Designing a Flow-based Mechanism for Accessing Electronic Health Records on a Cloud Environment

Tsung-Yin Ou[1] and Wen-Lung Tsai[2,*]

[1]*Department of Marketing and Distribution Management, National Kaohsiung University of Science and Technology, Kaohsiung 824, Taiwan*
[2]*Department of Information Management, Asia Eastern University of Science and Technology, New Taipei, 220 Taiwan*
E-mail: outy@nkust.edu.tw; wltsai@mail.aeust.edu.tw
[*]*Corresponding Author*

Received 09 July 2021; Accepted 24 April 2022;
Publication 30 July 2022

Abstract

Electronic health record (EHR) implementation not only to facilitate doctor-patient communication reduces paper consumption but also allows the rapid exchange of medical records, integrating patients' medical information from different locations. However, the costs of establishing massive and repetitive systems, constructing databases, and maintaining and exchanging data, as well as the energy consumption underscoring such an operation, represent substantial costs for a medical institution. Therefore, it is important to develop a cloud solution for EHRs and to provide a platform where resources are truly shareable. This study investigates the feasibility of cloud EHR services provided by trusted third parties. However, not only do medical records stored in an access environment with multiple users potentially endanger patient privacy, but also, without well-designed access control, such an environment may beget excessive unnecessary data access, which is costly and hinders

Journal of Web Engineering, Vol. 21_5, 1491–1518.
doi: 10.13052/jwe1540-9589.2156

cloud computing. To address the dual challenge of protecting patient privacy and allowing cloud computing, this study proposes the doctor–patient workflow and implements a web-based system. This mechanism ensures patients' data security and addresses the demand of EHR cloud sharing, i.e., controlling EHR access authorities. The proposed method can protect the privacy of patients' medical records on the cloud and grant users with minimum granularity access, thereby creating a system with the advantages of data security and cloud computing. This study proposes the doctor–patient workflow as the access control mechanism of cloud medical records, which minimizes the granularity of access. In addition, the access authority of the workflow dynamically changes with the environment, which ensures patients' access to their medical records and defines the appropriate timing of cloud data access operations, thereby preventing unnecessary energy consumption. In practice, considerable contributions can be made to the establishment of access control and promotion of the cloud environment for medical records.

Keywords: Electronic health records, cloud environment, access control, workflow, doctor-patient communication, web-based system.

1 Introduction

In an attempt to improve the quality of healthcare and patient safety, Taiwan initiated the implementation of electronic health records (EHRs) in 2008. This program accelerated the informatization of medical-related works in medical institutions and the electronization of medical records. Consequently, medical institutions have started storing patients' electronic medical records (EMRs) in each other's hospital information systems (HISs). Subsequently, to resolve the problem of incomplete medical records when patients visit different medical institutions, Taiwan established an EMR exchange center as a mechanism for sharing EMRs between different medical institutions. Owing to the possibility of exchanging medical records among different medical institutions, an EHR system was formed. The system provides doctors with accurate and comprehensive patient information in one diagnosis period, thereby preventing them from prescribing considerably repetitive and unnecessary tests and medications.

Although introducing the information system to medical institutions has many benefits, the costs of implementation, including hardware, software, IT technicians, and complicated system deployment, are substantial [1]. Most medical institutions in Taiwan are small clinics. Therefore, the

incomplete implementation of EHRs in Taiwan, due to the failure to introduce such information systems to these small clinics, impairs Taiwan's medical quality and patient rights.

As a cross-hospital EMR exchange involves retrieving medical records that meet the requirements of the HIS of each medical institution before integration, it cannot be referred to as an integral EHR. Furthermore, because the methods and details of internal data storage in the HIS vary between institutions, multiple primary standards that promote EHRs are available. As some areas have experienced an inadequate degree of informatization or insufficient funds, EMRs cannot be implemented in clinics in these areas, thereby further impairing the EHR development. In 2018, the proportion of EMR implementation in Taiwan was 80% (approximately 400) for hospitals and 70% (approximately 14,000) for clinics [2]. On the contrary, only 300 hospitals were equipped with EMR exchanges, indicating that achieving comprehensive EHR implementation remains a difficult task.

Cloud computing is a useful solution, where instead of investing in the in-house construction of information systems, users utilize the Internet to create an outsourcing operation mode [3, 4]. Gao and Sunyaev [5] indicated that cloud computing can improve healthcare services and therefore recommended the promotion of EHRs via cloud computing. They also suggested that cloud computing can help reduce the costs of EHR implementation, including cost related to hardware, software, and network and license fees, in small-scale medical institutions. A unified EHR control through the cloud data center can also promote integrity and consistency.

However, in an environment of resource sharing and common access by multiple users, challenges of such a unified EHR control system include data confidentiality, privacy, access control, authentication, and authorization. Shah et al. [6] pointed out that EMR security and privacy under a sharing environment deserve more attention than that those in the traditional model of in-house systems. The Health Insurance Portability and Accountability Act of 1996 [7] proposed by the United States declares that patients' medical records are a part of personal privacy and introduces two globally recognized health information privacy and security principles [8]: (1) the principle of non-disclosure and (2) the principle of minimum necessary. Whereas EMR is usually considered a private cloud system, the EHR is defined as a public cloud system. EMR and EHR can reside on different cloud environment under various technologies and standards. EMR contains local information and provides fast and accurate delivery, the major advantage of EHR in medical practice is the availability of cross-provider medical information [9].

That is, if an EMR is stored in a cloud environment without good access or authorization control, then patient privacy rights would be violated.

From the perspective of computing consumption, although cloud computing mitigates the excessive energy consumption from equipment over-expansion during the construction of in-house information systems, the cloud cluster composed of thousands of nodes still consumes a large amount of energy, including the power consumption of the host, air conditioning, and network transmission. Within the cloud computing system, the energy consumed by data transmission in the network is the most substantial [8]. Therefore, failure to create an effective access control mechanism to restrict users from accessing cloud data outside specific and appropriate timeframes incurs considerable additional costs.

Thus, to enable patient privacy while mitigating the inefficient use of cloud computing technology in EHR exchange systems, the purpose of this study designs a flow-based mechanism and implement a system scenario to access EHR and protect patient privacy. The following sections include literature review, methodology, case and system scenario, verification and discussion and conclusion.

2 Literature Review

2.1 Cloud Medical Records

Traditional in-house HISs encounter different problems, such as limited storage, continuously increasing data volume, excessively high data backup and storage costs, and difficulty in secure data exchanging [10]. Alternatively, a platform built via a cloud that allows exchanging and sharing medical information and provides cluster care service channels can promote a more effective cooperation between medical services provided by different medical institutions. In addition to eliminating the cost of setting up an internal information system at each medical institution, the service from cloud providers grants flexible access to medical record resources, thereby preventing over-investment in equipment and inadequate access at peak hours. Whether visiting or being referred to either a large hospital or a small clinic, in a large city or a small town, patients can benefit from the medical services that result from on-demand and broad network accesses supplied by cloud computing, which can provide the most complete information to doctors [11].

