An Internet of Things (IoT) Reference Model for an Infectious Disease Active Digital Surveillance System

Nur Hayati, Kalamullah Ramli, Muhammad Suryanegara, Muhammad Salman
Department of Electrical Engineering, Universitas Indonesia, Depok, Indonesia

***Abstract*—Internet of Things (IoT) technological assistance for infectious disease surveillance is urgently needed when outbreaks occur, especially during pandemics. The IoT has great potential as an active digital surveillance system, since it can provide meaningful time-critical data needed to design infectious disease surveillance. Many studies have developed the IoT for such surveillance; however, such designs have been developed based on authors' ideas or innovations, without consideration of a specific reference model. Therefore, it is essential to build such a model that could encompass end-to-end IoT-based surveillance system design. This paper proposes a reference model for the design of an active digital surveillance system of infectious diseases with IoT technology. It consists of 14 attributes with specific indicators to accommodate IoT characteristics and to meet the needs of infectious disease surveillance design. The proof of concept was conducted by adopting the reference model into an IoT system design for the active digital surveillance of the Covid-19 disease. The use-case of the design was a community-based surveillance (CBS) system utilizing the IoT to detect initial symptoms and prevent closed contacts of Covid-19 in a nursing home. We then elaborated its compliance with the 14 attributes of the reference model, reflecting how the IoT design should meet the criteria mandated by the model. The study finds that the proposed reference model could eventually benefit engineers who develop the complete IoT design, as well as epidemiologists, the government or the relevant policy makers who work in preventing infectious diseases from worsening.**

Keywords*—IoT; framework; digital surveillance; infectious disease; Covid-19

I. Introduction

The current Covid-19 pandemic era has taught us the importance of conducting surveillance of people who are carriers of infectious diseases. Such surveillance will provide the opportunity for medical personnel to monitor and avoid adverse events in the future. Infectious disease surveillance is a process that starts with data collection on the diseases and other relevant factors and is conducted continuously and systematically. It continues with a dynamic analysis of the disease spread from three different perspectives: temporal, spatial, and populational. This process aims to observe trends and current situations, and to provide data to help decide preventative measures and to control related diseases [1][2]. Therefore, the surveillance process is divided into the collection, analysis and interpretation, and dissemination of data [3][4].

The Internet of Things (IoT) is a technology with great scope for adoption as a tool in the digital surveillance of infectious diseases [5]. Functionally, IoT has the capacity to conduct an active surveillance process through the support of technological integration [2]. The IoT collects real data from sensors embedded in the end device, sends them to the data processing system, and shares the results in either real-time or through scheduling. Those activities demonstrate the IoT's ability to perform the surveillance process from start to end [6].

Many studies have been made of the development of the IoT for surveillance of infectious diseases [6][7][8][9]. However, such designs were developed based on the authors' own ideas or innovations, without taking into account a specific reference model. Therefore, it is important to build such a model which encompasses end-to-end system design.

This paper proposes a reference model for the design of an active digital surveillance system of infectious diseases employing IoT technology. We utilized the framework of the Center for Disease Control (CDC) surveillance evaluation [10][11][12], which consists of 10 parameters ranging from usefulness to representativeness, to which we added two modified parameters of security and standard [13][14], together with two others related to the essential concerns of mobility and sustainability. These framework constructs comprise the 14 new attributes of the reference model. Each of the attributes has specific indicators, which we customized to accommodate IoT characteristics and to meet the needs of infectious disease surveillance design.

To verify our proposal, we tested the reference model on a conceptual IoT design as a Covid-19 digital surveillance system. We analyzed the compliance of such a system design with the 14 attributes of our proposed reference model. The design of the Covid-19 digital surveillance system consisted of IoT end devices, local server, IoT gateway, internet connection, cloud server, and users' end-devices.

This work contributes to the work of designers or engineers on developing a complete IoT system for active surveillance of any infectious disease. The model can be used as a reference to evaluate whether their end-to-end design meets essential engineering parameters, as reflected by the 14 attributes in the reference model. The work should also eventually benefit epidemiologists, governments, or relevant policy makers. For example, the data quality attribute reflects epidemiologists' concerns over the completeness and validity of data. Compliance with this attribute will ensure that the system provides valid data, which will help epidemiologists advising the government or policy makers in making appropriate interventions to prevent infectious diseases from worsening.

Hibah Penelitian Disertasi Doktor, Kementerian Riset Dan Teknologi/Badan Riset Dan Inovasi Nasional, Indonesia

The remainder of the paper is organized into sections addressing the theories of the IoT as a surveillance system (Section II); the IoT as a form of active digital surveillance of infectious diseases (Section III); the reference model that we are proposing (Section IV); discussion of the proof of the concept (Section V); and the conclusion to the study (Section VI).

II. Theoretical Approach: The IoT as a Surveillance System

A. An Infectious Disease Surveillance System based on Digital Technology

The development of digital technology has reached the health-related sector, including the digital surveillance of infectious diseases [15]. Such surveillance can be conducted with either an active or passive approach, according to the data collection method [16]. Passive surveillance is generally performed by monitoring query logs from the users' search engines, keywords on the web, and hashtags on social media, to obtain the most widely circulated data related to infectious diseases, followed by analysis of the data [17]. Google Flue Trends is an example of an internet-based surveillance application which provides information about early detection systems for epidemics. The application was built based on trend data from the processing of users' keywords to search for disease information. This was then validated by matching the trend with confirmed case data from the laboratory [17]. Although passive surveillance obtains the data more quickly, it does not fully represent detailed geographic and demographic information [14]. Therefore, J.K. Harris et al. [18] concluded that technology is needed that allows the surveillance process to involve active participation from the community.

An example of active digital surveillance is reporting from the public through an online system. This means that the public's active participation using technological platforms is needed to obtain more accurate information [19]. However, such a reporting mechanism requires intense public intervention. The IoT is an alternative technological solution, which is suitable for active digital surveillance by utilizing sensors embedded in the IoT end devices (wearable medical devices) to collect specific data related to the disease. This solution made IoT minimizing users' efforts and concentrated intervention in the data reporting process.

B. The IoT as an Active Digital Surveillance System

The IoT has advantages in terms of processing speed and system automation [20]. Compared to traditional surveillance, internet-based technology has features which can automatically detect infectious diseases more quickly [17]. For such diseases, computing speed is valuable for shortening their detection time, allowing preventive measures to be taken immediately [21] [22]. System automation increases surveillance efficiency when disease transmission incidents occur on a large scale [7][14], and also effectively reduces the workload of medical personnel in pandemic situations [13].

Another advantage of the IoT is its technological ability to provide quality data [14], which are derived from the aggregated sources. The aggregated source completes the data to facilitate analysis, early detection, surveillance, and monitoring of the emergence of infectious diseases [23]. This advantage overcomes the shortcomings of traditional surveillance systems which result in incomplete reporting data on the emergence of infectious diseases due to limited resources, time, and reporting systems [17]. Because of these advantages, we are optimistic that the IoT can provide the meaningful time-critical data needed by infectious disease surveillance systems.

Several studies have developed the IoT as an active digital surveillance system for infectious diseases. In the case of Ebola, research [6] proposed as a framework to assist in detecting and monitoring patients suspected of being infected with the disease. The framework integrated RFID technology, wearable sensors, 3G/4G wi-fi internet connections, and cloud computing. In another example, in the respiratory infection SARI, the IoT was employed to prevent and treat the disease, to improve patient management, and to provide effective consultation [7]. According to Y. Song et al., in their research [7], the IoT infrastructure was used to develop long-distance communication between patient devices, hospitals, and medical equipment to manage SARI.

Research on the IoT for an infectious disease surveillance system can be implemented on a small and large scale. Research on the IoT as a small-scale surveillance system was conducted by Lundrigan et al. [9], who built an IoT-based monitoring system on a household scale to help epidemiologists observe disease exposure through the sensor data. In addition, research on larger scale implementation of the IoT was conducted by Nsoesie et al. [15], which found that mass gatherings with high densities, with residents close to each other, increased the risk of spreading diseases. Consequently, the IoT was utilized as early detection technology for controlling disease spread at mass gatherings [15]. Additionally, on a global scale, Zhu et al. [8] demonstrated IoT's ability to quickly perform detection and monitoring of infectious disease using cost-effective point-of-care (POC) diagnostic devices connected to the internet.

III. IoT Infrastructure for an Active Digital Surveillance System of Infectious Diseases

A. Illustration and Interpretation of an IoT Infrastructure for the Infectious Disease Surveillance Process

IoT is a technology whose infrastructure consists of four-layers of protocols with different technologies and functions on each layer. However, they complement each other in constructing an IoT-based end-to-end technology solution. The protocols comprise the sensing and identification layer, network infrastructure layer, data processing layer, and integrated application layer. This section maps each IoT layer onto each surveillance process to adjust the layer functionality of the IoT infrastructure in surveillance operations. In the IoT infrastructure design, infectious disease surveillance consists of four processes: collection, transmission, analysis and interpretation, and dissemination of data.

A visualization of the interpretation of the infectious disease surveillance process by the IoT infrastructure is shown in Fig. 1. According to the illustration, the surveillance process can be interpreted as follows. The data collection process

reflects the functionality of the sensing and identification layer. In the IoT design, the data transmission process realizes the tasks of the network infrastructure layer, while the dynamic analysis and interpretation realize the function of the data processing layer. Dissemination of data to provide evidence for the surveillance process performs the integrated IoT application layer function.

Active digital infectious disease surveillance begins with primary data collection from the community utilizing sensor technology. Data gathered from the sensor is then sent automatically to the data processing center over the transmission media. This automatic data transmission process is the fundamental difference between traditional and IoT surveillance systems. In traditional surveillance, officers collect data manually, input them into the system, and then distribute them. The following surveillance process is dynamic analysis and interpretation, which can be performed more quickly in IoT due to the supporting intelligent system features in its data processing center. The output of data processed by the IoT intelligent system is used to provide surveillance data ready to be disseminated as evidence.

B. Supporting Technology to the Design of an IoT Infrastructure Used for the Active Digital Surveillance System of Infectious Diseases

Each process in the active digital surveillance system requires supporting technology. For the collection of data in the IoT design, this is supported by sensors, which are usually embedded in the end device. Fig. 2 presents a technical diagram of the functions and types of sensor employed as data collection technology in IoT. The sensors can be categorized into three types:

- A sensor-type actuator, which operates by receiving stimuli then converting them into electrical signals.
- A network-based sensor type, which generates data via wireless communication between the transmitter and its receiver, and is characterized by integration of the transceiver with the IoT system.
- The Tags type sensor, which uses identifiers/codes that are scanned/tagged to obtain the data.

