release to the public. A third party may request a PII processor complete data analysis, aggregation, and anonymization on behalf of the third party, in accordance with instructions [24]. When a third party builds, maintains, and manages its own information system to process infection information, a PII processor could support the maintenance of such systems [24]. The PII processor processes the data and sends them to a third party after processing them for such a purpose. This information must only be used for the purposes of epidemic responses [23].

- Data Notification

When a PII principal is tested as positive or classified as a contact, the third party quickly notifies the PII principal of their status and quarantines them [28]. The third party receives the data, notifies PII principals that one has been in contact with a disease patient, and performs measures to prevent infectious diseases, such as quarantining a PII principal under their jurisdiction [28].

- Data Release

The third party releases the statistics of an infectious disease to inform the public about the outbreak and spread of the disease [23]. In order to do so, the third party could request the de-identification of PII processors that then only receive statistical information. Next, the third party conducts a data release and provides the media and the public with information about the status of medical institutions and contacts and the occurrence and testing of infectious diseases by region and age group [24].

- Data Retention and Deletion

All institutions must destroy all data when the purpose of an epidemic response is achieved, which must be destroyed without delay. For example, the data are destroyed after 4 weeks in regard to the impact of COVID-19 in Korea [29,30].

4. Security and Privacy Threats and Requirements

4.1. Security Threats and Requirements in ITU-T X.1121

In this study, we analyze the security and privacy threats and security requirements for the contact tracing system in Korea, as mentioned in Sections 4.2 and 4.4. However, there are security threats and requirements in ITU-T X.1121, which is the framework for security technologies for mobile end-to-end data communications. To analyze and identify more specific threats focusing on the centralized contact tracing system in Korea, we refer to ITU-T X.1121 and compare it with the security threats and the security–privacy threats in this study.

Table 3 shows the security threats and requirements in ITU-T X.1121 [31].

Table 3. Security threats and requirements in ITU-T X.1121.

Requirement \ Threat	Eavesdropping	Communication Jamming	Shoulder Surfing	Lost/Stolen Terminal	Unprepared Shutdown	Misreading/ Input Error
Identity management	X					
Communication data confidentiality	X					
Stored data confidentiality				X		
Communication data integrity						
Stored data integrity				X		
Entity authentication				X		
Message authentication						
Access control				X		
Non-repudiation						
Anonymity				X		
Privacy	X		X	X		
Usability						X
Availability		X			X	

We compared the security threats of ITU-T X.1121 with the threats derived by this paper. In addition, we could find additional threats related to the loss of terminals. Moreover, the security requirements for this additional threat were also addressed.

- Additional threat: Lost/stolen terminal
- Corresponding requirement: If a terminal is lost, people will not be able to receive the information related to it when they become a close contact. Therefore, various notification methods, such as e-mail notification, etc., for the recipient, that is, the closer contact, should be improved.

4.2. Security and Privacy Threats for the Contact Tracing System in Korea

This section lists the affectable security and privacy threats in the centralized privacy model of the mentioned system and maps each threat to the related entity, which are the affectable privacy threats to the privacy model of the health information system for epidemic alert and response:

ST1. Compromise of data confidentiality: threats to data being disclosed or available to the unintended entity;
ST2. Compromise of data integrity: threats to data being changed or destructed improperly;
ST3. Compromise of data availability: threats to data being accessed or used by unauthorized third parties;
ST4. Data recovery due to insufficient data deletion: threats to data being recovered from data storage, due to insufficient data deletion;
ST5. Degradation in data quality when processing: threats of data being corrupted or redundant due to processing on data such as de-identification and a failure to identify past or present physical proximity;
ST6. Malicious activities by internal attackers: threats of data being maliciously leaked by internal attackers from inside;
ST7. Use of unsecured tunneling protocol: protocol attacks caused by using versions to be vulnerable to communication protocols;
ST8. Lost/stolen terminal: threats to lost or stolen terminal such as mobiles;

PT1. Data use for purposes other than infectious disease responses: threats to data being used for purposes other than the prevention, management, and treatment of infectious diseases;
PT2. Unauthorized data transfer to third party: threats of data being acquired or provided to unauthorized third party by false or other fraudulent means or methods;
PT3. Insufficient legal and regulation grounds for PII processing: threats of insufficient legal grounds for collection of PII;