With the popularity of mobile devices, ubiquitous data access can be achieved by providing services from the cloud data center. In fact, multiple cloud innovations have utilized cloud data centers as the data access and

storage space. This solution not only solves the insufficient storage capacity problem of mobile devices but also grants access to medical information anywhere in the world through the portability of mobile devices [12]. Sending patient information back to the cloud data center through wireless sensing networks for doctors to use can also improve the quality of medical information transmission and exchange [13]. Furthermore, the adoption of cloud computing's decentralized processing to address the increasing number of medical image files can accelerate the analysis and processing of medical data [14].

2.2 EMRs

The term "EMR" in the medical dictionary has two versions: EMR and EHR. Despite their frequent alternate uses, health and insurance industries are not familiar with the differences of the two. EMR is a legal record of a patient's visit to a medical institution and is also the source of data that constitutes an EHR [15]. A brief description of the two definitions are provided below.

Table 1 Validation checks and definitions

	EMR	EHR
Definition	The legal record of a patient's visit to a medical institution	Composed of the EMRs from multiple medical institutions
Owner Access	Only accessible by the owner medical institution and does not include EMRs from other medical institutions	Accessible by the patient or an authorized person. EHR can be shared between different medical institutions via electronic data exchange

(1) EMR

According to the European Union's General Data Protection Regulation [16], the patient would be the owner of EMR. In Taiwan, with the development of EMR, EMR systems have been widely used in almost all medical institutions for routine clinical work. A large number of EMRs are generated and accumulate during everyday patient care [17]. A medical institution stores a patient's medical information in its own HIS. Upon a patient's visit, the doctor can view the EMR or add or revise the contents.

(2) EHR

An EHR consists of a combination of EMRs from different medical institutions, which allows patients to access their EMRs that exist with various

medical institutions from any location. Therefore, an EHR can only be generated through an electronic process that involves standardized EMRs, which are owned by the patients themselves.

Currently, most medical institutions use their own in-house information systems and databases to provide EMR services. Because the EMR is located in the same system, its exchange and administration are considerably easier than those of traditional paper medical records. However, to achieve a fully integrated EHR, where medical records can be shared between different medical institutions in a patient-centric approach, the existing implementation scheme relies on the complete establishment of an EMR exchange platform in each medical institution. This system however becomes a challenge for small-scale medical institutions [18]. On the contrary, cloud infrastructure can help build a unified data control center that provides integral EHR services, allowing a patient's personal medical records to be shared between medical institutions. In addition, such a cloud solution can eliminate the need for medical institutions to employ complex procedures and medical record formats previously required for EMR exchange and the need for a deployment of information equipment. Instead, a cloud infrastructure can provide on-demand services through a cloud EHR.

2.3 EHR Access Control on Cloud Environment

Because EHRs are composed of multiple EMRs, users must determine data access according to the authorization scope. To do so, Joshi et al. [19] proposed two types of attribute-based and role-based access control mechanisms to establish a secure access control model for EHRs. The attribute-based mechanism decomposes EHRs into multiple elements and sub-elements before presenting them in a hierarchical structure. Each element and sub-element are assigned one or more attributes, which are classified according to the degree of privacy, use intention, or type of element. Therefore, this hierarchical attribute structure can ensure that specific information can only be accessible by specific users in specific situations, thereby achieving granularity authorization and access control. However, when EHRs have a complicated system where multiple users have different granularities of data access, a significant number of attributes must be created, resulting in a complex structure that is difficult to implement and for which it is challenging to maintain access control rules. On the contrary, the role-based mechanism integrates the role and identity of the participating medical team, diagnosis

type, and EMR with authorized access into a tree structure, the root nodes of which represent the individual hash value of a patient. The advantage of this mechanism is as follows: when the medical team changes, the tree structure can be flexibly modified. However, although this approach can overcome the deficiencies of the attribute-based access control model, it restricts the granularity of the authorized access.

Alternatively, Rauf et al. [20] proposed a task-role-based access control mechanism to manage user data access in the cloud environment. Tasks sequentially executed by users form a workflow, the data access authorities of which are dynamically changed by sequential tasks. However, although this approach does allow minimum authorization, duty division, task delegation, and access at specific times and locations, these permissions are granted by the system administrators rather than according to the patient's behavior, which may lead to an abuse of authority.

Ramu et al. [21] proposed a fine-grained data access control in multi-owner settings, wherein patients used the attribute-based encryption (ABE) method to upload their medical records on the cloud. This method has improved the complexity of private key generation and distribution, where users obtain access rights through the attribute authorization center. However, by replacing the private key with the patient attribute, this approach becomes easy to declassify if the attribute structure is not complicated enough. On the contrary, an immensely complicated attribute structure is difficult to manage and maintain, as mentioned earlier. In addition, the assignment of private keys based on attributes through the authorization center also presents the risk of abuse of authority.

Other than the problems listed above, in clinical practices, instead of attending to a single or specific patient, doctors often diagnose many patients within a certain period. However, the access control studies mentioned above are designed for the access control of a single patient's data rather than for an overall medical record use environment where the characteristics and connections between multiple patients are utilized to design and restrict access authority. If the user's access to medical records cannot be limited to a minimum period, in addition to the confidentiality and privacy of patients' medical records being threatened, then the excessive energy consumption caused by users accessing too much unnecessary data on the cloud system can also compromise the environmental protection benefits brought by the cloud environment.

2.4 Workflow

The concept of workflow originated in the field of production process and office automation. Its purpose is to design a process plan for work activities with a fixed sequence. Subsequently, through the decomposition of designed activities, staff can perform tasks in accordance with existing rules and procedures, thereby increasing productivity and production while reducing costs. According to the definition of the Workflow Management Coalition [22], a workflow is a business program that can be fully or partially automated, and it involves the transfer of documents, information, or tasks between different executors based on a series of programmatic rules.

As an execution program composed of many tasks, each task in the workflow is conducted by one or more executors. This executor can be either an information system or a person. In the latter case, a workflow refers to the completion of tasks in a certain order by one or more people, during which the production is increased through collaboration. The emergence of the workflow management system [23] as a result of advanced digital technology has further enhanced the efficiency of the workflow.