Both wired and wireless technologies support IoT in the process of transmitting surveillance data. In the IoT design, wired technology is generally used to provide a high-speed network connection of the aggregated systems in a data center. On the other hand, wireless technology is used from IoT end devices to the gateway due to its design flexibility, which supports user mobility and installation simplicity during implementation. Fig. 3 presents considerations when choosing data transmission media. Internet service providers (ISPs) normally handle high-speed data transmission to data centers, with either wired or wireless connections, while the connection from the IoT end device to its gateway is generally an option selected by the developer when building a surveillance system.

Supporting technology for analyzing and interpreting surveillance data on the IoT include cloud computing, fog computing, edge computing, and cloudlets. Fig. 4 shows a diagram of the data processing technology function and options. Several factors need to be considered when selecting the technology, including the amount of data being processed, network connections, and the capacity of the data processing resources. Centralized processing utilizes cloud computing technology equipped with an intelligent system. In contrast, distributed data processing employs fog computing and edge computing technology. In addition, cloudlets are an option if the surveillance requires a distributed data processing system in many locations with light processing loads. These employ resource sharing to ease the burden on the data processing system. Distributed processing shortens the data path taken and the data transmission time.

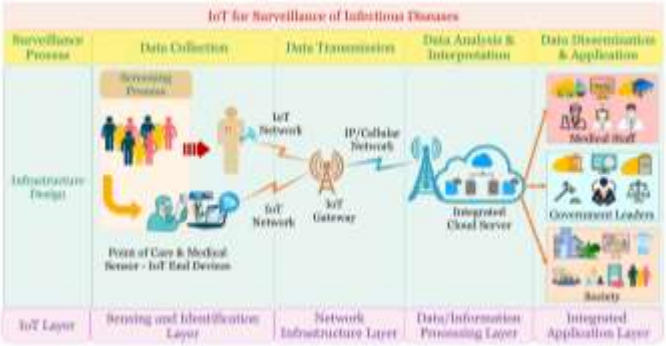

Fig. 1. Interpretation of the IoT Infrastructure as an Infectious Disease Surveillance System.

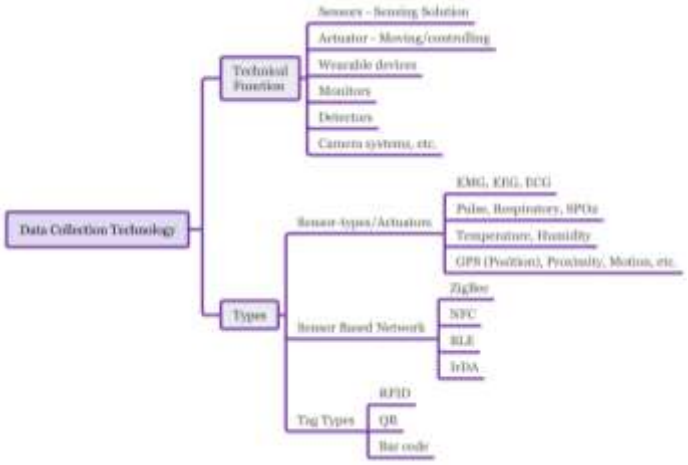

Fig. 2. Diagram Functions and Types of Data Collection Technology.

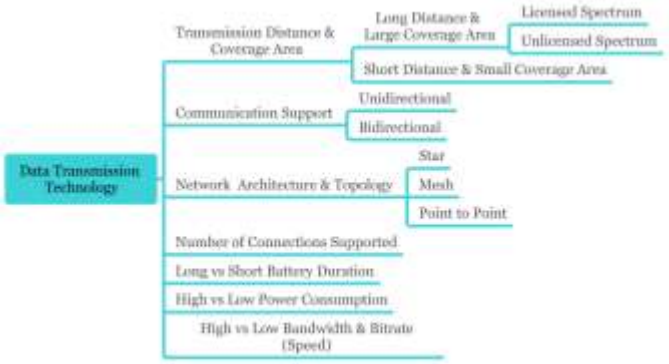

Fig. 3. Diagram of the Factors for Consideration when Selecting Data Transmission Technology.

Fig. 4. Diagram Functions and Types of Data Collection Technology.

In IoT design, surveillance data are disseminated online via web-based or mobile-based applications. Web-based ones are more suitable with respect to the data processing center. On the end-user side, mobile applications employing the CoAP (Constrained Application Protocol) or MQTT (Message Queue Telemetry Transport) protocols are more suitable because of the IoT environment.

IV. A Reference Model for the Design of an IoT-based Active Digital Surveillance System of Infectious Diseases

This section describes our proposed reference model for the design of an IoT-based active digital surveillance system of infectious diseases. The model consists of 14 attributes divided into several technical detail indicators. We customized the indicators of each attribute to accommodate IoT characteristics and meet the needs of infectious disease surveillance design. We derived ten of the 14 attributes from the CDC's surveillance evaluation with their modified indicators [10][11][12]. We adapted two attributes from the papers by R. P. Singh, M. Javaid, A. Haleem, and R. Suman in [13] and by S. L. Groseclose and D. L. Buckeridge in [14]. We then added the remaining two attributes, namely mobility and sustainability. Table I presents the proposed reference model, comprising the 14 attributes together with their respective indicators.

Unlike the case of noninfectious diseases, infectious disease surveillance requires control of the disease spread through contact tracing mechanisms. Therefore, the mobility attribute plays an important role in complying with the basic need for infectious disease surveillance. In addition, IoT technology has a relatively long-life span, so maintaining sustainability in its implementation is necessary, especially when the IoT is employed in the health sector. Several indicators, such as maintenance, inspection, evaluation, and auditing, are essential for maintaining sustainability and preventing any technical issues from arising in the IoT surveillance system.

1) ATTRIBUTE #1: USEFULNESS: Attribute #1 refers to the usefulness needed to align the IoT design with the surveillance objectives and to ensure that the IoT infrastructure and service benefit the IoT-based surveillance. This attribute consists of two indicators, applicability and customizability. The applicability indicator refers to the adjustment of IoT technological capabilities to the design needs for epidemiological surveillance, while the customizability indicator refers to a customizable IoT design for a single or multi-purpose surveillance system.

2) ATTRIBUTE #2: DATA QUALITY: Attribute #2 refers to the data quality demanded by epidemiologists to determine the most appropriate interventions for infectious disease. This attribute is realized by two indicators: data completeness and data validity. Data completeness is generated through the IoT infrastructure, which acts as global healthcare and monitoring technology to increase data gathering in the system [5]. In addition, the IoT is designed to run a verification program to validate all the data entering the system.

TABLE I. Proposed Reference Model for the Design of an IoT-based Active Digital Surveillance System of Infectious Diseases

No	Reference Model Attribute	Reference Model Indicator
1	Usefulness	Applicability
		Customizability
2	Data Quality	Data completeness
		Data validity
3	Timeliness	Rapidity
		Timeliness
4	Flexibility	Adaptability
		Scalability and extensibility
5	Simplicity	Manageability
		Automatic system
6	Acceptability	Interoperability
		Compatibility
		User friendly
7	Stability	Reliability and availability
		Accessibility
8	Sensitivity	Precision
		Threshold configuration
		Calibration
9	Positive Predictive Value	Accuracy
10	Representativeness	Data Synchronization
		Data traceability
11	Security	Infrastructure and management security
		Data security and privacy
12	Standards	Standardization
		Regulation
		Certification
13	Mobility	Tracking system
		Handover and roaming
		Portability
14	Sustainability	Maintenance
		Inspection
		Evaluation and audit

3) ATTRIBUTE #3: TIMELINESS: Attribute #3 refers to the timeliness of the surveillance system. This attribute plays an important role in reporting the emergence of infectious diseases, finding suspects of the infectious disease, and preventing the disease from spreading in outbreak situations. In an IoT-based system designed for infectious disease surveillance, the timeliness attribute is divided into two indicators, rapidity and timeliness.

4) ATTRIBUTE #4: FLEXIBILITY: Attribute #4 refers to the flexibility of design related to surveillance needs. A surveillance system should be flexible, able to follow the changes in epidemiological patterns, information needs, clinical practice, reporting sources, and other required changes [4][11] [14]. The attribute of flexibility consists of two indicators: adaptability and scalability and extensibility. Adaptability refers to IoT infrastructure and platforms that are able to keep up with changes in the surveillance environment. Scalability and extensibility refer to changes in the levels of hardware, software, and services that can be added or subtracted physically or logically.

5) ATTRIBUTE #5: SIMPLICITY: Attribute #5 refers to simplicity, meaning the ease of operating the surveillance system. In IoT design, the simplicity attribute is realized through two indicators: manageability and automatic systems. Manageability is concerned with managing the complex IoT systems to obtain full visibility from a series of processes that work automatically [24]. Technically, the IoT can be managed in a centralized or distributed manner. An automatic system allows the IoT infrastructure operational design to work automatically, thus reducing human intervention.

6) ATTRIBUTE #6: ACCEPTABILITY: Attribute #6 refers to acceptability, which has three indicators: interoperability, compatibility, and user friendly. The acceptability attribute in IoT-based surveillance is defined as the system's ability to involve technology as a surveillance provider, and the community as surveillance users. Involvement of technology in systems is realized through the interoperability and compatibility indicators, while community engagement in accessing the system is facilitated through a user-friendly design.

7) ATTRIBUTE #7: STABILITY: Attribute # 7 refers to stability in the performance of IoT-based surveillance systems. This attribute is supported by indicators of accessibility, availability and reliability. The accessibility indicator ensures that the available resources are accessible by users, while reliability and availability are related to determination of the Service Level Agreement (SLA) value of the built surveillance systems, which is affected by agreements with supporting parties as service providers.

8) ATTRIBUTE #8: SENSITIVITY: Attribute #8 refers to sensitivity and indicates the ability of IoT surveillance to identify every case. There are three indicators for realizing sensitivity in IoT design: precision, threshold configuration, and calibration. Precision in the IoT-based surveillance system setting helps to obtain data precisely. Accurate threshold configuration of each required parameter also ensures that the data are precise. Calibration is used to maintain system accuracy; the calibration process is performed periodically.