PT4. Excessive data processing beyond the intended purposes: threats of data being collected unreasonably because of too many attributes for the original purpose;
PT5. Data collection without the consent of a PII principal: threats in a process of collection when prior consent of a PII principal is not being obtained;
PT6. De-identification risk of re-identified data: the potential that some supposedly anonymous or pseudonymous data sets could be being de-anonymized to recover the identities of users [32];
PT7. Identification of a specific data from publicly announced data: threats to leak specific PII by using and combining publicly announced information or data such as the movement routes of people with infectious diseases;
PT8. Leakage of PII on a handwritten list: threat to leakage of a specific PII being written on a handwritten list when an individual enters various facilities.

Here, ST and PT mean security threat and privacy threat, in order to assign numbers to use in the mapping tables shown in Table 4.

Table 4. Security and privacy threats by stakeholders.

Stakeholders	Security and Privacy Threats															
	ST1	**ST2**	**ST3**	**ST4**	**ST5**	**ST6**	**ST7**	**ST8**	**PT1**	**PT2**	**PT3**	**PT4**	**PT5**	**PT6**	**PT7**	**PT8**
PII Controller	○	○	○	○		○	○	○	○	○			○			○
Third Party	○	○	○	○	○		○				○	○		○	○	
PII Processor	○	○	○	○	○		○				○	○		○		

○ means that relevance issue is addressed.

As can be seen from Table 4, two types of threats can occur for each stakeholder. Since the contact tracing system should collect and handle personal sensitive data, especially if the system is based on the centralized model, the threats that can occur are classified as general security or privacy. When analyzing threats such as the above, each stakeholder has two types of threats all, though a PII controller could have more privacy threats.

4.3. Mapping Security and Privacy Threats to LINDDUN and STRIDE Threat Models

In Section 4.2, we map the security and privacy threats derived in Section 4.1 to LINDDUN and STRIDE, which are security-threat modeling techniques. This would mean that the threats derived in this study are complete. LINDDUN is a privacy-threat modeling methodology that supports analysts in systematically eliciting and mitigating privacy threats in software architectures [33]. The STRIDE models were developed by Microsoft for categorizing threats. The classification of threats in this model is accomplished by categorizing the kind of exploit done by an attacker or intruder [34].

The LINDDUN model has seven threat categories, and each category is as follows:

- **L (Linkability):** An adversary is able to link two items of interest without knowing the identity of the data subjects involved [33];
- **I (Identifiability):** An adversary is able to identify a data subject from a set of data subjects through an item of interest [33];
- **N (Non-repudiation):** The data subject is unable to deny a claim [33];
- **D (Detectability):** An adversary is able to distinguish whether an item of interest about a data subject exists or not, regardless of being able to read the contents itself [33];
- **D (information Disclosure):** An adversary is able to learn the content of an item of interest about a data subject [33];
- **U (content Unawareness):** The data subject is unaware of the collection, processing, storage, or sharing activities and the corresponding purposes of their personal data [33];
- **N (policy and consent Non-compliance):** The processing, storage, or handling of personal data is not compliant with legislation, regulation, and/or policy [33].

The mapping table for each category of the derived threat and LINDDUN is shown in Table 5.

Table 5. Security–privacy threats and LINDDUN mapping lists.

No.	Threats	L	I	N	D	D	U	N
ST1	Compromised data confidentiality					○		
ST2	Compromised data integrity			○				
ST3	Compromised data availability					○		
ST4	Data recovery due to insufficient data deletion					○		
ST5	Degradation in data quality when processing	○	○					
ST6	Malicious actions by internal attackers		○		○	○		
ST7	Risk of using unsecure tunneling protocol							○
ST8	Lost/stolen terminal						○	
PT1	Data use for purposes other than infectious-disease responses							○
PT2	Data transfer to unauthorized third party						○	
PT3	Insufficient legal basis for PII collection							○
PT4	Excessive data collection and use beyond purpose					○		○
PT5	Data collection without consent of PII principal	○	○					○
PT6	Risk of re-identification due to data combination	○	○					
PT7	Threats to know a specific subject of information using publicly announced information	○	○					
PT8	Leakage of PII on the handwritten list	○	○			○		

○ means that relevance issue is addressed.