There is an optimal execution order for tasks composing the workflow. Each task is sequentially completed by the executor following a given order. In the context of this study, based on their sequential and dependent characteristics, tasks within the workflow are replaced with doctors and patients. Therefore, two workflows are created: a patient workflow consisting of several patients who register with the same outpatient clinic and a doctor workflow where doctors delegate patients to other doctors during the diagnosis process. In this study, the two-workflow system is referred to as the doctor–patient workflow. Due to the mutual constraints of the processes performed by doctors and patients, the authorization must be dynamically changed according to the execution status of the processes, thereby achieving environment-based dynamic access control.

3 Methodology

3.1 Concept Illustration

To allow patients to authorize and control EHRs themselves, this study considers the compulsory pre-visit registration action of a patient as the trigger. Therefore, each registration action of a patient authorizes the access of a specific doctor during a specific diagnosis period. During this period, a specific doctor can access the patient's specific medical records only when the

doctor's credentials and the patient's credentials (e.g., a health insurance card) are both verified. The related specific nouns of Doctor–patient Workflow and in this study are defined and illustrated as follows.

- Doctor: The doctor holds the primary diagnostic role of a patient workflow or a diagnosis period and is a cloud EHR user that requires authorization.
- Diagnosis Period: The diagnosis period refers to the doctor's outpatient consultation scope. All patients in this diagnosis period form the patient workflow according to the registration order.
- Granularity: In this study, granularity refers to the time scope during which cloud EHR authorizations are open.
- Doctor–patient Workflow: To minimize the granularity of the authorization scope, this study utilizes the order of multiple patient registrations to generate the so-called patient workflow. The authorization timing of the patient's previous and current medical records is determined by consecutive patients in the workflow and the execution status of the patient's medical records. For example, a doctor can acquire the execution authority of the N + 1th patient only after the doctor has performed some actions (e.g. read (R), write (W) and prohibit (P), shown in Equation (1) Section 3.2) on the medical records of the Nth patient. In other words, it means that the authority is in the execution queue when these actions are performed on Nth patient. In addition to using the patient workflow formed during a diagnosis period, the doctor may also refer the patient to other doctors for tasks, such as blood tests or X-ray imaging during the diagnosis. When a patient has seen more than one doctor, the patient has crossed different patient workflows, which forms the so-called doctor workflow described in this study. The execution authority of the Nth doctor who has delegated the task to other doctors will be temporarily restricted and will not be restored until the delegated N + 1th doctor completes the necessary action in the medical record. The concept of the doctor–patient workflow is shown in Figure 1.

3.2 Research Design

This study aims to apply the doctor–patient workflow to the access of patients' medical records on the cloud, the authority of which is dynamically adjusted according to the connections formed during clinical consultations. By restricting doctors' access control to the minimum necessary granularity, a safe access control mechanism can be established.

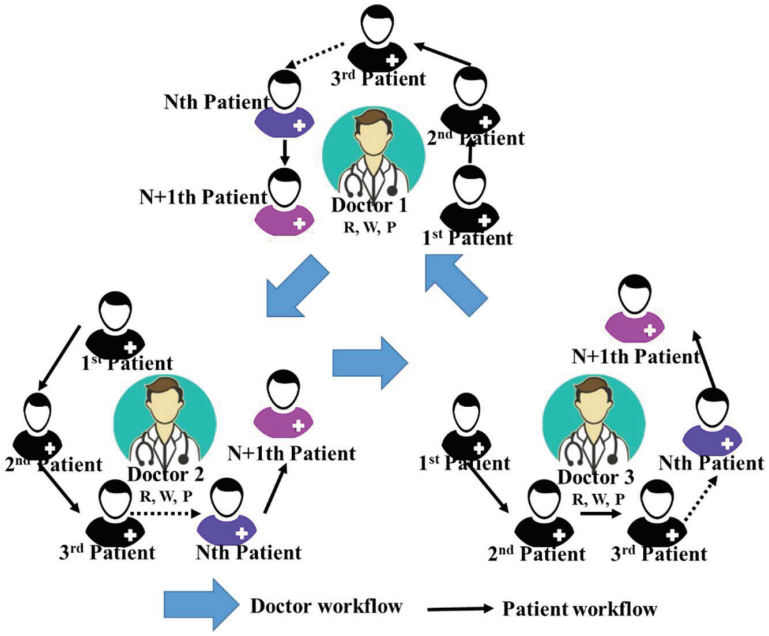

Figure 1 Doctor–patient workflow.

3.2.1 Authorization formulation

An authorization, shown in Equation (1), includes the authorization's current execution status, its authorized actions, and the scope of its diagnosis period:

$$\text{Auth}_{ij}\ (\text{status, action, diagnose period})$$

$$\begin{cases} \text{i: index of diagnose period} \\ \text{j: index of Patient Workflow} \end{cases}$$

$$\text{Status} = \begin{cases} \text{N: never} \\ \text{B: buffer} \\ \text{D: delegation} \\ \text{C: completion} \end{cases} \qquad \text{Action} = \begin{cases} \text{R: read} \\ \text{W: write} \\ \text{P: prohibit} \end{cases} \tag{1}$$

Status denotes the current authorization status, which includes four states: never (N), buffer (B), delegation (D), and completion (C). N indicates that the authorized medical record has not been processed by the doctor; B indicates that the patient who is due is absent and therefore has been temporarily placed in the queue by the doctor; D indicates that during the diagnosis period, the

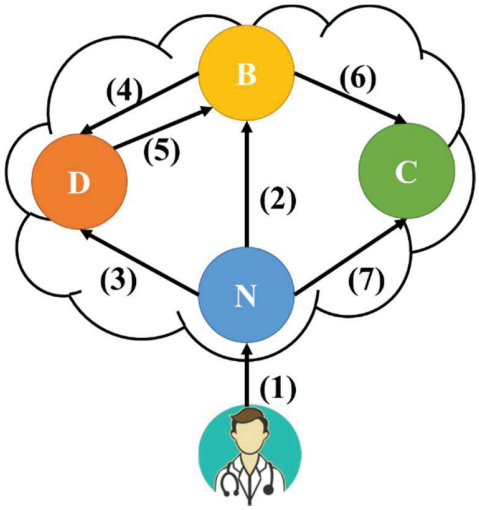

Figure 2 Authorization status.

doctor has assigned this patient to the patient workflow of another diagnosis period; and C indicates that the patient has completed his visit and the doctor has uploaded and signed off the medical record.

Action denotes the executable access authority. It includes three access permissions: read (R), write (W), and prohibit (P). R indicates that the authorized user can only view the medical records, without the need to verify the patient's credentials; W covers the authority of R and allows the user to add a new entry to the medical record once the patient's credentials are verified; and P indicates that authorization has been banned. Figure 2 illustrates the transition path of the authorization status.