9) ATTRIBUTE #9: POSITIVE PREDICTIVE VALUE: Attribute #9 refers to the positive predictive value, which is defined as the IoT surveillance system's ability to report data according to the case definition. The indicator of this attribute is data accuracy. Therefore, IoT-based system design should produce accurate infectious disease case data, which should be validated with other relevant data.

10) ATTRIBUTE #10: REPRESENTATIVENESS: Attribute #10 refers to representativeness. In designing IoT-based surveillance system, representativeness refers to the system's ability to present data which depict the number of cases in the population under surveillance. This is achieved through two indicators: data synchronization and data traceability. Both of these are essential for ensuring data correctness and portraying the data's originality consistent with the source [25][26].

11) ATTRIBUTE #11: SECURITY: Attribute #11 refers to security. This attribute plays an important role in maintaining public trust in the surveillance process using the IoT. It is supported by two indicators: infrastructure and management security and data security and privacy. Infrastructure and management security is a series of processes to secure the system end to end, from sensors to applications. It involves various types of action and policy to secure the infrastructure and to ensure that the security arrangement works properly and efficiently. Security and data privacy is an effort to preserve data at rest, in motion, and in use, which involves process and transmission media.

12) ATTRIBUTE #12: STANDARDS: Attribute #12 refers to standards, which consist of three indicators: standardization, regulation, and certification. Standardization is a global reference for building an integrated IoT-based surveillance system, while regulation refers to national or regional standards, and the rules derived from global standards. It is used to regulate IoT implementation design in each country or region. Subsequently, certification is applied to guarantee the system's operation and its security and safety. This should be done before mass implementation.

13) ATTRIBUTE #13: MOBILITY: Attribute #13 refers to mobility. This attribute is related to three indicators: tracking system, portability, and handover and roaming. A tracking system in IoT-based surveillance is applied to track the infectious disease suspects, and also to prevent and find any close contact in community interactions. Portability of devices effectively supports the functionality of IoT-based systems, which operate at rest and in motion. Handover and roaming support IoT mobile devices to operate in the moving system.

14) ATTRIBUTE #14: SUSTAINABILITY: Attribute #14 refers to sustainability, which has three indicators: maintenance, inspection, and evaluation and audit. Sustainable IoT design for surveillance system is needed, since they are planned to be implemented over a relatively long period. The IoT system requires maintenance to optimize its performance during its lifetime, and also requires inspection to avoid malfunctions and maintain its operational quality. Each change or improvement to the IoT system should be documented in a reporting system. The report can then be used as a supporting document for evaluation and audit in order to accomplish management requirements [27][28].

V. PROOF OF CONCEPT

In this section, we test our proposed reference model by designing an IoT-based community Covid-19 surveillance system. We illustrate the IoT infrastructure design supporting a Covid-19 active digital surveillance system. We then analyze the compliance of the system design by utilizing the 14 proposed reference model.

A. IoT Infrastructure Design for Community-based Covid-19 Surveillance

Covid-19 is an infectious disease spreading all over the world which has attained pandemic status [29] and has a high rate of spread and transmission. According to data published by WHO [30], the number of confirmed cases around the world had reached 57,882,183 including 1,377,395 deaths, as of November 22, 2020.

This study tested the proposed reference model by designing a community-based surveillance (CBS) system for Covid-19 employing the IoT. The community was represented by a nursing home for elderly people with a high risk of contracting the disease, as they tend to socialize with others in the home, which is contrary to the efforts to prevent Covid-19, namely minimizing gatherings and maintaining a distance. Eradication of the virus in such a setting will increasingly become a challenge considering that Covid-19 spreads through droplets, and as some elderly people have poor hearing and tend to interact at close range. We designed the infrastructure for the Covid-19 surveillance in the nursing home as depicted in Fig. 5. The end-to-end IoT infrastructure design consisted of wearable IoT medical devices, communication media, an integrated processing system, and user end devices. Hereafter, wearable IoT medical devices are referred to as IoT end devices.

In designing the Covid-19 surveillance in the nursing home, IoT end devices are employed to detect initial symptoms and prevent closed contact. The devices were built from an ESP32 development board equipped with a wireless system to manage the connection. Each board was configured with a unique identification code indicating the identity of the device. The code was then synchronized with a unique identifier for those using the device and being monitored. Therefore, medical staff could conduct the individual monitoring of the registered users under surveillance via the attached IoT end device. Initial Covid-19 symptoms were detected from body temperature through a DS18B20 sensor and breathing patterns through a heart rate and oxygen saturation sensor, namely MAX30102. In addition, close contact prevention was performed using a real-time location sensor, DWM1000.

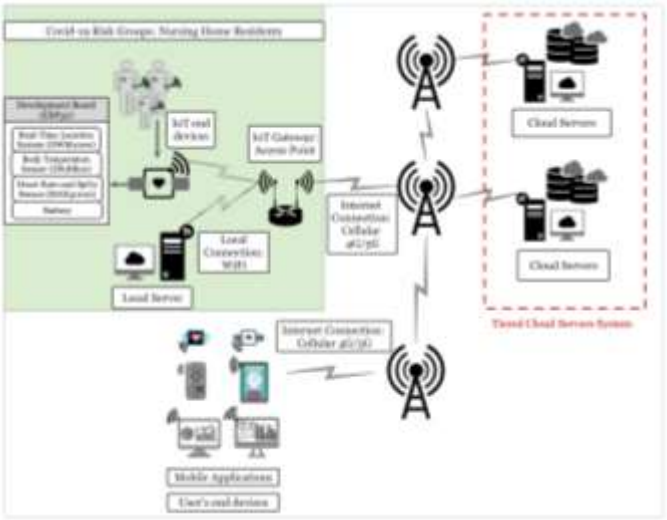

Fig. 5. IoT Infrastructure Design as a Covid-19 Active Digital Surveillance System.

Data collected from the sensor were encrypted and transmitted through Wi-Fi using the ESP32 module to the access point. In the design, the access point acts as an IoT gateway connected to the local and internet systems. Local systems were represented by IoT end devices worn by the elderly and a local server managed by surveillance staff in the nursing home. The local server was supported by cloudlet technology and served as a distributed data recording and processing system in the local community. The local server was connected to the cloud server with a tiered level. It means that the local server had a connection to cloud servers in the nearest cloud server, such as in community health centers or referral hospital, and then to cloud servers at a regional or national level. The local server's database was then synchronized with other databases on a larger scale in a cloud server, supported by cloud computing technology. The WHO cloud servers acting as the global data centers are used to aggregate the Covid-19 related data from each country.

Data from many sources were collected and integrated in the cloud servers for further processing. Complete, accurate, and up-to-date data from various sources enrich our knowledge of the incidence of Covid-19 from temporal, spatial, and populational aspects. The data can also be used to determine trends and to predict the distribution of Covid-19 cases at the regional level or aggregated at the national level.

The users' end devices, as shown in Fig. 5, included a mobile phone, gadget, laptop, or computer belonging to the community members or their guardians, stakeholders, or public. For guardians and medical staff, the user's end device had an additional function, allowing it to be used as a

medium for receiving alerts when Covid-19 symptoms or close contact interaction were detected in the elderly or community members. The device's general function was as a means to access and report the Covid-19 data according to the user's role. Public participation in reporting cases via the online system significantly and concurrently increases the completeness of the surveillance data [2].

In term of security, a lightweight security program was configured to secure the IoT end device entity and encrypt the data. The design of lightweight IoT security was based on the work of the authors of the reference [31]. IoT end devices must not be duplicated and must be secure from any types of attack. In addition to securing the devices, firmware and local storage were configured so that they could only be accessed and modified by the authorized parties. End-to-end encryption was designed to be configured in the transmission media. Wireless security standard was applied to secure data during transmission. The security applications were applied on local and remote servers of the processing system's infrastructure to secure the Covid-19 related data. Appropriate security implementation was needed in both the hardware and software to strengthen the security system. The security design should also include regulations to manage access to the data processing system securely by setting up access control and strict authentication. Additionally, update and patch mechanisms should be scheduled regularly. The mechanism is applied following the software security requirements to avoid system vulnerability [32]. As part of solution in preserving data security and privacy in the users' side, they were requested to regularly update their mobile application password installed on the end device. In terms of data access and reporting, privacy protection must be applied to protect the distribution and utilization of data [33].

In this designed scenario, the surveillance operation was performed in a tiered system with various supporting technologies. Hence, we designed the IoT operation in a real-time and scheduled system. The real-time system operation was applied to detect the Covid-19 symptoms and prevent closed contact. It was applied between the IoT end device to the nearest cloud server in a community health center, or referral hospital with more medical specialists and adequate facilities. In contrast, the scheduled system was applied to report and synchronize Covid-19-related data between cloud servers at a regional or national level.

As tools for active digital Covid-19 surveillance, IoT-based systems require public participation. Therefore, user-side systems should be designed with a user-friendly approach to attract the public. Such systems contribute to determining the interest of the public and organizations in collecting surveillance data [34]. User-friendly systems that are straightforward and intuitive are essential for the community, especially those who are not familiar with technology applications [35]. Fig. 5 shows the user-side systems representing front-end systems consisting of IoT end devices worn by the elderly or other community members and the users' end devices. IoT end devices require a user-friendly interface in order to be used by community members with varying levels of technological understanding. The user end-device applications also require a user-friendly interface to facilitate access and reporting of Covid-19-related data or to receive alerts and proactive notifications in the case of anomalies [36]. Furthermore, the user side representing the backend system is part of the IoT-based surveillance, apart from the frontend. This is operated by the surveillance staff, epidemiologists, or stakeholders. A user-friendly interface system in the backend system is also required to assist the surveillance staff in operating and efficiently managing the surveillance systems.

B. Analysis of Design Compliance with the Proposed Reference Model

The Covid-19 surveillance system implemented in the nursing home started with data collection from a screening process targeted at the elderly with signs or symptoms of the disease and all suspected cases. Fig. 6 illustrates the initial Covid-19 surveillance and screening process in the community. As shown in the figure, the elderly as community members are considered as mobile users. The nursing home health facilities located in each community are illustrated as local systems. The remote system represents the systems installed outside the nursing homes, which is a centralized aggregation system supported by cloud computing technology for the Covid-19 management center.

