IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 1, 2017, accepted January 21, 2018, date of publication February 5, 2018, date of current version March 13, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2800288

Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System

KWANGSOO SEOL[1], YOUNG-GAB KIM[2], EUIJONG LEE[1], YOUNG-DUK SEO[1], AND DOO-KWON BAIK[1]

[1]Deptatment of Informatics, Korea University, Seoul 02841, South Korea
[2]Department of Computer and Information Security, Sejong University, Seoul 35006, South Korea

Corresponding authors: Young-Gab Kim (alwaysgabi@sejong.ac.kr) and Doo-Kwon Baik (baikdk@korea.ac.kr)

This work was supported by the Institute for Information and Communications Technology Promotion through the Korean Government (MSIT), Development of Interoperability and Management Technology of IoT System with Heterogeneous ID Mechanism, under Grant 2017-0-00756.

ABSTRACT Cloud-based electronic health record (EHR) systems enable medical documents to be exchanged between medical institutions; this is expected to contribute to improvements in various medical services in the future. However, as the system architecture becomes more complicated, cloud-based EHR systems may introduce additional security threats when compared with the existing singular systems. Thus, patients may experience exposure of private data that they do not wish to disclose. In order to protect the privacy of patients, many approaches have been proposed to provide access control to patient documents when providing health services. However, most current systems do not support fine-grained access control or take into account additional security factors such as encryption and digital signatures. In this paper, we propose a cloud-based EHR model that performs attribute-based access control using extensible access control markup language. Our EHR model, focused on security, performs partial encryption and uses electronic signatures when a patient's document is sent to a document requester. We use XML encryption and XML digital signature technology. Our proposed model works efficiently by sending only the necessary information to the requesters who are authorized to treat the patient in question.

INDEX TERMS Access control, data privacy, encryption, digital signature.

I. INTRODUCTION

Recently, the development of information technology has made great strides in the field of medical information. In order to manage large amounts of medical data transparently and cost-effectively, the need for computerized medical data has increased, and paper-based recording methods are gradually being replaced by digitized medical information systems [1]. EHRs are electronically stored digital forms containing all of a patient's medical information [2]. EHRs follow international standards to ensure interoperability so that patient data is not created and managed by a single health care organization, but by multiple medical institution systems that allow sharing between various health care providers and organizations [3] (e.g., hospitals, laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and universities). The adaption of EHR can play an important role in improving patient safety and health care quality [4]–[6].

The existing EHR system was constructed in a centralized database environment and medical information was stored and managed in the context of hospital systems. However, this approach incurs high costs due to the initial construction of the system, maintenance, background knowledge, lack of skilled system engineers, and issues with patient medical information being incompatible with the systems in other hospitals. One potential solution for the problems described above has begun attracting significant attention [7]. That solution is an EHR system based on the cloud environment. Cloud computing is managed by a cloud provider, which has advantages in terms of cost and system expansion when compared to existing systems [8]. Patient data can also be shared and managed by various healthcare providers.

However, an EHR system in the cloud environment comes with additional security issues compared to a single-system environment because patient data exchange occurs between the cloud platform and various healthcare institutions [9]. Patient personal information may cause security and privacy problems because it contains sensitive and confidential data about the patient (e.g., health status information, provision of health care, payment for health care, identification of the patient) [10]. This information must be handled with care because its exposure would constitute a severe breach of the privacy of the individual. The EHR system must be designed to guarantee security and privacy when sharing personal patient information [11].

Access control is very important for protecting patient privacy when providing health services. Access control means only transmitting patient documents to authorized doctors. However, most recent access control systems for health services are inflexible due to using role-based access control (RBAC) schemes [12]. Furthermore, additional security issues may arise due to a lack of consideration for various security factors. Therefore, in order to design a secure and flexible access control system to protect patient privacy, we propose an attribute-based access control model using extensible access control markup language (XACML) [13].