The authorization status transition shown in Figure 2 consists of the following: (1) indicates the establishment of the authorization either triggered by patients or delegated by doctors, the initial status of which is N; (2) indicates the placement of the authority into the queue by the doctor, as the patient, whose status has been transitioned to B, has not arrived within the time limit; (3) and (4) indicate the delegation of the authority to a doctor in another diagnosis period as the current doctor cannot complete the diagnosis during the consultation, which requires the patient's credentials; (5) indicates the completion of the diagnosis by the delegated doctor, which changes the medical record authorization status of the diagnosis period from D to B; and (6) and (7) indicate the completion of the diagnosis, during which the doctor uploads and signs off on the medical record.

3.2.2 Access control in the patient workflow

The process of establishing the authorization by the patient through the registration action is shown in Equation (2). All patients in the same diagnosis period are arranged according to the registration order. Except for the last patient, each patient is connected to the next one. Such a connection is referred to as the dependency patient here. Because the doctor in charge of this diagnosis period must consult patients one by one following this order, a dependency patient workflow is created (Equation (3)):

$$\mathrm{P_j(dependency\ patient)} \rightarrow \mathrm{Auth_{ij}(S, A, DP_i)} \tag{2}$$

$$\text{Patient Workflow} = \begin{cases} \mathrm{P_1(P_2)} \rightarrow \mathrm{Auth_{i1}(N, W, DP_i)} \\ \mathrm{P_2(P_3)} \rightarrow \mathrm{Auth_{i2}(N, R, DP_i)} \\ \mathrm{P_3(P_4)} \rightarrow \mathrm{Auth_{i3}(N, R, DP_i)} \\ \cdots\cdots\cdots\cdots \\ \mathrm{P_j(null)} \rightarrow \mathrm{Auth_{ij}(N, R, DP_i)} \end{cases} \tag{3}$$

The dependency patient of PN is PN + 1, and so on, until the last patient (Pj), whose dependency patient is null as there are no more patients in the diagnosis period. The initial statuses of all authorizations are N, indicating that the doctor has not performed any action on the medical records. Moreover, except for that of the first patient, which is W, the access authorities of all remaining patients are R, thereby only authorizing the doctors to view the medical records. Subsequently, when doctors change the authorization status through the user interface during the diagnosis period (Figure 2), the access authority of the dependency patient changes accordingly.

- (2), (3), (7): Once the doctor has processed the medical record of patient PN, the action authorization of patient PN + 1 changes from R to W.
- (3), (4): Once the doctor delegates patient PN to another diagnosis period, the action authorization of this patient changes from W to R, which is scaled down.
- (6), (7): Once the doctor completes the diagnosis of patient PN and uploads and signs off on this patient's records, the action authorization changes from W to P, prohibiting any further operations.

3.2.3 Access control in the doctor–patient workflow

When doctors (Dr) delegate a patient to other patient workflows due to the need for a diagnosis (Equation (4)), except for the first doctor, other

doctors, referred to as the dependency doctors here, are assigned by the previous doctor. The authority of the delegating doctor must be changed when assigning patients to another patient workflow, so the delegating doctor's access authority is restricted. Owing to the delegation process, the patient can be consulted by different doctors in different patient workflows, thereby forming the doctor workflow (Equation (5)).

$$\mathrm{P_j\ (dependency\ doctor)} \rightarrow \mathrm{Auth_{ij}\ (S,\ A,\ DP_i)} \tag{4}$$

$$\text{Doctor Workflow} = \begin{cases} \mathrm{P_1(P_2)} \rightarrow \mathrm{Auth_{i1}(N, W, DP_i)} \\ \mathrm{P_2(P_3)} \rightarrow \mathrm{Auth_{i2}(N, R, DP_i)} \\ \mathrm{P_3(P_4)} \rightarrow \mathrm{Auth_{i3}(N, R, DP_i)} \\ \cdots\cdots\cdots\cdots \\ \mathrm{P_i(Dr_{i-1}} \rightarrow \mathrm{Auth_{ij}(N, R, DP_i)} \end{cases} \tag{5}$$

The dependency doctor of DrN is DrN-1, and so on, until that of Dr1, which is null. In addition, except for that of DrN, which is N, the authorization statuses of all other doctors are D as they wait for the assigned doctor to complete the diagnosis. The status and access authority of DrN are administered by the patient workflow mentioned in the previous section, until the status changes in Step (6) or (7) (Figure 2). At this moment, the completion of the delegated diagnosis changes the status of DrN-1 to (5) and the action authorization of DrN-1 from R to W.

3.3 Doctor–patient Workflow vs. a Workflow

A workflow is composed of tasks, whereas the doctor–patient workflow proposed here is composed of doctors and patients. Different entities in the process will lead to different characteristics of the workflow. Because the purpose of a workflow is to improve production efficiency through the division and cooperation of labor between different tasks, its tasks are conducted by multiple executors, either sequentially or in parallel. On the contrary, during a certain diagnosis period, the sole executor of the doctor–patient workflow is a specific doctor. Because a doctor cannot diagnose more than one patient at a time, the task cannot be conducted in parallel.

Furthermore, because a workflow is planned in advance with a fixed execution order to achieve a specific purpose, to complete the entire process, all tasks must follow this order without any arbitrary addition or deletion. However, in the doctor–patient workflow, the consultation of subsequent

patients can be continued, e.g., in the case of a patient's absence. In addition, the insertion of a patient to the outpatient visit queue through the emergency department is also acceptable in this process.

4 Case and System Scenario

4.1 Case Scenario

The following scenario is used to demonstrate and explain the proposed workflow. Suppose there are six patients, P1–P6. During the visit, P1–P4 are sequentially referred to doctor Dr1 at the Division of Pediatric (DP1), whereas P5 and P6 are sequentially referred to Dr2 for blood tests (DP2). Therefore, two patient workflows are created, as shown in Equation (6):

$$\begin{aligned}
\mathrm{Dr}_1 &\begin{cases} \mathrm{P}_1(\mathrm{P}_2) \rightarrow \mathrm{Auth}_{11}(\mathrm{N}, \mathrm{W}, \mathrm{DP}_1) \\ \mathrm{P}_2(\mathrm{P}_3) \rightarrow \mathrm{Auth}_{12}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_1) \\ \mathrm{P}_3(\mathrm{P}_4) \rightarrow \mathrm{Auth}_{13}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_1) \\ \mathrm{P}_4(\mathrm{null}) \rightarrow \mathrm{Auth}_{14}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_1) \end{cases} \\
\mathrm{Dr}_2 &\begin{cases} \mathrm{P}_5(\mathrm{P}_6) \rightarrow \mathrm{Auth}_{25}(\mathrm{N}, \mathrm{W}, \mathrm{DP}_2) \\ \mathrm{P}_6(\mathrm{null}) \rightarrow \mathrm{Auth}_{26}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_2) \end{cases}
\end{aligned} \tag{6}$$

Except for the access authorities of P1 and P5, which are both W, those of the subsequent patients are R, thereby only granting the users with the authority to view the medical records of P2, P3, P4, and P6.