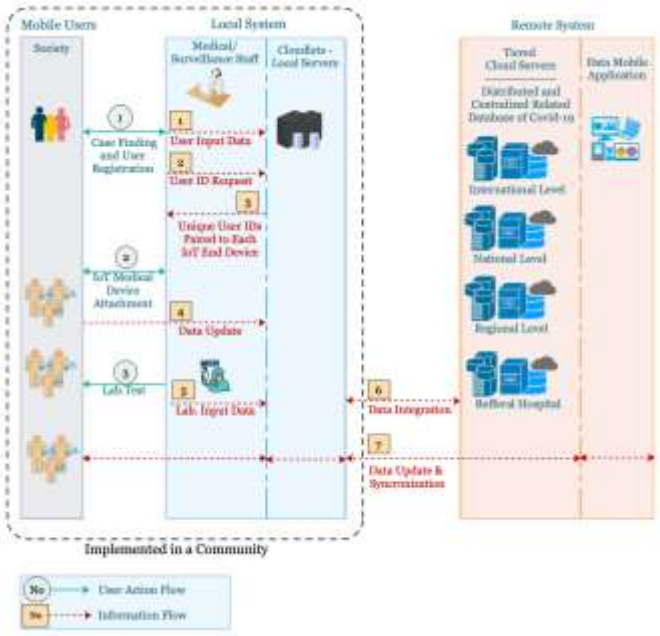

Fig. 6. Design of the Screening Mechanism and Initialization of the Covid-19 Surveillance Process.

Three steps were involved in implementing the Covid-19 surveillance system with the IoT. The first step was to find a case at the community level by examining the members. Initial laboratory tests were performed in this step to maximize the prevention spread of asymptomatic Covid-19. The surveillance staff recorded each community member on a registration form and input their medical data records into the Covid-19 database in the local system. The second step was to attach a wearable IoT medical device (IoT end device) to each community

member, which continuously monitored three parameters: users' body temperatures, and whether they had reached 38°C; respiratory rates; and real-time user location. The first two parameters were used to check the users' possibility of respiratory tract infection symptoms and to monitor the condition of those who had already had congenital SARI disease. The last parameter was used to prevent close contact interaction. The last step was Covid-19 laboratory testing. For community-based surveillance, it is better to utilize point-of-care laboratory test devices that are portable, support mobility and are connected to a data center via an internet network. Example portable laboratory devices are GeNose [37] [38] or in the case of this research point-of-care RT-PCR devices [8]. For the design, as an IoT point of care device, RT-PCR was designed to support mobility and to be connected to a data center via an internet network.

The IoT end devices were attached until the quarantine or treatment period was over. Following WHO procedures, IoT end devices were taken off suspect users whose results from two RT-PCR tests on two consecutive days with an interval of> 24 hours were negative. The devices were unattached from close contact users who had completed a 14-day quarantine period. However, for suspect and probable users whose RT-PCR test results were confirmed positive, the monitoring and examination process was conducted continuously according to the Covid-19 handling procedures, until the patient recovered.

After data collection, the surveillance process continued with data transmission, analysis and interpretation. In the community-based Covid-19 surveillance utilizing the IoT, data gathered from the IoT end devices were recorded on the local server and then updated and synchronized with the remote system on a broader scope to be integrated with other databases for analysis and interpretation. This was so that the IoT-based Covid-19 data were complete, detailed, valid, and continuously updated data. The data processing system implemented at either cloudlet or cloud computing level was equipped with intelligent systems to support the data analysis and interpretation. This intelligent IoT system played an essential role in accelerating and aggregating the data computation process in both the cloudlets and cloud computing. The last surveillance process was data dissemination and application. In this design, the process was propagated via lightweight mobile applications towards the users' end device.

Following the illustrations in Fig. 5 and 6, we now analyze how the IoT design for an active digital community Covid-19 surveillance system complies with the 14 attributes proposed in the reference model (Table I).

1) DESIGN COMPLIANCE WITH ATTRIBUTE #1 (USEFULNESS): Attribute #1 has two indicators, applicability and customizability. The applicability of IoT in Covid-19 surveillance relates to rapid case detection and close contact prevention. The community-based application is part of national and global surveillance systems to find large numbers of cases and prevent contact quickly. As shown in Fig. 6, the applicability of IoT-based surveillance in detecting cases follows three steps: user data collection, medical screening, and monitoring of users' condition through the IoT end devices. These actively check users' temperature and breathing patterns in the form of initial symptom data. The device is attached for approximately 14 days as long as there is no interaction with Covid-19 patients, or for more than 14 days as a result of growth in local transmission cases in each region.

The customizability of IoT-based system in Covid-19 surveillance is needed to adjust the design to different surveillance scenarios. Following WHO guidelines, each region or community could have a different surveillance scenario according to the Covid-19 transmission level. For example, in a nursing home located in an area with community transmission, the surveillance is applied to all community members, with standard sensors in their IoT end devices. On the other hand, in hospital-based surveillance the IoT end device design can be customized to have more functions in a complex system. Aside from detecting early symptoms, use of the IoT for Covid-19 can be in the form of a multi-purpose system, such as an integrated application for tracking suspect cases and detecting clusters, or a system for online reporting and trend monitoring. The IoT system can also provide additional health services, such as preparing up-to-date patient and family medical data. This helps medical personnel with predictions, diagnoses, treatments, and decisions related to infectious disease cases [39].

2) DESIGN COMPLIANCE WITH ATTRIBUTE #2 (DATA QUALITY): Attribute #2 has two indicators, data completeness and data validity. Data completeness for Covid-19 surveillance is obtained by integrating primary and secondary IoT data. Primary data are collected from the initial screening process, online reporting and the IoT end devices used by the elderly in nursing homes, or by subjects of community-based surveillance during the observation period. The primary data encompass personal data, telephone numbers, residence address during the last 14 days, travel history, date of the appearance of symptoms related to Covid-19, and associated conditions. The data are recorded on the local server or cloudlet, and labeled with a unique identifier to represent each user's identity. This identifier also acts as a synchronization code to identify its IoT end device pair. The auto-updated system also supports data completeness in the IoT-based surveillance. On the other hand, secondary surveillance data are obtained from the database. These are used for complementing the dynamic analysis and validating the primary data. Examples of secondary data are related to population and GIS; hospital databases; laboratory, pharmaceutical and EHR data; and other related data.

Data validity of the IoT-based Covid-19 surveillance is checked from the screening process in nursing homes and other communities. All personal data registered on the system is validated using an identity card or passport. Symptom data from the initial medical examination are validated by integrating them with each patient's EHR data. This integration is continued by incorporating data collected from the IoT end devices and advanced laboratory RT-PCR tests. Additional

symptom data beyond the basic examination and IoT end device capability can be added or reported via a mobile application system. Medical personnel need to validate all the additional reported data.

The Covid-19 data quality generated by the IoT-based surveillance systems should be more complete and valid since the data are integrated thoroughly. Data integration enriches the Covid-19 analysis related to patients' comorbidities and their advanced symptoms. Such integrated data also helps professionals provide much more appropriate treatment and follow up on emergency health events more accurately [2].

3) DESIGN COMPLIANCE WITH ATTRIBUTE #3 (TIMELINESS): Attribute #3 has two indicators, rapidity and timeliness. The rapidity of IoT-based Covid-19 surveillance in a community is needed to address the increasing spread of the disease. The pandemic has put the global health situation at very high risk; a significant number of Covid-19 positive cases leads to many casualties and the exhaustion of medical personnel. The design of rapidity in IoT-based Covid-19 surveillance in each community is achieved by the implementation of a partial real-time system. The system that connects the IoT end device to the nearest cloud server or Covid-19 management center is set to operate on a real-time basis. It is designed to assist medical personnel in detecting and monitoring Covid-19 suspects and their probable condition directly. Real-time surveillance design also influences Covid-19 patients' rapidity in receiving medical treatment or other follow up care according to public health management procedures.

The timeliness of IoT-based Covid-19 surveillance is achieved by combining real-time and scheduled system design. A real-time system is operated for Covid-19 case management in each community, while a scheduled system is operated to provide aggregated case data reporting. According to WHO provisions, all suspected, probable, and confirmed Covid-19 cases must be reported to the health office and the Public Health Emergency Operation Center. Immediate reporting should be made within 24 hours of the epidemiological investigations, and the timeliness of the IoT system can be designed to satisfy these provisions. Therefore, the IoT system accelerates the process of reporting data, which is useful for advanced Covid-19 analysis and cluster identification [13]. The IoT also speeds up the updating of infectious disease-related data to stakeholders and the public for surveillance dissemination [23]. Overall, the end-to-end IoT integration system is key to the rapidity and timeliness of IoT-based Covid-19 surveillance held in each community. However, the rapidity and timeliness of IoT integration are influenced by data processing and transmission speed, and IoT end device response time.

4) DESIGN COMPLIANCE WITH ATTRIBUTE #4 (FLEXIBILITY): Attribute #4 has two indicators, adaptability and scalability and extensibility. The adaptability of IoT-based Covid-19 surveillance is required since each community has different scenarios and technology support. Since Covid-19 transmission has reached the global community in many countries, adaptability design should comply with many different conditions; those which may differentiate the design include the unequal distribution of IoT infrastructure, differences in geographic area, and the population density in each community. The adaptability of IoT ensures that the surveillance process can work properly under various conditions. In designing the system, the IoT network from the end device to the gateway should be adapted to the local infrastructure, while maintaining the quality of network services. The local server's processing resources should consider the computational load. Specification of the processing device implemented in a region with community transmission scenarios will differ from sporadic case scenarios. The adaptability of IoT design also includes flexibility in the selection of technology for mass community implementation. However, the selected technology must comply with the specified standards, pass medical device test standards, and be certified.

The scalability and extensibility design of IoT-based Covid-19 surveillance is correlated with the expansion of the system implementation. It is required when communities or regions change their Covid-19 surveillance due to growth in case numbers. The scalability and extensibility of IoT design includes both physical and logical systems. A scenario change in the community can be scalable by upgrading the device and adjusting its specifications so that it can be applied to the new scenario. It also can be extensible by optimizing the functionality, performance and efficiency of the existing system. Optimization of the existing network can be made by increasing bandwidth capacity and giving priority to the QoS of the existing network. Additionally, optimization of the IoT mobile application can also be made by supplementing its features to support hospital management. This could reduce medical personnel's workload in the current Covid-19 pandemic situation. With specific regard to patient management, IoT saves patients' time with the readmission feature for those who have been confirmed Covid-19 positive, thereby reducing the density of service centers and speeding up the patient handling process [13].