The STRIDE model has 7 threat categories, and each category is as follows:

- **S (Spoofing):** Spoofing or "identity spoofing" is a scenario in which a user X pretends to be a user Y by changing their identity or data and, thus, gains illegal access to data [35];
- **T (Tampering):** Tampering refers to the change of data by an illegal person who is not authorized to modify them [35];
- **R (Repudiation):** Repudiation relies on the fact that a security system must always be able to trace the entity responsible for any illegitimate modification and illegal access of resource or account [35];
- **I (Information disclosure):** Information disclosure assists an attacker or malicious user in accessing confidential information that they are not permitted to view [35];
- **D (Denial of service):** A denial-of-service (DoS) attack is an attempt to disturb a resource, network, or system in such a way that an intended and valid user would not be able to use it [35];
- **E (Elevation of privilege):** Elevation of privilege is the category of attacks in which an intruder gains authorization to access more than what has been granted originally [35].

The mapping table for each category of the derived threat and STRIDE is shown in Table 6.

Table 6. Security threats and STRIDE mapping list.

No.	Threats	S	T	R	I	D	E
ST1	Compromised data confidentiality				○		
ST2	Compromised data integrity		○	○			
ST3	Compromised data availability						○
ST4	Data recovery due to insufficient data deletion				○		
ST5	Degradation in data quality when processing					○	
ST6	Malicious actions by internal attackers				○		
ST7	Risk of using unsecured tunneling protocol	○		○			
ST8	Lost/stolen terminal	○	○		○		

○ means that relevance issue is addressed.

4.4. Security and Privacy Requirements for the Contact Tracing System in Korea

This section provides the security requirements to mitigate the listed privacy and security threats identified in Section 4.1 and enhance the privacy and security for the centralized privacy model of a contact tracing system. The security requirements for responding to the security and privacy threats mentioned above are as follows.

- **SR1. Processing based on legal and regulation grounds:** There are seven types of PII data to collect (location data, personally identifiable information, medical and prescription records, immigration records, credit/debit and prepaid card transaction data, public transportation use records, and CCTV images); however, only necessary information should be collected, and the consent of the data subject should be checked. In this case, if it is required or permitted by law, the above may not be considered. When providing to a third party, it is necessary to identify whether there is any personal information to be provided and to review what kind of disadvantage there is to the information subject if the information subject does not agree.
- **SR2. Minimizing data collection:** Obtaining the consent of the data subject is of the highest priority. PII should be collected and used only within the scope of the agreed purpose (conclusion and implementation), and multiple pieces of PII with similar characteristics should not be collected for the same purpose. Information automatically generated in the process of using a website, such as cookies, should be collected minimally.
- **SR3. Ensuring individual rights of PII:** When the PII controller collects PII with the consent of the data subject, the following needs to be ensured: (1) the contents of the consent, (2) the fact that the data subject has the right to refuse consent, and (3) the contents of the disadvantage if there is a disadvantage due to the refusal of consent should be specified specifically. In addition, the consent of the data subject is premised on a substantive right of choice. Even if the information subject does not agree to the optional items, a service provider cannot refuse to provide the service [35].
- **SR4. Strong access control:** Data access rights for each component of the PII processing model should be set, and a system should be established so that the data can be accessed according to the level of authority.
- **SR5. Use of a strong encryption mechanism:** Access control and restriction on PII, encryption technology, or equivalent measures that can safely store and transmit PII should be applied.
- **SR6. Providing data integrity:** In the process of sending PII (data sharing), passwords, bio information, and unique identification information must be encrypted before transmission. Theymust be encrypted and stored. The encryption technique used when data transmission is transmitted must be using a symmetric key encryption algorithm or a public key encryption algorithm; when data are stored in the system, they must be stored using a one-way encryption algorithm such as a hash function.
- **SR7. Data backup for availability:** Due to the characteristics of PII, media such as a tape or external USB are judged to be inappropriate, so it is considered appropriate to store data on media such as a disk or in the cloud. Even when backing up PII, it is necessary to store encrypted data rather than plain text; in the case of data storage, data should be located on the internal network rather than on an external network or DMZ.
- **SR8. Use of a complete data-deletion mechanism:** After the PII controller achieves the purpose for the user's PII, when the retention and use period ends, a PII controller should destroy the PII without delay [22,36]. When PII is destroyed, it must be destroyed in a way that cannot be restored or reproduced.
- **SR9. Data processing only for the intended purposes:** In the case of establishing an internal management plan to block the use of data for anything other than the intended purpose and requesting an external party to process PII, the purpose for which the PII processor can process PII must be determined in advance.