In this scenario, P1 comes to the doctor on time. Upon his arrival, the doctor verifies the patient's identity and his health insurance card and then consults the patient. In this case, as the authorization of the action of Auth11 is W, Dr1 can add new entries to this patient's medical records to document his treatment. Subsequently, when Dr1 uploads and signs off the new entry with his login, as the status transition of Step (7) is triggered (Figure 2), the status and authority of DP1 in the patient workflow are changed as per Equation (7).

$$\mathrm{Dr}_1 \begin{cases} \mathrm{P}_1(\mathrm{P}_2) \rightarrow \mathrm{Auth}_{11}(\mathrm{C}, \mathrm{P}, \mathrm{DP}_1) \\ \mathrm{P}_2(\mathrm{P}_3) \rightarrow \mathrm{Auth}_{12}(\mathrm{N}, \mathrm{W}, \mathrm{DP}_1) \\ \mathrm{P}_3(\mathrm{P}_4) \rightarrow \mathrm{Auth}_{13}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_1) \\ \mathrm{P}_4(\mathrm{null}) \rightarrow \mathrm{Auth}_{14}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_1) \end{cases} \tag{7}$$

When P1 completes his visit, it is P2's turn. Suppose at this time P2 is not present; Dr1 can temporarily place the authorization of P2 in the queue. Because this method initiates the status transition of Step (2), the status and authority of DP1 in the patient workflow are changed as per Equation (8).

$$\mathrm{Dr}_1 \begin{cases} \mathrm{P}_1(\mathrm{P}_2) \rightarrow \mathrm{Auth}_{11}(\mathrm{C}, \mathrm{P}, \mathrm{DP}_1) \\ \mathrm{P}_2(\mathrm{P}_3) \rightarrow \mathrm{Auth}_{12}(\mathrm{B}, \mathrm{W}, \mathrm{DP}_1) \\ \mathrm{P}_3(\mathrm{P}_4) \rightarrow \mathrm{Auth}_{13}(\mathrm{N}, \mathrm{W}, \mathrm{DP}_1) \\ \mathrm{P}_4(\mathrm{null}) \rightarrow \mathrm{Auth}_{14}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_1) \end{cases} \tag{8}$$

Due to P2's absence, it is P3's turn to see the doctor, and P3 has already arrived. However, during P3's consultation, Dr1 believes that P3 must have a blood test (DP2) before continuing his treatment at DP1. Therefore, Dr1 delegates P3 to the patient workflow of DP2 under Dr2. In addition to triggering the status transition of Step (3), because the patient has crossed multiple patient workflows, a doctor workflow is created between Dr1 and Dr2. In this case, the statuses and authorities of the patient workflows of DP1 and DP2, as well as the doctor workflow created as a result of the delegation, are shown in Equation (9):

$$\begin{aligned} \mathrm{Dr}_1 &\begin{cases} \mathrm{P}_1(\mathrm{P}_2) \rightarrow \mathrm{Auth}_{11}(\mathrm{C}, \mathrm{P}, \mathrm{DP}_1) \\ \mathrm{P}_2(\mathrm{P}_3) \rightarrow \mathrm{Auth}_{12}(\mathrm{B}, \mathrm{W}, \mathrm{DP}_1) \\ \mathrm{P}_3(\mathrm{P}_4) \rightarrow \mathrm{Auth}_{13}(\mathrm{D}, \mathrm{R}, \mathrm{DP}_1) \\ \mathrm{P}_4(\mathrm{null}) \rightarrow \mathrm{Auth}_{14}(\mathrm{N}, \mathrm{W}, \mathrm{DP}_1) \end{cases} \\ \mathrm{Dr}_2 &\begin{cases} \mathrm{P}_5(\mathrm{P}_6) \rightarrow \mathrm{Auth}_{25}(\mathrm{N}, \mathrm{W}, \mathrm{DP}_2) \\ \mathrm{P}_6(\mathrm{P}_3) \rightarrow \mathrm{Auth}_{26}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_2) \\ \mathrm{P}_3(\mathrm{null}) \rightarrow \mathrm{Auth}_{23}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_2) \end{cases} \\ \mathrm{P}_3 &\begin{cases} \mathrm{P}_1(\mathrm{null}) \rightarrow \mathrm{Auth}_{13}(\mathrm{D}, \mathrm{R}, \mathrm{DP}_1) \\ \mathrm{P}_2(\mathrm{null}) \rightarrow \mathrm{Auth}_{23}(\mathrm{N}, \mathrm{R}, \mathrm{DP}_2) \end{cases} \end{aligned} \tag{9}$$

At this moment, because of the restrictions of the doctor workflow, the action authorization of Auth13 is restrained by Auth23. When Dr1 continues to see P4, Dr2 executes the patient workflow of DP2 as before, until Auth23 triggers the status transition of Steps (6) and (7), the status and authority of

which change as per Equation (10).

$$\begin{aligned}
\mathrm{Dr}_1 &\begin{cases} \mathrm{P}_1(\mathrm{P}_2) \rightarrow \mathrm{Auth}_{11}(\mathrm{C},\mathrm{P},\mathrm{DP}_1) \\ \mathrm{P}_2(\mathrm{P}_3) \rightarrow \mathrm{Auth}_{12}(\mathrm{B},\mathrm{W},\mathrm{DP}_1) \\ \mathrm{P}_3(\mathrm{P}_4) \rightarrow \mathrm{Auth}_{13}(\mathrm{B},\mathrm{W},\mathrm{DP}_1) \\ \mathrm{P}_4(\mathrm{null}) \rightarrow \mathrm{Auth}_{14}(\mathrm{N},\mathrm{W},\mathrm{DP}_1) \end{cases} \\
\mathrm{Dr}_2 &\begin{cases} \mathrm{P}_5(\mathrm{P}_6) \rightarrow \mathrm{Auth}_{25}(\mathrm{C},\mathrm{P},\mathrm{DP}_2) \\ \mathrm{P}_6(\mathrm{P}_3) \rightarrow \mathrm{Auth}_{26}(\mathrm{C},\mathrm{P},\mathrm{DP}_2) \\ \mathrm{P}_3(\mathrm{null}) \rightarrow \mathrm{Auth}_{23}(\mathrm{C},\mathrm{P},\mathrm{DP}_2) \end{cases} \\
\mathrm{P}_3 &\begin{cases} \mathrm{P}_1(\mathrm{null}) \rightarrow \mathrm{Auth}_{13}(\mathrm{B},\mathrm{W},\mathrm{DP}_1) \\ \mathrm{P}_2(\mathrm{null}) \rightarrow \mathrm{Auth}_{23}(\mathrm{C},\mathrm{P},\mathrm{DP}_2) \end{cases}
\end{aligned} \tag{10}$$

Lastly, once Dr1 finishes the execution of all the patient workflows for which Dr1 is responsible, the statuses of all patients are changed to C and their authorities to P, marking the completion of the access control of the entire doctor–patient workflow.