5) DESIGN COMPLIANCE WITH ATTRIBUTE #5 (SIMPLICITY): Attribute #5 has two indicators, manageability and automatic system. The manageability of IoT-based Covid-19 surveillance applied in communities is paramount. This is because surveillance involves many resources and users and consists of many tiers. The ease of manageability of IoT simplifies the varying Covid-19 surveillance activities. In community-based surveillance, as illustrated in Fig. 5, it can be seen that the number of IoT end devices is directly proportional to the number of users under surveillance. The devices can be easily managed because each of them has a device identity, namely, a unique identification code configured on the ESP32 development board. In addition, the IoT infrastructure that supports the surveillance can be managed by using

hardware, software, or system management tools. These are configured to send an alert and notification when part of the system fails, or when anomalous activities occur. Overall, IoT design manageability should be compatible with heterogenous IoT protocols and platforms in its integrated system [40].

The automatic system of the IoT applied in each community simplifies operation and minimizes the manual process of Covid-19 surveillance. The IoT end device for detecting symptoms and preventing close contact is designed to be worn by all community members, including those with disabilities. Therefore, it is ideally set to minimize user intervention. The device's sensors operate automatically in detecting Covid-19 symptoms and the devices can also be configured to automatically send an alert. In the design shown in Fig. 5, an automatic alert is sent out when a user is detected as having a temperature of ≥38°C, a high respiratory rate or unstable breathing pattern. Simultaneously, an automatic alert is also sent when a community member is detected to have interacted with Covid-19 patients within a radius of 1 meter for >15 minutes [41]. In larger community-based surveillance, the IoT end device can be equipped with GPS technology to accommodate an automatic system for tracing contacts over a wide area. The device is configured to monitor users' history of locations visited based on GPS coordinates, from two days before the onset of the disease up to 14 days afterwards [41]. All IoT end device alerts are sent to community members' guardians and medical personnel at the local level. Furthermore, the automatic system of IoT-based Covid-19 surveillance can be seen in its data updating and synchronization, which impacts on the rapidity of Covid-19 data dissemination to stakeholders. We can thus state that an automatic system of IoT integration greatly helps Covid-19 surveillance in high-risk communities with fewer medical staff.

6) DESIGN COMPLIANCE WITH ATTRIBUTE #6 (ACCEPTABILITY): Attribute #6 has three indicators, interoperability, compatibility, and user friendly. An interoperable system is required since IoT-based Covid-19 surveillance is constructed from different protocols, devices, and communication media. The various technologies comprising the IoT system should operate seamlessly. IoT system interoperability can minimize the technical constraints that might appear with global implementation. It also can minimize the problem of differences in technological backgrounds between developed and developing countries which adopt IoT-based surveillance to fight Covid-19. Consequently, communities with different settings and technological backgrounds can synergize the end-to-end process of Covid-19 surveillance.

Compatibility of devices, platforms, and services is required to build an integrated IoT-based surveillance system. Hardware and software must be compatible with the main technology infrastructure in each community or region. Hence each community can implement the IoT-based Covid-19 surveillance system efficiently. The compatibility of mobile applications with various device platforms and network conditions is also required to facilitate user access. Another type of compatibility related to IoT-based surveillance is that of data format. The system implemented in each community should generate a standardized data format that can be interchangeable purely for Covid-19 surveillance purposes.

A user friendly system is necessary to facilitate the end-to-end operation of IoT-based Covid-19 surveillance. As illustrated in Fig. 5, the IoT infrastructure system for such community-based surveillance design is divided into backend and frontend systems. User friendly design dashboards assist stakeholders in managing the IoT infrastructure and all the systems, while user friendly application interfaces assist surveillance staff in managing surveillance-related data. In general, both designs help staff to simplify operations on the backend system. With regard to the frontend system, a user-friendly system encompasses hardware and software interfaces. An example of a hardware interface is the IoT end device worn by the elderly. The user friendly hardware design must consider user comfort across all age categories, including the elderly, and the supporting technology infrastructure. User friendly software should be designed to be an easy-to-use application for all communities with different technological understanding and language skills. Such user friendly software encompasses the design of the mobile application interface installed on user end devices. Community members or societies require a user friendly frontend application to quickly understand the agreement related to data privacy [42]. Moreover, those with special needs require a simpler application interface for accessing and reporting Covid-19 data; for example, by simply pressing a specific button on their mobile application. We therefore hope that information technology can play a significant role in involving the community in improving health surveillance [14].

7) DESIGN COMPLIANCE WITH ATTRIBUTE #7 (STABILITY): The attribute #7 indicators are accessibility, availability and reliability. Accessibility design refers to convenient access to a globally integrated IoT-based Covid-19 surveillance information system. IoT-based surveillance is designed to provide easy access to the integrated system and its data from various technological platforms. Access can be made anytime, anywhere, and by anyone, according to the users' role. Accessibility design for medical professionals is used to access and monitor those suspected of having Covid-19 and patients' updated condition in real-time. Accessibility design for community members and the public is used to access and report Covid-19 related information to the official and trusted system.

The availability and reliability of IoT design for Covid-19 surveillance are correlated with the service delivery of the system in each community. They are influenced by the approved Service Level Agreement (SLA), which determines its uptime and downtime. Internet Service Providers (ISPs) and application service providers are the parties involved in determining SLAs to support the overall IoT infrastructure. If the community-based surveillance system commits to providing integrated services with an SLA value of 99.999%, this means that the IoT infrastructure built to support the surveillance system should be ready to operate 24 hours a day

and 7 days a week, with a downtime of 5.26 minutes per year. To monitor the system's availability and reliability, we can apply an internet-based management system application. This will generate and send a notification to the administration when the system is inaccessible so that the problem can be followed up immediately.

Regarding technical detail, the design of IoT infrastructure availability and reliability can be realized by implementing redundancy topology and configuring high availability in crucial devices. Redundancy applies to infrastructure lines and devices so that there is no single point of failure. The high availability configured in the crucial devices indicates the system's capability to perform a failover function. Next, the Quality of Services (QoS) feature can be applied to the IoT infrastructure [43] to guarantee excellent service, namely, one that can be accessed concurrently and is seamlessly connected to the system. Simultaneously, the availability of surveillance data can be maintained by preparing a data recovery and backup system. The IoT-based surveillance system should be supported by appropriate storage capacity. Furthermore, higher IoT stability design can be achieved by considering a resilient system, which refers to the IoT's ability to defend against various types of interference, restabilize changing conditions, and adapt its behavior and structure to constant changes [44][45].

8) DESIGN COMPLIANCE WITH ATTRIBUTE #8 (SENSITIVITY): Attribute #8 has three indicators: precision, threshold configuration, and calibration. The precision of the ongoing IoT-based Covid-19 surveillance system is primarily determined by the measurement sensitivity of the IoT end device sensors. In general, the sensors' precision affects the handling procedure of Covid-19, since the sensor detection results contribute to determining individual cases. This precision greatly impacts the measurement accuracy of users' body temperature, respiratory rate patterns, and the distance between interacting users. The DS18B20 sensor should precisely check users' body temperature; if this reaches 38°C, it is the first sign that an initial Covid-19 symptom has been detected. The second sign is the user's breathing pattern detected by the MAX30102 sensor, whose detection precision is used to check whether the breathing pattern is irregular. In addition, to prevent close interaction, the DWM1000 sensor is configured to monitor each user's position in real-time. All the sensor measurements then become a reference for detecting initial Covid-19 symptoms and preventing close contacts and also for activating alerts sent to community members' guardians and medical staff. In contrast, any imprecision of IoT end devices will worsen the Covid-19 control measures.

Threshold configuration is applied to the IoT end device sensor. The device is designed to send out an alert when the user's body temperature is ≥38°C, and their respiratory rate patterns change. This threshold configuration is applied following interim WHO guidance for determining initial Covid-19 symptoms. A real-time position sensor is configured to ensure a safe distance is maintained between users when they interact. The threshold configuration is set to a 1-meter distance, with less than 1 meter assumed to be physical contact, and it is combined with a device timing system with a threshold of 15 minutes. An alert is sent out when the sensor detects an interaction between users and Covid-19 patients within a radius of 1 meter or less for > 15 minutes [41]. The precision of setting the threshold determines the accuracy of the alerts. An incorrect threshold setting will lead to inaccurate and late alerts and alarms sent to users and medical personnel. This situation also means that case detection will become less accurate, resulting in medical treatment delays and endangering patients. Therefore, precision and thresholds must be set appropriately and accurately.

The calibration process of the IoT end devices is performed before the devices are distributed. After a certain period, device re-calibration is needed to maintain measurement precision. Device calibration keeps the IoT system's operational capabilities standardized, thus minimizing the tendency to generate anomalous data. Therefore, the calibration process is performed to ensure that IoT devices can be employed anywhere and will produce the same data quality.

9) DESIGN COMPLIANCE WITH ATTRIBUTE #9 (POSITIVE PREDICTIVE VALUE): The attribute #9 indicator is accuracy. The accuracy of reporting Covid-19 data following the WHO case definition guidelines is essential for presenting factual data. The latest version of the WHO interim guidance currently gives three terms to define Covid-19 cases: suspect, probable, and confirmed. These three case definitions are used as the standard for ongoing Covid-19 surveillance. Therefore, IoT-based Covid-19 surveillance needs to translate each case definition of the clinical symptom criteria proposed by WHO into the IoT system's technical functionality. WHO also differentiates the details of Covid-19 symptom criteria for children and adults into mild, moderate, and severe illnesses, including asymptomatic patients. To achieve the accuracy of the system for finding case data in the field, IoT end devices and their supporting systems must be designed and configured strictly, following the WHO clinical criteria provisions. The IoT system's accuracy should ensure that all reported Covid-19 case data meet with the case definition accurately.

The accuracy design of IoT-based surveillance is illustrated in Fig. 6. There are three steps to finding Covid-19 suspects in community-based surveillance, such as in a nursing home. These are initial laboratory tests, monitoring of each community by IoT end devices, and advanced laboratory tests. After passing the screening process, namely the initial laboratory test, the ongoing surveillance is performed with the assistance of the IoT end devices. Initial Covid-19 symptoms are detected according to data parameters gathered from the attached IoT end device. To confirm the symptoms, advanced laboratory tests, such as RT-PCR, are conducted on each suspect and probable Covid-19 case. In this way, medical staff will have accurate data regarding the case, positive or negative. For further examination, the RT-PCR test results that confirm

positive cases are aggregated with EHR data to complement the comorbid analysis and other required medical data to achieve more accurate Covid-19 analysis. Consequently, epidemiologists will have more in-depth and comprehensive analysis data related to Covid-19 occurrence, trends, predictions, and other health-related data.