The main contributions of this paper are as follows. 1) The attribute-based access control used in the proposed model can provide flexible and fine-grained access control when compared to existing RBAC schemes. 2) By performing partial encryption of patient privacy-related elements in patient documents via extensible markup language (XML) encryption [14], the risk of additional privacy exposure for the patient when an authorized user views the patient documents can be prevented. 3) The digital signature process can prove that a document has not been falsified or altered, and can prevent non-repudiation of the document. Additionally, the proposed model conforms to the technical safeguards of the American standard health insurance portability and accountability act (HIPAA) [15].

The remainder of this paper is organized as follows. Section 2 discusses the related standards and access control studies for EHR system development. Section 3 introduces a two-phase model for developing a privacy-preserving EHR system. Section 4 describes the prototype implementation of the proposed model based on actual medical data. Section 5 shows the results of the comparison between the existing studies and the proposed model in terms of security aspect. Section 6 provide conclusions and future work.

II. RELATED WORK

A. STANDARDS FOR EHR SYSTEMS

There are currently several standards in development for specifying EHRs, such as HIPAA, OpenEHR [16], the health level 7 (HL7) clinical document architecture (CDA) [17], [18], and continuity of care document(CCD) [19]. HIPAA provides security measures and privacy protection mechanisms to protect health information. HIPAA has defined personal identifiable information (e.g., social security number, medical ID number, credit card number, driver's license number, home address, telephone number, medical records, and other important information) as protected health information (PHI). HIPAA was created to protect the individual's PHI. In 2009, HIPAA was upgraded into health information technology for economic and clinical health (HITECH) [20]. HITECH provides additional compliance standards for companies involved in healthcare. The technical safeguard portion of HIPAA specifies what requirements must be met in the design of access control, transmission security, etc. when developing medical systems.

The HL7 CDA is a markup standard that defines the structure and semantics of CDA clinical documents for sharing purposes. Clinical documentation is a record of medical observations and services, and CDA records may include text, images, sounds, and other multimedia content. The CDA is encoded in XML, and an execution system that exchanges CDA documents must meet all legal requirements for authentication, confidentiality, and retention of records. Since the CDA was approved as an American national standards institute (ANSI) standard in 2005, the HL7 committee has focused on creating reusable templates and constraints for commonly used clinical documentation. For interoperability of medical data, American society for testing and materials (ASTM) established continuity of care record (CCR) [21] and HL7 association established CCD standard by combining HL7 CDA and CCR. These standards express personal health information based on the XML language.

OpenEHR is designed to enable interoperability of health information between EHR systems (or within an EHR system). OpenEHR is a stable model that has been used for over 15 years and is freely available to anyone, anytime, anywhere with an open license. Unlike the traditional EHR development model, because the technical reference model is completely separated from clinical knowledge using a two-level information model, the technical portion can be designed by engineers, and the clinical knowledge portion can be designed by clinicians.

B. PRIVACY-PRESERVING APPROACHES FOR EHR SYSTEMS

Several survey papers have reviewed privacy-preserving schemes for EHR systems [12], [22]–[27]. Abbas and Khan [12] described the requirements that should be considered for privacy in an E-health cloud. To preserve health data privacy in a cloud environment, they described how the e-Health system should consider the following requirements: integrity, confidentiality, authenticity, accountability, audit, non-repudiation, anonymity, and unlinkability. They also assessed how well studies on privacy preservation in EHR systems consider these factors. They classify privacy-preserving approaches in e-Health Clouds as cryptographic approaches and non-cryptographic approaches. The cryptographic approaches use encryption schemes such as public key encryption (PKE), symmetric key encryption (SKE), and attribute-based encryption (ABE) to protect health data in e-Health Cloud environments. Studies classified as non-cryptographic approaches mainly use techniques such as policy-based access control. Pussewalage and Oleshchuk [22] classify technologies for privacy preservation into cryptographic mechanism approaches (e.g., PKE, SKE, and ABE), access control approaches (e.g., RBAC, ABAC), and biometric approaches. They classify the security and privacy requirement elements for e-health as a patient's understanding, a patient's control, confidentiality, data integrity, consent exception, non-reputation, and auditing. Then, they assess whether papers proposing privacy-preserving schemes reflect these factors. Fernández-Alemán *et al.* [23] selected the top papers in the field and analyzed the latest research trends. Their results show that more than half the EHR systems using access control use RBAC, and that 22% use a public key infrastructure (PKI)-based digital signature mechanism.