4.2 System Scenario

In this section, the system's workflow will be explained by simulating a scenario where a doctor is seeing patients. The characters in this scenario and their actions are shown in Table 2.

As this system was constructed in a web-based environment, Google Chrome was used to show its interfaces. Based on the users of the system, the usage scenarios that were examined here included the registration of patients and the addition of new medical records by a doctor. First, the patient used the system to register themselves (the screen after patient registration is shown in Figure 3) and then gave the doctor authorization to access their medical records. After a number of patients have been registered, a patient flow will be

Table 2 Characters and their actions in the simulated scenario

Character	Actions
Dr. Chen	Seeing patients
Dr. Chen	Adding new medical records
C. T. Lin	Seeing a doctor
B. C. Liou	Seeing a doctor
S. H. Wang	Seeing a doctor

Figure 3 Screen after patient registration.

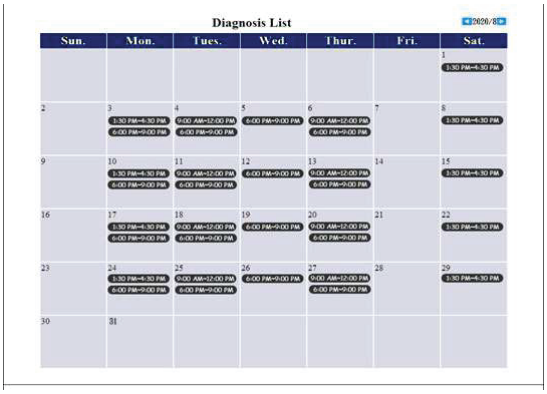

Figure 4 Screen showing all of a doctor's appointments.

formed according to their appointment times. The access rights of the doctor to the medical record of each patient will then be controlled by this patient flow.

After all of the patients at this clinic have been registered, Dr. Chen will arrange the registered patients into a patient flow for the 8/18/2020 9:00–12:00 examination period. Dr. Chen must log into this system before seeing any patients. The screen that appears after the doctor logs in is shown in Figure 4. Here, all of the patient appointments of the doctor will be shown in the form of a calendar, and the doctor may click on an appointment to see the patient treatment screen, as shown in Figure 5. The menu on the left shows the three hypothetical registered patients, C. T. Lin, B. C. Liou and S. H. Wang, and the patient flow formed by other patients.

Figure 5 Patient treatment screen.

Table 3 State-icon legend

Icon	State	Meaning
	N	Never
	B	Buffer
	D	Delegated
	C	Completed

Figure 5 shows that in the patient flow, there is an icon next to each patient name that indicates the state of use of the patient's medical record. As per Equation (1) in Section 3, these states are never (N), buffer (B), delegated (D), and completed (C). The icons and states they represent are shown in Table 3.

Because this scenario assumes that the three aforementioned patients have not seen a doctor yet, the state of their medical records is N. If a patient misses an appointment, then the doctor may temporarily assign this patient to a queue to move on to the next patient. In this case, the system will change the state of this patient's medical record to B. During treatment, a doctor may also use the "delegate" function to assign this patient to other patient flows. The state of this patient's medical record then becomes D. After the treatment of a patient is completed, the doctor will store a record of the patient's most recent treatment in the system, and the state of the patient's medical record will change to C.

Due to the patient-flow access control mechanism, if, for instance, a doctor did not perform a "create," "pending," or "delegate" operation on the medical record of C. T. Lin, he/she will then be prevented from accessing the medical records of patients that come after C. T. Lin in the patient flow, as shown in Figure 5. Because the treatment of C. T. Lin is still in progress,

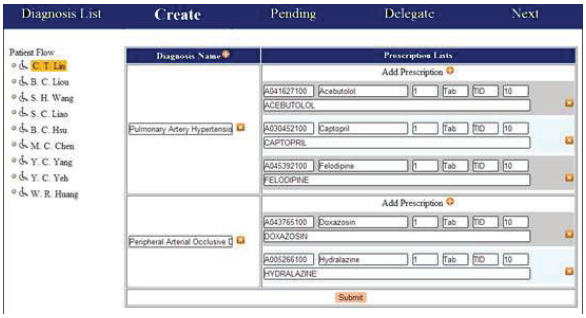

Figure 6 Addition of a new treatment record.

should the doctor try to access the medical record of B. C. Liou, the following error message will appear "You have no enough authorization to operate this patient's diagnosis records!" and no further action will occur. To record the prescription that was used for the current treatment, the doctor simply has to fill a form for a new prescription, as shown in Figure 6. After this form has been filled, pressing "submit" will store the prescription in the system. This step facilitates the exchange of EMRs that are stored in the system.

5 Verification and Discussion

5.1 Design and Reliability of the Questionnaire

A questionnaire was designed to evaluate the proposed doctor–patient workflow. The first four questions in the questionnaire are meant to gauge how experts feel about the problems being addressed by this study, based on current EHR arrangements and issues, such as patient rights and interests. The fifth to eighth questions were designed to evaluate the access control mechanism proposed by this study. The fifth question is about the principle of nondisclosure and the protection of patient rights and interests, and the sixth question is about the direct collection and most reasonable use of personal data. The seventh question is about the minimum required granularity, and the eighth questions is about the principle of respect and fairness. Finally, the ninth and tenth questions are meant to assess how experts feel about the overall benefit provided by the proposed mechanism.

In addition, 10 experts were asked to use a system that was created based on the proposed access control mechanism, and then fill out the aforementioned questionnaire. The questionnaire items were answered using a 5-point

Likert scale, that is, the answer to each question can be "strongly disagree," "disagree," "neutral," "agree," and "strongly agree."

This questionnaire was filled by 10 experts (N) from the fields of IT and medicine. The IT experts were five senior employees who have worked in hospital IT departments. The medical experts were five attending physicians from different hospital departments.