10) DESIGN COMPLIANCE WITH ATTRIBUTE #10 (REPRESENTATIVENESS): Attribute #10 has two indicators, data synchronization and data traceability. Data synchronization in community-based Covid-19 surveillance, as illustrated in Fig. 6, occurs between IoT end devices and the local and remote servers. IoT-based surveillance can provide representative data by employing individual devices to monitor the condition of each community member under surveillance. Through direct user involvement, the data collection process can represent the actual number of suspects, probable, and confirmed positive cases of Covid-19. Employing IoT end devices as part of an active digital surveillance system provides the advantage of real field data. Each user's data are securely synchronized with the attached IoT end device, employing the user's identity code for individual monitoring. The IoT end device data are complemented through the reporting mechanism via the users' mobile applications. Automatic data synchronization is then applied to individual medical data and the real field data collected from the IoT end devices and reporting applications. These data are then integrated with the Geographical Information System (GIS) data and population distribution data. Eventually, IoT-based surveillance is expected to help epidemiologists to obtain more representative Covid-19 data which portrays the number of cases with the updated and accurate demographic data in some geographic regions under surveillance.

The data traceability of the IoT-based Covid-19 surveillance system is used to maintain data consistency. An integrated surveillance system from an end-to-end IoT infrastructure makes it easier to realize this traceability. According to the data activity logs, data cloud computing in the remote system can be traced to its source. The tiered system design of the IoT infrastructure supports data tracing down to its original source. Any data entering the IoT information system must be traceable transparently, because it is difficult to use inconsistent data to represent the number of cases in a particular population. An alternative solution to accommodating data traceability is the data standardization format and data security application. The standardization of data reporting formats simplifies data tracing in the IoT system. The security application can be applied to check the data manipulation. Data changes can be easily traced when data integrity checking is applied. Additionally, the non-repudiation feature of security could also be used to trace data sources.

11) DESIGN COMPLIANCE WITH ATTRIBUTE #11 (SECURITY): Attribute #11 has two indicators: infrastructure and management security and data security and privacy. The infrastructure and management security design of IoT-based Covid-19 surveillance is divided based on a layering approach. The selection of security technology and methodology applied to the Covid-19 surveillance system should be suitable for each IoT layer. The IoT infrastructure and management security' layers include the security applied in IoT end devices, transmission media, data processing systems, and applications. In the IoT end devices, security involves various techniques that ensure the devices are authenticated and the data are encrypted to global standards. A lightweight security application is more suitable for application in IoT end devices. In the transmission media, security should cover certain mechanisms to maintain infrastructure resilience against various attacks, vulnerabilities, and threats that commonly occur on the networks, both accidental and incidental. In the data processing systems, security generally applies layered designs, ranging from physical location security to computing process applications. In IoT applications, security covers possible mechanisms to ensure that application services are secure from any threats of identity theft or of other important data while continuing to deliver valid information to the appropriate users. Users are requested to change the application system passwords regularly, and a notification will be sent to remind them. If the application is updated, then the users will also be reminded to install the updated version so that application vulnerabilities can be minimized. The overall security applied to the end-to-end IoT system for the Covid-19 surveillance design should be managed in a decentralized model, yet also be connected to a central security management system. Additionally, the implementation of security management technologies such as Syslog and SNMP is required to prepare a forensic analysis if an attack occurs.

Data security and privacy are the main concern when involving technology in the medical sector, such as the IoT-based Covid-19 surveillance system. Most Covid-19 surveillance data consist of personal and medical data, which are classified as confidential. Therefore, the IoT system design should guarantee users' data security and privacy. These can be maintained by implementing the security parameter in the IoT system software, hardware, and services. According to security standards for maintaining data security and privacy, the IoT security system should fulfill four parameters: confidentiality, integrity, availability, and non-repudiation. The confidentiality parameter protects against data abuse and leakage. If the IoT system fails to maintain data confidentiality, it might have fatal consequences for society's trust in Covid-19 surveillance participation. Simultaneously, the integrity parameter ensures that data related to Covid-19, especially data from the IoT end devices; do not change from source to destination. If there is a change, this might lead to patient misdiagnosis due to invalid data, which could endanger their safety. Data availability is also a vital parameter in the Covid-19 pandemic. Unavailability of data could interfere with the situation, since controlling the

disease without data support would be a hard task. In addition, a non-repudiation parameter in the IoT design for Covid-19 surveillance is associated with the certainty of data collected from users' IoT end devices. Non-repudiation ensures that the IoT end devices truly monitor the users whom data synchronized to the surveillance system. The synchronized users' data is beneficial for individual case handling which they can by getting more specific treatment based on their accurate medical data.

12) DESIGN COMPLIANCE WITH ATTRIBUTE #12 (STANDARDS): Attribute #12 has three indicators: standardization, regulation, and certification. Standardization in IoT-based Covid-19 surveillance systems is necessary to maintain system implementation at ideal levels. The implementation of community-based Covid-19 surveillance has various scenarios and conditions which may vary across countries. Therefore, standardization can be used as a global reference in building IoT-based surveillance systems, with the aim to stabilize and measure system performance. Global standardization involves various technical aspects, including standards for the software, hardware, protocols, and technology services used to build the surveillance systems. In practice, standardization facilitates the integration process between devices, media, and services to provide globally formatted surveillance data. Standardization of the thresholds and operations of the IoT end devices helps medical personnel to find cases precisely. Parameter standardization of network and data processing maintains the quality of the surveillance process. Standard parameters allow the system to operate in real-time or to be set following the WHO schedule. The processing system should be standardized to generate data in a standard format set by WHO, and should have the additional ability to process data in a non-standard format. In addition, standardization of system security is also needed to assure users' confidential data and preserve public trust in participating in the active surveillance of Covid-19.

Regulation of the technical details for adopting an IoT-based Covid-19 surveillance system in each country and its district could be derived from global standards. National- scale regulations need to be developed as more specific technical guidelines for designing systems following each country's applicable regulations and conditions. Moreover, regulation could overcome language barriers to the use of specific applications by individual users in different countries. Regulations are applied to the entire IoT system, starting from attached devices on the end-user side, transmission, the processing system, and data delivery. Regulations on medical devices ensure their safety, with the level of regulation required depending on the level of risk associated with the device [46]. Regulations regarding the security of both data and infrastructure also need to be devised so that the system can guarantee users' trust to be actively involved in surveillance. Furthermore, the government also needs to develop a regulation to ensure that each party involved in supplying hardware, software, and applications follows standard guidelines. This kind of regulation is needed in mass field implementation. For example, a country may have a specific regulation related to the radio frequency used that differs from those of other countries. Hence, device specifications need to be adjusted to that radio frequency. Another example is that there are many technology brands and technical details of programming application in field implementation. Consequently, chips and sensors installed in the IoT end device in one region could be slightly different from those of other regions, as may be the applications.

Certification is a way of ensuring that the quality of system performance is maintained [47]. It is needed in every implementation of IoT-based Covid-19 surveillance to keep the system quality standardized. Certification in IoT implementation is required for both software [48] and hardware [49]. Especially in the case of hardware that interacts directly with users, it is necessary to ensure that it has passed technical and safety testing and certification before use. The certification system maintains the quality standard of the surveillance in each community facing different Covid-19 transmission scenarios.

13) DESIGN COMPLIANCE WITH ATTRIBUTE #13 (MOBILITY): Attribute #13 has three indicators: tracking system, portability, handover and roaming. In IoT-based surveillance, these are applied to support the mobile design of active digital surveillance for Covid-19. In community-based surveillance, such as nursing homes, the tracking system is designed to prevent close contact interaction. A real-time position sensor, DWM1000, is applied to track community members' movements at a close distance. In the previous section, we stated that the IoT end device is configured to send an alert when close interaction occurs, thus helping to prevent the spread of Covid-19 in a community building. This real-time position sensor is part of a tracking system for indoor environments or buildings, in which short distances can be detected. However, for tracking in an outdoor and a large-scale environment, an additional sensor such as a GPS sensor is needed. It should be noted that GPS has limitations in detecting very short distances accurately; therefore, we chose a DWM1000 sensor that can detect short distances much more accurately, which is appropriate for a design employed in a nursing home. A GPS sensor is an example of a tracking system used in large-scale Covid-19 surveillance systems to monitor participants' movements during the process. Participants or users can continue performing their activities following health protocols while being continuously monitored by the system.

In IoT-based Covid-19 surveillance, besides preventing close contact, the tracking system also facilitates tracking contacts. Contact tracing using technology has been supported by WHO, which has issued guideline on such use of digital devices [50]. Contact tracing is conducted continuously, considering that Covid-19 transmission is high-risk, taking place person to person through contact and droplets. Transmission could occur to residents who interact with

probable or confirmed positive Covid-19 cases. The higher the number of interactions is, violating health protocols, the greater the need for tracing contacts. Therefore, manual contact tracing is not recommended, since it requires intensive resources and the risk of medical personnel becoming infected when performing their duties. For this reason, the IoT serves mobility design to ease medical personnel's burden through digital contact tracing with less effort, especially in community transmission areas. According to WHO provisions, contact tracing in different location settings has different criteria. The most general criteria are having a history of face-to-face interaction contact with Covid-19 patients at a minimum distance of 1 meter for more than 15 minutes, or direct physical contact with Covid-19 patients. Both criteria are valid for tracing contacts in community location settings, closed places, healthcare facilities, public transportation, and community gathering locations. Other detailed criteria are adjusted to the location setting. The contact tracing period for Covid-19 exposure determination in the community starts from 2 days before the development of symptoms, up to 14 days after such development (symptomatic cases), or 2 days before and 14 days after the date of a confirmed laboratory check (asymptomatic cases) [41].

The tracking system design in the IoT for Covid-19 surveillance helps digital contact tracing through a combination of the real-time position sensor and GPS sensors installed in the IoT end devices. The real-time position sensor DWM1000 acts as a proximity sensor that detects the interaction distance between individuals and Covid-19 patients. Simultaneously, the GPS sensor generates position coordinates to determine each suspect's travel history in the contact tracing period. Data from the proximity and GPS sensors are combined to simplify the finding of close contacts and to increase the awareness of those who have visited the same location as Covid-19 patients and have interacted with them. This data combination is also useful in a large-scale and real-time tracking system of Covid-19 patients. In areas which apply the zonation system, the combination of proximity data and users' actual locations could be used to notify the, when they are entering Covid-19 danger zones.