- **SR10. Prevention from inside attacks:** Since it is impossible to apply security policies to internal attackers with a firewall, security procedures should be clarified and checked regarding whether they are being continuously implemented.
- **SR11. Use of de-identification techniques:** The appropriateness of data de-identification measures should be evaluated to ensure that necessary identification information is used after de-identification measures. Measures to monitor the possibility of re-identification of de-identified information should be taken, and, when outsourcing the processing of pseudonymous information, the contract should include notification of the prohibition of re-identification, restrictions on re-supply/re-entrustment, and notification of the risk of re-identification.
- **SR12. Use of a strong end-to-end encryption protocol with authentication such as SSH (Secure Shell):** The latest version of the secure and secure tunneling protocol should be made sure to provide encrypted communication sessions. SR12 can counter ST2 and ST7 threats.
- **SR13. Use of data anonymization:** All information collected for tracking is converted into anonymous information and announced. SR13 can counter PT7 threats.
- **SR14. Providing various notification methods:** If a terminal is lost, people will not be able to receive the information related to it when they become a close contact. Therefore, various notification methods, such as e-mail notification, etc., for the recipient, that is, the closer contact, should be improved.

Table 7 shows the 1:1 or 1:N mapping data of the model's security and privacy threats for the corresponding security requirements.

Table 7. Security–privacy threats and security requirements mapping list.

Security and Privacy Threats	Security Requirements													
	SR1	**SR2**	**SR3**	**SR4**	**SR5**	**SR6**	**SR7**	**SR8**	**SR9**	**SR10**	**SR11**	**SR12**	**SR13**	**SR14**
ST1				○	○									
ST2						○						○		
ST3				○			○							
ST4								○						
ST5											○			
ST6										○				
ST7												○		
ST8														○
PT1									○					
PT2				○										
PT3	○		○											
PT4	○	○							○					
PT5	○		○											
PT6											○			
PT7													○	

ST: security threats, PT: privacy threats. ○ means that relevance issue is addressed.

5. Conclusions

This study demonstrates a centralized contact tracing system for infectious diseases focusing on a case study of the Republic of Korea, and it derives the security and privacy threats to that system. In addition, we identify corresponding security requirements for each threat one by one. Thirteen security requirements are provided to mitigate the threats for the system.

The centralized contact tracing system identifies subjects who have close contact with confirmed cases in specific partitioned spaces such as restaurants, offices, theatres, etc., based upon the substantial data control of PII. Hence, there need to be considerations such as scanning QR codes, including the PII of a subject, calling a designated official phone number provided by government offices to record subjects' visits, and obligatorily writing

down the names and phone numbers on provided, formatted papers when subjects visit specific places.

It means that centralized models can undermine PII sovereignty over data. Since the privacy model of a centralized contact tracing system can have specific security requirements against threats that occur when the legal basis for PII collection is insufficient, the consent of the PII subject is not obtained in the process of data collection. Therefore, a strengthened collection process should be established to secure a legal basis for collecting data from PII subjects and prevent the invasion of the privacy of PII subjects, to utilize the centralized contact tracing system securely. In addition, more secure use of the centralized contact tracing system can be promoted by considering the threats identified in this paper and the corresponding security and privacy requirements.

As a future work, in-depth and intensive comparison studies regarding various types of contact tracing systems, such as centralized, decentralized, and hybrid-based contact tracing systems, will be carried out in terms of their security and privacy aspects.