In this work, Cronbach's alpha was used to test the internal homogeneity, consistency, and stability of the expert questionnaire. This method was invented by Cronbach in 1951 (Cronbach, 1951), and the alpha (α) represents the internal consistency of the scale. The higher the value of α, the more reliable the scale, and a reliable questionnaire will obtain consistent answers from different experts. This reliability coefficient is the most widely used method for evaluating consistency, and it is generally believed that an α value of 0.7 is the minimum threshold for reliability (Hair et al., 2010). Statistical Package for the Social Sciences (SPSS) was used to perform the reliability analysis. The Cronbach's α of the questionnaire is 0.837, which is above the 0.7 threshold. Hence, the questionnaire is reliable, and the questionnaire answers from the 10 experts can be used to perform the expert evaluation of the proposed doctor–patient workflow. In this way, we shall assess whether the proposed workflow has resolved the problems targeted by this study.

5.2 Results and Discussion

A statistical analysis was performed on the answers to each item in the questionnaire, as shown in Table 4. The first 10 questions, which are about the mechanism proposed in this study, generally had average scores (AVG) above 4 (except for Q9, which had an average score of 3.9). This finding shows that the experts almost always answered "agree" or "strongly agree" to the questions. The standard deviations (SD) of the questions were all less than 0.707, with Q4 having the highest variance. The results of the questionnaire are analyzed below.

In addition, to classify the AVG of low, medium and high scores, this study also used the AVG in Table 5.

Table 4 shows that Q1 and Q7 had the highest average score, at 4.8. The level of agreement in Table 5, Q1 shows that the experts strongly agree that treatment quality is affected by inconsistencies between the EMRs of different hospitals. Q2, which has an average score of 4.7, shows that the experts strongly agree that it is viable to use a cloud-based solution to provide EMRs, which are currently difficult to share between different hospitals

Table 4 Statistical analysis of the questionnaire

Seq.	Question	AVG	SD	N
Q1	Do you agree that inconsistencies between the electronic health records stored by different hospitals and clinics will affect the quality of the medical treatment provided by doctors?	4.8	0.422	10
Q2	Do you agree that a cloud-based electronic health record service will help to alleviate the difficulty of sharing electronic health records between different hospitals and clinics?	4.7	0.483	10
Q3	Do you agree that access rights to a patient's electronic health records in a cloud server must be granted by the patient?	4.0	0.667	10
Q4	Do you agree that medical personnel who have not been granted authorization should not be able to access electronic health records that are stored in a cloud server?	4.5	0.707	10
Q5	Do you agree that the proposed patient flow mechanism will ensure the security and privacy of cloud-stored electronic health records?	4.2	0.632	10
Q6	Do you agree that the proposed patient flow mechanism will allow doctors to have an optimal level of access to their patients' cloud-stored medical records?	4.4	0.516	10
Q7	Do you agree that the proposed patient flow mechanism will optimally limit the granularity of a doctor's access to cloud-stored medical records?	4.8	0.422	10
Q8	Do you agree that the use of the proposed patient flow mechanism for access control is fair for patients and doctors alike?	4.5	0.527	10
Q9	As a whole, do you agree that the proposed patient flow mechanism will effectively reduce access control costs for cloud-stored electronic health records?	3.9	0.568	10
Q10	As a whole, do you agree that the proposed patient flow mechanism will improve the quality of the treatment process?	4.0	0.667	10
Q11	Is the system easy to use?	4.7	0.483	10
Q12	Is the interface easy to understand?	4.7	0.422	10
Q13	Is the workflow smooth and intuitive?	4.9	0.316	10
Q14	Are the patient medical records provided by this system complete and comprehensive?	4.7	0.483	10
Q15	Does the system provide patient medical records in a timely manner?	4.9	0.316	10
Q16	Are the patient medical records provided by the system useful for medical personnel?	4.7	0.483	10
Q17	Do the functions of the system protect the privacy and security of the patients' personal data?	4.8	0.422	10
Q18	Do the functions of the system impose an optimal limit to the granularity of access to patient medical records by medical personnel?	4.8	0.422	10
Q19	Are the functions of the system compatible with the doctor–patient workflow?	4.6	0.516	10
Q20	Do the functions of the system provide an adequate reflection of the strengths of the doctor–patient workflow?	4.7	0.483	10

Table 5 Analysis of Likert scale

AVG	The Level of Agreement	Value	Seq.
0.00∼1.50	Strongly disagree	1	
1.51∼2.50	Disagree	2	
2.51∼3.50	Neutral	3	
3.51∼4.50	Agree	4	Q3, Q4, Q5, Q6, Q8, Q9, Q10
4.51∼5.00	Strongly Agree	5	Q1, Q2, Q4, Q7, Q11, Q12, Q13, Q14, Q15, Q16, Q17, Q18, Q19, Q20

and clinics. Q7, which asks whether the proposed patient flow mechanism will limit operations on medical records stored on the cloud to an optimal time span, obtained a relatively high level of agreement from the experts. This finding shows that the doctor–patient flow does provide the minimum required level of granularity. The average scores of Q5, Q6, and Q8 were generally higher than 4.50, which shows that the experts agree that the patient flow access control mechanism will adequately address patient privacy and security issues.

However, some experts opined that if the proposed doctor–patient workflow aims to simultaneously address issues, such as permission changes, granularity restrictions, and patient–doctor rights and benefits, it is necessary to test this system in the real world to ascertain whether unexpected problems and issues may arise. Hence, this mechanism may be further improved in the future.

Q11–Q20 in Tables 4 and 5 are questions about the system itself, and all of these questions had average scores greater than 4.51. Hence, the experts generally showed a high level of agreement in terms of the usability of the system, the usefulness of the information provided by the system, and the mechanism that was designed in this study.

6 Conclusions and Future Works

6.1 Conclusions

To allow patient EMRs to be shared between different hospitals and clinics in a comprehensive and holistic manner, we propose that a third-party cloud service provider can be used to provide EHR services. In this way, doctors can obtain the latest medical records of a patient through the Internet. However, as medical records are private personal data, it is necessary to provide a comprehensive access control mechanism for cloud-stored EMRs. To this

end, we designed an access control mechanism based on doctor appointments and called it the doctor–patient workflow. The access rights of a doctor to medical records stored in the cloud will be limited to patients who have registered with their clinic. Furthermore, the doctor can only access patient medical records according to their patient flow, and these access rights will also change according to the patients' statuses. This mechanism protects the privacy of each patient and limits the granularity of access to the cloud. Furthermore, to ensure that the cloud application can be freely accessed by its users, a web-based system was constructed based on the proposed access control mechanism. Doctors are thus able to access the EHR cloud by simply using a web browser, such as Google Chrome.