The portability of IoT-based Covid-19 surveillance design is applied in the form of IoT end devices worn by community members and point-of-care (POC) devices used for laboratory testing. These portable devices assist the mobility of IoT-based surveillance and accommodate users' and medical personnel's mobilization during Covid-19 surveillance. Therefore, user monitoring can be conducted continuously, and laboratory testing can be conducted flexibly, either in a fixed or mobile situation. In the nursing home, as illustrated in Fig. 5, IoT end device portability is designed to be worn on community members' wrists. On the other hand, point-of-care device portability is exemplified by the utilization of the point-of-care RT-PCR device [8] or GeNose [37][38]. Point-of-care diagnostics tools utilize a Polymerase Chain Reaction (PCR) system equipped with a chip to connect to Bluetooth on a mobile phone and then to the internet [8]. Meanwhile, Genose is a portable Covid-19 detection tool that only takes around 2-3 minutes to test and obtain a result. GeNose is beneficial for medical personnel to detect massive cases of Covid-19 using a simple procedure without reagents or other chemicals. The test is conducted by taking a breath exhalation sample, which is more comfortable than a PCR or swab test [37][38]. Overall, the portable system can detect real-time samples and has a user friendly design which simplifies the detection process and supports medical personnel mobility.

Handover and roaming in community-based Covid-19 surveillance are needed to support user movement in areas covered by the IoT network infrastructure. IoT end device operation is supported by wireless networks, which have limitations in terms of coverage area. Hence, a soft handover configuration is applied in the local wireless system, consisting of several access points or other wireless technology. The local wireless system could be in a nursing home or community member's building, and it can be integrated into a regional or national wireless system. A soft handover configuration maintains the device's connection while moving in certain wireless network coverage area. In comparison, a roaming configuration is applied in an international wireless system. In global surveillance design, roaming configuration maintains a device's movement across countries' geographical boundaries, and generally occurs in border areas. Therefore, IoT end devices and point of care devices can connect to the IoT back-end system over the IoT network infrastructure, and surveillance can take place continuously at a local and global scale. Ultimately, this IoT design supports the generation of spatial-based surveillance data without the limitations of geographical boundaries.

14) DESIGN COMPLIANCE WITH ATTRIBUTE #14 (SUSTAINABILITY): Attribute #14 indicators are maintenance, inspection, evaluation and audit. Maintenance is used to ensure the sustainability of the IoT-based Covid - 19 surveillance system. Such a process has been enforced in many countries for more than a year, since the outbreak was first detected. Sustainable surveillance has been conducted to date, following the dramatic rise in confirmed cases and the incremental number of deaths due to COVID-19 exposure. This situation indicates that a maintenance system is needed to maintain IoT performance in Covid-19 surveillance. Maintenance systems can be implemented by applying appropriate preventive and corrective maintenance measures to the IoT infrastructure and service systems in each community and back-end system. An undeniable fact is that IoT design implementation utilizes numerous devices and many types of technology that might differ in each tier. Device and service failures are unavoidable in massive technology utilization. However, if the system is well organized and monitored, failure in one part would be easier to overcome if other parts remain operating optimally [51].

Inspection of IoT-based Covid-19 surveillance can minimize system malfunctions, especially IoT end devices that directly interact with users in the community. IoT end-device applications must have no impact on public safety. Inspection of devices is made to maintain the precision of devices in detecting initial symptoms and tracing contacts accurately. Inspection in network transmission is also necessary to ensure

that it is seamless, while inspection in the data computation system can ensure the processing is powerful and trivial mistakes are avoided. In general, inspection measures can speed up the process of replacing malfunctioning devices and upgrading resources beyond scheduled maintenance. Immediate inspection of anomalous systems prevents adverse impacts on IoT implementation.

Evaluation and audit should be implemented at the community scale and in larger-scale situations running IoT-based Covid-19 surveillance systems. Evaluation and audit are conducted to preserve the operational quality and stability of the IoT-based surveillance. Proper documentation in IoT-based surveillance system development complements the evaluation and audit process. Internal and external audits should be conducted to meet management needs [27][28]. Audit helps discover and minimize any impacts and risks arising from technological and non-technological aspects. During system maintenance and inspection, changes should be administratively reported, including the replacement of malfunctioning devices, resource upgrading, software updating, and patching to fix built system gaps. Data from regular and incidental reporting can be used as a guideline for improving the surveillance system performance. Data parameters for each device configuration and service must be correctly set and evaluated to avoid instability in the surveillance system. Every action to maintain stability and improve the IoT-based surveillance system quality is recorded in the online reporting management system.

VI. Conclusion

This paper has proposed a reference model for designing an IoT-based active digital surveillance system of infectious diseases. The proposed reference model consists of 14 attributes with respective indicators. The attributes were developed by utilizing the basic 10 parameters from CDC, adapting two attributes of security and standards from the other studies, and adding the new attributes of mobility and sustainability. Each of the parameters has specific indicators which need to be considered to complement design requirements when adopting IoT technology as an infectious disease surveillance tool.

In the reference model, we highlight the mobility attribute, which plays a special role in infectious disease surveillance; namely, to control disease spread. The attribute helps medical personnel to prevent close contact, conduct large-scale contact tracing and to monitor suspects and patients on a real-time basis. The mobility attribute also facilitates the community to remain active in line with health protocols while participating in the surveillance process. Hence, we hope that the attribute can indirectly increase the community's active participation in surveillance. Another attribute that we added was sustainability. This was included as an IoT-based surveillance system is designed to be implemented over a relatively long time, and its infrastructure can be reused for different surveillance requirements. The sustainability of IoT-based surveillance is realized by implementing maintenance, inspection, evaluation, and audit of the system.

Testing of the concept was performed by adopting the proposed reference model in an IoT-based active digital surveillance system for the Covid-19 disease. We elaborated the compliance of such end-to-end design in line with the 14 attributes of our proposed reference model. The compliance was analyzed on the basis of the specific indicators of each of the 14 attributes, reflecting how the IoT design should meet the criteria of our proposed reference model. As future work, a testbed should be conducted to examine further the field implementation of the framework and its design.

Acknowledgment

This research is supported by Kementerian Riset Dan Teknologi/Badan Riset Dan Inovasi Nasional – Republik Indonesia through Hibah Penelitian Disertasi Doktor Scheme under contract number NKB-332/UN2.RST/HKP.05.00/2021, in which Prof. Dr-Ing. Kalamullah Ramli is the corresponding author. Ms Hayati is in PhD study supported by Beasiswa Unggulan Dosen Indonesia Dalam Negeri (BUDI-DN), Lembaga Pengelola Dana Pendidikan (LPDP), and a cooperation of the Ministry of Research and Higher Education and the Ministry of Finance of the Republic of Indonesia.

References

[1] S.B. Thacker, R.L. Berkelman, PUBLIC HEALTH SURVEILLANCE IN THE UNITED STATES, Epidemiologic Reviews. 10 (1988) 164–190. https://doi.org/10.1093/oxfordjournals.epirev.a036021.

[2] L. Wang, L. Jin, W. Xiong, W. Tu, C. Ye, Infectious Disease Surveillance in China, in: Early Warning for Infectious Disease Outbreak, Elsevier, 2017: pp. 23–33. https://doi.org/10.1016/B978-0-12-812343-0.00002-3.

[3] Jamison DT, Breman JG, Measham AR, et al., editors., Chapter 53. Public Health Surveillance: A Tool for Targeting and Monitoring Interventions, in: Disease Control Priorities in Developing Countries. 2nd Edition, The International Bank for Reconstruction and Development / The World Bank, Washington (DC); Oxford University Press, New York, 2006: pp. 997–1016. https://www.ncbi.nlm.nih.gov/books/NBK11770/?report=reader.

[4] U.S. Department of Health and Human Services, CDC, Public Health 101 Series: Introduction to Public Health Surveillance, (2014). https://www.cdc.gov/publichealth101/surveillance.html (accessed July 20, 2020).

[5] Md.S. Rahman, N.C. Peeri, N. Shrestha, R. Zaki, U. Haque, S.H.A. Hamid, Defending against the Novel Coronavirus (COVID-19) outbreak: How can the Internet of Things (IoT) help to save the world?, Health Policy and Technology. 9 (2020) 136–138. https://doi.org/10.1016/j.hlpt.2020.04.005.

[6] S. Sareen, S.K. Sood, S.K. Gupta, IoT-based cloud framework to control Ebola virus outbreak, Journal of Ambient Intelligence and Humanized Computing. 9 (2018) 459–476. https://doi.org/10.1007/s12652-016-0427-7.

[7] Y. Song, J. Jiang, X. Wang, D. Yang, C. Bai, Prospect and application of Internet of Things technology for prevention of SARIs, Clinical EHealth. 3 (2020) 1–4. https://doi.org/10.1016/j.ceh.2020.02.001.

[8] H. Zhu, P. Podesva, X. Liu, H. Zhang, T. Teply, Y. Xu, H. Chang, A. Qian, Y. Lei, Y. Li, A. Niculescu, C. Iliescu, P. Neuzil, IoT PCR for pandemic disease detection and its spread monitoring, Sensors and Actuators B: Chemical. 303 (2020) 127098. https://doi.org/10.1016/j.snb.2019.127098.

[9] P. Lundrigan, K.T. Min, N. Patwari, S.K. Kasera, K. Kelly, J. Moore, M. Meyer, S.C. Collingwood, F. Nkoy, B. Stone, K. Sward, EpiFi: An in-Home IoT Architecture for Epidemiological Deployments, in: 2018 IEEE 43rd Conference on Local Computer Networks Workshops (LCN Workshops), IEEE, Chicago, IL, USA, 2018: pp. 30–37. https://doi.org/10.1109/LCNW.2018.8628482.

[10] European Centre for Disease Prevention and Control., Data quality monitoring and surveillance system evaluation: a handbook of methods and applications., Publications Office, LU, 2014. https://data.europa.eu/doi/10.2900/35329 (accessed November 13, 2020).

[11] W. Ahrens, I. Pigeot, eds., Handbook of Epidemiology, Springer New York, New York, NY, 2014. https://doi.org/10.1007/978-0-387-09834-0.

[12] Updated Guidelines for Evaluating Public Health Surveillance Systems: Recommendations from the Guidelines Working Group: (548222006-001), (2001). https://doi.org/10.1037/e548222006-001.