There have been several access control studies on EHR systems with the goal of protecting the privacy of patients [28], [29], [31]–[47]. Bahga and Madisetti [28] adopted a two-level modeling approach for achieving semantic interoperability. It supports security features and addresses the key requirements of HIPAA and HITECH. Hsieh and Chen [29] proposed a design for a secure interoperable cloud-based EHR service. It applies a broad spectrum of security mechanisms including XACML access control, XML encryption, and XML digital signatures [30]. Rezaeibagha and Mu [31] proposed a secure EHR system architecture for secure data sharing. Their study divided the EHR system domain into direct and indirect access, and protected patient privacy using RBAC. Premarathne *et al.* [32] presented a cryptographic RBAC model for EHR systems. For user authentication, location and biometric authentication techniques were introduced, and steganography was applied to electrocardiogram (ECG) signal data. Peleg *et al.* [33] highlighted the problems with the RBAC model used in existing EHR system and proposed a situation-based access control model (SitBAC). SitBAC is designed to use patient data access request scenarios as the basis for patient privacy. Gjanayake *et al.* [34] considered flexible access control techniques for protecting patient privacy. Their proposed access control model consists of four modules: RBAC, MAC, DAC, and PBAC. They also developed a web-based prototype. Lunardelli *et al.* [35] proposed an analytic hierarchy process (AHP) model for solving policy conflict issues in EHR systems. They created a prototype and analyzed the system performance was using XACML Access control. Calvillo-Arbizu *et al.* [36] addressed the issue of most current clinical and EHR systems using access control measures to support requirements within only a single organization. They proposed an access control mechanism based on XACML attribute-based access control (ABAC), which conforms to ISO 13606, which supports multi-domain sharing. The proposed system applies an ontology for automatic reasoning to a decision-making process. Yang *et al.* [39] proposed a cryptographic approach for video data sharing in a cloud-based multimedia system environment. they propose a time-domain ABE scheme that includes time in ciphertext and key so that only users with sufficient attributes in a particular time slot can decrypt the video content. Li *et al.* [44] proposed a patient-centric framework and demonstrated mechanisms for performing access control in a semi-trusted server environment. To perform fine-grained and scalable access control, they used ABE technology to encrypt patient data. They applied their mechanisms and reduced the complexity of key management in scenarios where multiple data owners and patients were distributed across various security domains. Abomhara *et al.* [46] proposed a work-based access control model that modifies the user-role assignment model through the concept of team role. They modeled and verified the policies using model checking techniques called access control policy testing (ACPT) and showed their proposed model is flexible and easy to manage. Sicuranza and Esposito [47] showed a new approach combining several access control models. They considered the requirements of patients, healthcare organizations, international norms and directives for model design and showed an algorithm for access control management. However, most of these studies do not consider security factors, such as confidentiality or integrity, in their designs, or use inflexible access control techniques, such as RBAC.

III. THE PROPOSED EHR SYSTEM MODEL FOR PROTECTING PATIENT PRIVACY

In the proposed EHR model, ABAC using XACML and XML security for encryption and digital signatures is used to protect patient privacy. This can protect patients from the risk of privacy infringement by providing only the required content from the requested patient medical documents to authorized users.

A. FRAMEWORK

We propose a new methodology for the development of an EHR system that protects the privacy of patients in a cloud environment. An overview of the proposed model is presented in Fig. 1. The proposed model works in two main phases. The purpose of the proposed model is to provide medical documentation only to authorized users, without infringing on the patient's privacy. First, access control based on XACML language is performed. It evaluates whether the user is authorized to receive the medical document. After access control is performed, if the user is allowed to access the documents for the patient, Phase 2 is performed to protect the patient's privacy. In Phase 2, partial encryption and digital signatures are used to transmit the privacy-protected documents to the requesting user.