Author Contributions: Conceptualization, S.P. and H.-Y.Y.; methodology, S.P. and H.-Y.Y.; validation, S.P. and H.-Y.Y.; formal analysis, S.P. and H.-Y.Y.; investigation, S.P. and H.-Y.Y.; resources, S.P. and H.-Y.Y.; writing—original draft preparation, S.P. and H.-Y.Y.; writing—review and editing, S.P. and H.-Y.Y.; visualization, S.P. and H.-Y.Y.; supervision, S.P. and H.-Y.Y.; project administration, S.P. and H.-Y.Y.; funding acquisition, H.-Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by an Institute of Information and Communications Technology Planning and Evaluation (IITP) of Korea grant, funded by the Ministry of Science and ICT of Korea under grant number 2021-0-00112.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

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

References

1. Shahroz, M.; Ahmad, F.; Younis, M.S.; Ahmad, N.; Kamel Boulos, M.N.; Vinuesa, R.; Qadir, J. COVID-19 digital contact tracing applications and techniques: A review post initial deployments. *Transp. Eng.* **2021**, *5*, 100072. [CrossRef]
2. World Health Organization. Available online: https://innov.afro.who.int/global-innovation/robert-robust-and-privacy-preserving-proximity-tracing-protocol-1827 (accessed on 25 September 2022).
3. Github. Available online: https://github.com/DP-3T/documents (accessed on 25 September 2022).
4. Hogan, K.; Macedo., B.; Macha., V.; Barman., A.; Jiang., X. Contact Tracing Apps: Lessons Learned on Privacy, Autonomy, and the Need for Detailed and Thoughtful Implementation. *JMIR Med. Inform.* **2021**, *9*, 27449. [CrossRef] [PubMed]
5. Boutet., A.; Castelluccia., C.; Cunche., M.; Lauradou., C.; Roca., V.; Baud., A.; Raverdy., P. Desire: Leveraging the Best of Centralized and Decentralized Contact Tracing Systems. *Digit. Threat. Res. Pract.* **2022**, *3*, 1–20. [CrossRef]
6. Giuseppe, G.; Tim, H.; Davy, P.; Wouter, J.; Aysajan, A.; Mustafa, A.M. PIVOT: PrIVate and effective cOntact Tracing. *IEEE Internet Things J.* **2021**, *9*, 22466–22489. [CrossRef]
7. Johannes, M.; Kretzschmar, M. Contact tracing—Old models and new challenges. *Infect. Dis. Model.* **2021**, *6*, 222–231. [CrossRef]
8. Park, S.; Choi, G.J.; Ko, H. Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies. *JAMA Netw. Open* **2020**, *323*, 2129–2130. [CrossRef] [PubMed]
9. Jian, S.-H.; Cheng, H.-Y.; Huang, X.-T.; Liu, D.-P. Contact tracing with digital assistance in Taiwan's COVID-19 outbreak response. *Intern. J. Infect. Dis.* **2020**, *101*, 348–352. [CrossRef] [PubMed]
10. Garrett, P.M.; Wang, Y.-W.; White, J.P.; Kashima, Y.; Dennis, S.; Yang, C.-T. High acceptance of COVID-19 Tracing Technologies in Taiwan: A nationally representative survey analysis. *Int. J. Environ. Res. Public Health* **2022**, *19*, 3323. [CrossRef] [PubMed]
11. Yanji, P.; Dongyue, C. Privacy Analysis and Comparison of Pandemic Contact Tracing Apps. *KSII Trans. Internet Inf. Syst.* **2021**, *15*, 4145–4162. [CrossRef]
12. 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. [CrossRef]
13. UK Health Security Agency. NHS COVID-19 App. 13 May 2022. Available online: https://www.gov.uk/government/collections/nhs-covid-19-app (accessed on 23 September 2022).
14. Liang, F. COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China. *Soc. Media Soc.* **2020**, *6*, 2056305120947657. [CrossRef] [PubMed]