[13] R.P. Singh, M. Javaid, A. Haleem, R. Suman, Internet of things (IoT) applications to fight against COVID-19 pandemic, Diabetes & Metabolic Syndrome: Clinical Research & Reviews. 14 (2020) 521–524. https://doi.org/10.1016/j.dsx.2020.04.041.

[14] S.L. Groseclose, D.L. Buckeridge, Public Health Surveillance Systems: Recent Advances in Their Use and Evaluation, Annual Review of Public Health. 38 (2017) 57–79. https://doi.org/10.1146/annurev-publhealth-031816-044348.

[15] E.O. Nsoesie, S.A. Kluberg, S.R. Mekaru, M.S. Majumder, K. Khan, S.I. Hay, J.S. Brownstein, New digital technologies for the surveillance of infectious diseases at mass gathering events, Clinical Microbiology and Infection. 21 (2015) 134–140. https://doi.org/10.1016/j.cmi.2014.12.017.

[16] O.B. Leal-Neto, G.S. Dimech, M. Libel, W. Oliveira, J.P. Ferreira, Digital disease detection and participatory surveillance: overview and perspectives for Brazil, Revista de Saúde Pública. 50 (2016). https://doi.org/10.1590/S1518-8787.2016050006201.

[17] G.J. Milinovich, G.M. Williams, A.C.A. Clements, W. Hu, Internet-based surveillance systems for monitoring emerging infectious diseases, The Lancet Infectious Diseases. 14 (2014) 160–168. https://doi.org/10.1016/S1473-3099(13)70244-5.

[18] J.K. Harris, R. Mansour, B. Choucair, J. Olson, C. Nissen, J. Bhatt, Health Department Use of Social Media to Identify Foodborne Illness — Chicago, Illinois, 2013–2014, 63 (2014) 40.

[19] S.P. van Noort, C.T. Codeço, C.E. Koppeschaar, M. van Ranst, D. Paolotti, M.G.M. Gomes, Ten-year performance of Influenzanet: ILI time series, risks, vaccine effects, and care-seeking behaviour, Epidemics. 13 (2015) 28–36. https://doi.org/10.1016/j.epidem.2015.05.001.

[20] H.D. Park, O.-G. Min, Y.-J. Lee, Scalable architecture for an automated surveillance system using edge computing, The Journal of Supercomputing. 73 (2017) 926–939. https://doi.org/10.1007/s11227-016-1750-7.

[21] E. Christaki, New technologies in predicting, preventing and controlling emerging infectious diseases, Virulence. 6 (2015) 558–565. https://doi.org/10.1080/21505594.2015.1040975.

[22] P. Rattanaumpawan, A. Boonyasiri, S. Vong, V. Thamlikitkul, Systematic review of electronic surveillance of infectious diseases with emphasis on antimicrobial resistance surveillance in resource-limited settings, American Journal of Infection Control. 46 (2018) 139–146. https://doi.org/10.1016/j.ajic.2017.08.006.

[23] J. Murray, A.L. Cohen, Infectious Disease Surveillance, in: International Encyclopedia of Public Health, Elsevier, 2017: pp. 222–229. https://doi.org/10.1016/B978-0-12-803678-5.00517-8.

[24] Cisco Industrial Network Director, (2018). https://www.cisco.com/c/en/us/products/cloud-systems-management/industrial-network-director/index.html (accessed October 2, 2020).

[25] A. Demuth, R. Kretschmer, A. Egyed, D. Maes, Introducing Traceability and Consistency Checking for Change Impact Analysis across Engineering Tools in an Automation Solution Company: An Experience Report, in: 2016 IEEE International Conference on Software Maintenance and Evolution (ICSME), IEEE, Raleigh, NC, USA, 2016: pp. 529–538. https://doi.org/10.1109/ICSME.2016.50.

[26] W. Tibboel, M. Barnasconi, "Advancing traceability and consistency in Verification and Validation," in 2014 Design and Verification DVCon Conference and Exhibition Europe, Munich, Germany, Oct. 2014.

[27] Protiviti Team, "The Internet of Things: What Is It and Why Should Internal Audit Care?," 2016, https://www.protiviti.com/.

[28] I. Cooke and R. V. Raghu, "IS Audit Basics: Auditing the IoT," ISACA Journal, vol. 5, p. 5, Sep. 2018. https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/is-audit-basics-auditing-the-iot.

[29] D. Atri, H.K. Siddiqi, J.P. Lang, V. Nauffal, D.A. Morrow, E.A. Bohula, COVID-19 for the Cardiologist, JACC: Basic to Translational Science. 5 (2020) 518–536. https://doi.org/10.1016/j.jacbts.2020.04.002.

[30] World Health Organization, WHO Coronavirus Disease (COVID-19) Dashboard, Coronavirus Disease (COVID-19) Weekly Epidemiological Update and Weekly Operational Update. (2020). https://covid19.who.int.

[31] N. Hayati, K. Ramli, M. Suryanegara, Y. Suryanto, Potential Development of AES 128-bit Key Generation for LoRaWAN Security, in: 2019 2nd International Conference on Communication Engineering and Technology (ICCET), IEEE, Nagoya, Japan, 2019: pp. 57–61. https://doi.org/10.1109/ICCET.2019.8726884.

[32] M. Suryanegara, N. Hayati, An Integrated Model of Technical and Non-Technical Perspectives on Managing IoT Security, in: Proceedings of the 9th International Conference on Information Communication and Management - ICICM 2019, ACM Press, Prague, Czech Republic, 2019: pp. 142–146. https://doi.org/10.1145/3357419.3357450.

[33] M. Suryanegara, A.S. Mirfananda, M. Asvial, N. Hayati, 5G as Intelligent System: Model and Regulatory Consequences, in: Y. Bi, S. Kapoor, R. Bhatia (Eds.), Proceedings of SAI Intelligent Systems Conference (IntelliSys) 2016, Springer International Publishing, Cham, 2018: pp. 893–902. https://doi.org/10.1007/978-3-319-56994-9_61.

[34] E. Fadda, D. Mana, G. Perboli, R. Tadei, Multi Period Assignment Problem for Social Engagement and Opportunistic IoT, in: 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), IEEE, Turin, 2017: pp. 760–765. https://doi.org/10.1109/COMPSAC.2017.173.

[35] G. Jonsdottir, D. Wood, R. Doshi, IoT network monitor, in: 2017 IEEE MIT Undergraduate Research Technology Conference (URTC), IEEE, Cambridge, MA, 2017: pp. 1–5. https://doi.org/10.1109/URTC.2017.8284179.

[36] S.-H. Chang, R.-D. Chiang, S.-J. Wu, W.-T. Chang, A Context-Aware, Interactive M-Health System for Diabetics, IT Professional. 18 (2016) 14–22. https://doi.org/10.1109/MITP.2016.48.

[37] Natasa Adelayanti, UGM Innovation: GeNose Can Detect Covid-19 Less Than 2 Minutes, (2020). https://www.ugm.ac.id/en/news/20122-ugm-innovation-genose-can-detect-covid-19-less-than-2-minutes (accessed December 20, 2020).

[38] Natasa Adelayanti, UGM GeNose Receives Distribution and Marketing Permission, (2020). https://ugm.ac.id/en/news/20557-ugm-genose-receives-distribution-and-marketing-permission (accessed January 2, 2021).

[39] R. Madurai Elavarasan, R. Pugazhendhi, Restructured society and environment: A review on potential technological strategies to control the COVID-19 pandemic, Science of The Total Environment. 725 (2020) 138858. https://doi.org/10.1016/j.scitotenv.2020.138858.

[40] S. Sinche, D. Raposo, N. Armando, A. Rodrigues, F. Boavida, V. Pereira, J.S. Silva, A Survey of IoT Management Protocols and Frameworks, IEEE Communications Surveys & Tutorials. 22 (2020) 1168–1190. https://doi.org/10.1109/COMST.2019.2943087.

[41] WHO Team, Contact tracing in the context of COVID-19: interim guidance, 10 May 2020, (2020). https://apps.who.int/iris/handle/10665/332049.

[42] S.-C. Cha, M.-S. Chuang, K.-H. Yeh, Z.-J. Huang, C. Su, A User-Friendly Privacy Framework for Users to Achieve Consents With Nearby BLE Devices, IEEE Access. 6 (2018) 20779–20787. https://doi.org/10.1109/ACCESS.2018.2820716.

[43] A. Khalil, N. Mbarek, O. Togni, Self-Configuring IoT Service QoS Guarantee Using QBAIoT, Computers. 7 (2018) 64. https://doi.org/10.3390/computers7040064.

[44] K.A. Delic, On Resilience of IoT Systems: The Internet of Things (Ubiquity symposium), Ubiquity. 2016 (2016) 1–7. https://doi.org/10.1145/2822885.

[45] K. A. Delic and D. M. Penkler, "Architecting Resilient IoT Systems," Project: Exascale Computing Systems, Mar. 2018. Accessed: Jan. 07, 2021. [Online]. Available: https://www.researchgate.net/publication/331072091_Architecting_Resilient_IoT_Systems.

[46] M.J. McGrath, C.N. Scanaill, Regulations and Standards: Considerations for Sensor Technologies, in: Sensor Technologies, Apress, Berkeley, CA, 2013: pp. 115–135. https://doi.org/10.1007/978-1-4302-6014-1_6.

[47] IoT Device Certification Landscape, (2019). https://www.gsma.com/iot/resources/iot-device-certification-landscape/ (accessed September 20, 2020).

[48] G. Ferreira, Software Certification in Practice: How Are Standards Being Applied?, in: 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), IEEE, Buenos Aires, Argentina, 2017: pp. 100–102. https://doi.org/10.1109/ICSE-C.2017.156.

[49] A. Muñoz, A. Maña, Software and Hardware Certification Techniques in a Combined Certification Model:, in: Proceedings of the 11th International Conference on Security and Cryptography, SCITEPRESS - Science and and Technology Publications, Vienna, Austria, 2014: pp. 405–410. https://doi.org/10.5220/0005098204050410.

[50] WHO Headquarters (HQ), Digital tools for COVID-19 contact tracing, Digital Tools for COVID-19 Contact Tracing. (2020). https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1 (accessed September 25, 2020).

[51] J.V.L. do Monte, V.M. da S. Fraga, A.M.N.C. Ribeiro, D. Sadok, J. Kelner, IMMS: IoT Management and Monitoring System, in: 2018 IEEE Symposium on Computers and Communications (ISCC), IEEE, Natal, 2018: pp. 00422–00425. https://doi.org/10.1109/ISCC.2018.8538755.