Finally, the results of this study were validated by 10 experts, who generally approved of the system. The experts generally agreed with the views of this study and also agreed that there are problems in the way EMRs are currently being handled. In addition, they showed a high level of agreement with the proposed doctor–patient workflow in all aspects, including the protection of patient privacy, the time limits to a doctor's access to patient medical records, and the fairness of the system for doctors and patients alike. These results prove that the proposed mechanism does improve on the problems that were highlighted in this study.

6.2 Limitations and Future Works

The proposed doctor–patient workflow is an access control mechanism for cloud-based EHR, and the goal of this workflow is to protect patient privacy and security in a multi-user access environment. In this study, it was assumed that this system would only be used by a doctor who is treating or delegating patients. However, medical records are not just used by doctors, as there are other users who require this information to make decisions, such as doctors on patrol or nurses administering medications. In addition, because the doctor–patient workflow is a completely new concept of access control, more work is required to improve this mechanism so that it can be used to control the access rights of all users who require access to medical records.

In this study, it was assumed that the doctors and patients will verify their identities using personal identification documents, such as patient health ID cards. The doctor will only be able to gain access to the patient's medical records after the patient's health ID card and the doctor's personal identification have been verified. After the end of a treatment, the doctor will store the records of the current treatment on the cloud system and terminate

the treatment process, thus completing the current transaction and ending the program. However, due to material limitations, we were only able to test the identity validation process via a simulated scenario. Nonetheless, because there is no absolute dependence between the validation process and the proposed doctor–patient workflow, this condition does not have any effect on the processes and results of this study. In future works, we will transfer our system to IT department of a hospital. They can complete all functions of our designed system.

References

[1] Rajabion, L., Shaltooki, A. A., Taghikhah, M., Ghasemi, A., and Badfar, A. (2019). Healthcare big data processing mechanisms: the role of cloud computing. International Journal of Information Management, 49, 271–289.

[2] Sher, M. L., Hwang, H. G., and Weng, L. J. (2019). Factors affecting physicians' intention to use electronic medical record exchange for older patients. Taiwan Gong Gong Wei Sheng Za Zhi, 38(4), 416–430.

[3] Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., and Muhammad, K. (2019). The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 10(10), 4151–4166.

[4] Dong, X. D. (2019). Cloud Computing Application to Manage Smart Grid System. Science, 4(3), 369–374.

[5] Gao, F., and Sunyaev, A. (2019). Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare. International Journal of Information Management, 48, 120–138.

[6] Shah, S. M., and Khan, R. A. Secondary use of electronic health record: Opportunities and challenges. IEEE Access, 8, 136947–136965.

[7] Yang, C. M., Lin, H. C., Chang, P., and Jian, W. S. (2006). Taiwan's perspective on electronic medical records' security and privacy protection: Lessons learned from HIPAA. Computer Methods and Programs in Biomedicine, 82(3), 277–282.

[8] Ali, O., Shrestha, A., Soar, J., and Wamba, S.F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. International Journal of Information Management, 43, 146–158.

[9] Heart, T., Ben-Assuli, O., and Shabtai, I. (2017). A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. Health Policy and Technology, 6(1), 20–25.

[10] Masud, M., and Hossain, M. S. (2018). Secure data-exchange protocol in a cloud-based collaborative health care environment. Multimedia Tools and Applications, 77(9), 11121–11135.

[11] Aceto, G., Persico, V., and Pescapé, A. (2018). The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. Journal of Network and Computer Applications, 107, 125–154.

[12] Wang, X., and Jin, Z. (2019). An Overview of Mobile Cloud Computing for Pervasive Healthcare. IEEE Access, 7, 66774–66791.

[13] Sajid, A., and Abbas, H. (2016). Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. Journal of medical systems, 40(6), 155.

[14] Gokilavani, M., Mannickathan, G. P., and Dorairangaswamy, M. A. (2018). A Survey of Cloud Environment in Medical Images Processing. Monthly Journal of Computer Science and Information Technology, 7(11), 68–73.

[15] Garets, D., and Davis, M. (2006). Electronic medical records vs. electronic health records: Yes, there is a difference. Policy white paper. Chicago, HIMSS Analytics, 1–14.

[16] Hoofnagle, C. J., van der Sloot, B., and Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65–98.

[17] Shao, S. C., Chan, Y. Y., Kao Yang, Y. H., Lin, S. J., Hung, M. J., Chien, R. N., Lai C. C. and Lai, E. C. C. (2019). The Chang Gung Research Database—a multi-institutional electronic medical records database for real-world epidemiological studies in Taiwan. Pharmacoepidemiology and Drug Safety, 28(5), 593–600.

[18] Sligo, J., Gauld, R., Roberts, V., and Villa, L. (2017). A literature review for large-scale health information system project planning, implementation and evaluation. International journal of medical informatics, 97, 86–97.

[19] Joshi, M., Joshi, K. P., and Finin, T. (2018). Delegated authorization framework for EHR services using attribute based encryption. IEEE Transactions on Services Computing, 1–12.

[20] Rauf, A., Abdullah, A. H., Iqbal, S., and Awan, K. (2019). Perception Reasoning Task-Role RBAC for Data Access Control in Cloud Computing. International Journal of Computing and Communication Networks 1(1), 1–9.
[21] Ramu, G., Reddy, B. E., Jayanthi, A., and Prasad, L. N. (2019). Fine-grained access control of EHRs in cloud using CP-ABE with user revocation. Health and Technology, 9(4), 487–496.
[22] Workflow Management Coalition. Workflow management coalition glossary & terminology, 1999. Retrieved from: http://www.aiai.ed.ac.uk/project/wfmc/ARCHIVE/DOCS/glossary/glossary.html.
[23] Ahmad, Z., Nazir, B., and Umer, A. (2021). A fault-tolerant workflow management system with Quality-of-Service-aware scheduling for scientific workflows in cloud computing. International Journal of Communication Systems, 34(1), e4649.

Biographies

Tsung-Yin Ou now is an Associate Professor in Department of Marketing and Distribution Management at National Kaohsiung University of Science and Technology. He received Ph.D. degrees in Industrial Engineering and Engineering Management from National Tsing Hua University, Taiwan. His currently research interests include Data Mining, Smart Retailing, Application of Artificial Intelligence and Operation Management on Service Industry.

Wen-Lung Tsai was born in New Taipei, Taiwan in 1974. He received his M.S. degree in information management from the Chinese Culture University, Taipei, in 2007 and Ph.D. in information management from National Central University, Taoyuan in 2015. From 2012 to 2015, he was an Engineer and Project Manager with the Institute of Information Industry. Since 2016, he has been an Associate Professor with the Department of Information Management at Asia Eastern University of Science and Technology (AEUST). He is the author of more than 40 articles and more than 10 industry research plans. His current research and teaching interests include project management, software engineering, information systems, data quality, and digital content. He has been serving as a reviewer for many highly respected journals.