15. Bay, J.; Kek, J.; Tan, A.; Hau, C.S.; Yongquan, L.; Tan, J.; Quy, T.A. *BlueTrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing across Borders*; Government Technology Agency: Singapore, 2020.
16. PEPP-PP. PEPP-PT Documentation. 2020. Available online: https://github.com/pepp-pt/pepp-pt-documentation (accessed on 23 September 2022).
17. Troncoso, C.; Payer, M.; Hubaux, J.P.; Salathé, M.; Larus, J.; Bugnion, E.; Lueks, W.; Stadler, T.; Pyrgelis, A.; Antonioli, D.; et al. Decentralized Privacy-Preserving Proximity Tracing. *arXiv* **2020**, arXiv:2005.12273. [CrossRef]
18. Small, L.S.; John, H.; Matt, H.; Nathaniel, L. Summary of Bluetooth Contact Tracing Options. 2020. Available online: https://www.dta.mil.nz/assets/Publications/Bluetooth-Contact-Tracing-Options.pdf (accessed on 23 September 2022).
19. Google. Exposure Notifications: Help Slow the Spread of COVID-19, with One Step on Your Phone. 2020. Available online: https://www.google.com/covid19/exposurenotifications/ (accessed on 23 September 2022).
20. Kintvedt, M.N. COVID-19 Tracing Apps as a Legal Problem: An Investigation of the Norwegian 'Smittestopp' App. *Oslo Law Rev.* **2021**, *8*, 69–87. [CrossRef]
21. Jhanwar, M.P.; Sarkar, S. Phyct: Privacy Preserving Hybrid Contact Tracing. *IACR Cryptol. ePrint Arch.* **2020**, *2020*, 793.
22. Development Asia. COVID-19 Smart Management System (SMS) in Korea. Available online: https://events.development.asia/system/files/materials/2020/04/202004-covid-19-smart-management-system-sms-republic-korea.pdf (accessed on 25 September 2022).
23. Reliable Ministry of Government legislation Korean Law Information Center. Infectious Disease Control and Prevention Act. Available online: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%90%EC%97%BC%EB%B3%91%EC%9D%98%EC%98%88%EB%B0%A9%EB%B0%8F%EA%B4%80%EB%A6%AC%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0 (accessed on 25 September 2022).
24. ICT Standardization Committee. TTAK.KO-12.0376:Privacy Protection Guidelines for Infectious Diseases Control and Prevention. Available online: https://committee.tta.or.kr/data/standard_view.jsp?order=t.publish_date&by=desc&nowPage=1&pk_num=TTAK.KO-12.0376&commit_code=TC5 (accessed on 25 September 2022).
25. Jeon, H. Official Operation of the 'COVID-19 Epidemiological Investigation System' on the 26th and Identify the Movement of Confirmed Patients. 2020. Available online: https://www.news1.kr/articles/?3884765 (accessed on 24 September 2022).
26. LX Spatial Information Research Institute. Available online: https://lxsiri.re.kr/frt/biz/bbs/selectBoardArticle.do?bbsId=BBSMSTR_000000000221&nttId=7323 (accessed on 27 April 2022).
27. International Organization for Standardization (ISO). ISO/IEC 29100:2011; Information Technology—Security Techniques—Privacy Framework. Available online: https://www.iso.org/standard/45123.html (accessed on 25 September 2022).
28. Korea Disease Control and Prevention Agency. Available online: https://www.kdca.go.kr/contents.es?mid=a20301110100 (accessed on 28 April 2022).
29. Korea Policy Briefings. Available online: https://www.korea.kr/news/policyNewsView.do?newsId=148895400#sitemap-layer (accessed on 25 September 2022).
30. Ministry of Land, Infrastructure and Transport (MOLIT). Available online: http://www.mohw.go.kr/react/al/sal0301vw.jsp?PAR_MENU_ID=04&MENU_ID=0403&CONT_SEQ=359845 (accessed on 25 September 2022).
31. International Telecommunication Union(ITU-T). ITU-T X.1121: Framework of Security Technologies for Mobile End-To-End Data Communications. Available online: https://www.itu.int/rec/T-REC-X.1121/en (accessed on 24 September 2022).
32. Google Cloud. Available online: https://cloud.google.com/blog/products/identity-security/taking-charge-of-your-data-understanding-re-identification-risk-and-quasi-identifiers-with-cloud-dlp (accessed on 1 May 2022).
33. LIDDUN. Available online: https://www.linddun.org/linddun (accessed on 12 February 2022).
34. Khan, S.A. A STRIDE Model based Threat Modelling using Unified and-Or Fuzzy Operator for Computer Network Security. *Int. J. Comput. Netw. Technol.* **2017**, *5*, 13–20. [CrossRef] [PubMed]
35. Lee, I.; Keh., J.S. Cross-Border Transfers of Personal Data and Practical Implications. *J. Korean L.* **2017**, *17*, 33–52.
36. Korea Legislation Research Institute. Personal Information Protection Act. Available online: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG (accessed on 15 July 2022).