B. ABAC USING XACML (PHASE 1)

In Phase 1 of the proposed model, ABAC using XACML is performed. This phase is comprised of three main components: the policy enforcement point (PEP), the policy decision point (PDP), and the policy administration point (PAP). By performing access control, the system can determine if a request should be permitted or denied. The PEP is responsible for receiving user requirements and enforcing decisions based

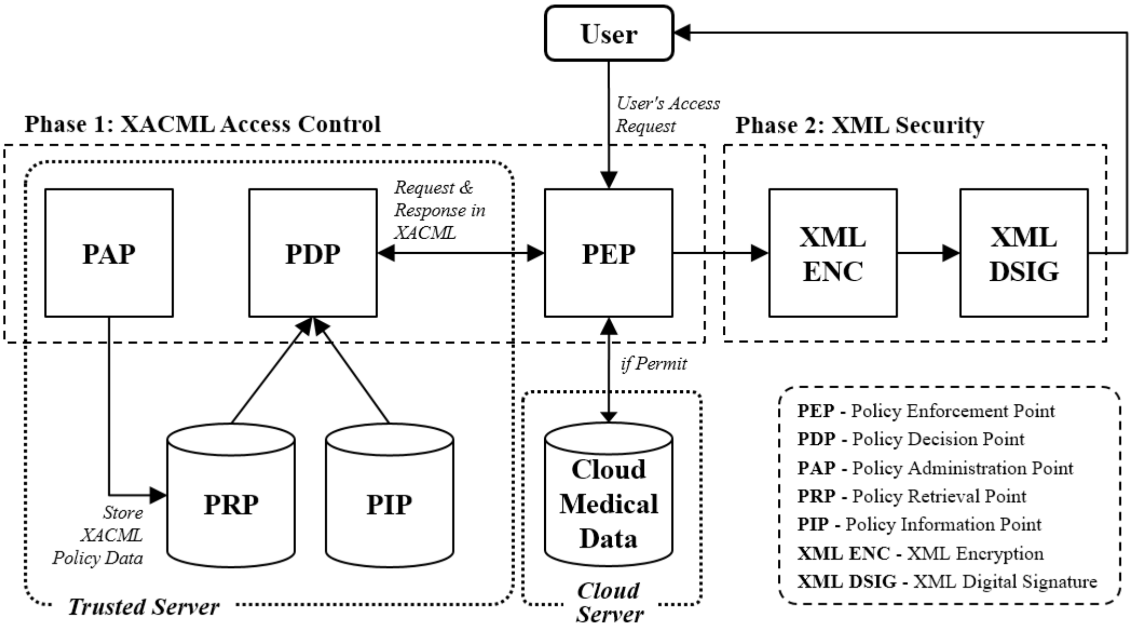

User
User's Access Request
Phase 1: XACML Access Control
Phase 2: XML Security
PAP
PDP
Request & Response in XACML
PEP
XML ENC
XML DSIG
if Permit
PRP
PIP
Store XACML Policy Data
Cloud Medical Data
Trusted Server
Cloud Server
PEP - Policy Enforcement Point
PDP - Policy Decision Point
PAP - Policy Administration Point
PRP - Policy Retrieval Point
PIP - Policy Information Point
XML ENC - XML Encryption
XML DSIG - XML Digital Signature

FIGURE 1. Framework for our proposed model.

on processed results. When a user sends an access request through the PEP, the PEP generates a request message in the form of XACML based on the user requirements and passes it to the PDP. The PDP retrieves the XACML request, searches for and analyzes related policies, makes a final authorization decision, and generates an XACML response message. The generated response message is delivered back to the PEP, which enforces the received decision. The PDP refers to information from the policy information point (PIP) and policy retrieval point (PRP) to evaluate user requests. The PIP stores the additional attributes required to evaluate the policy (e.g., user role, clearance, and document classification). The PRP stores XACML policy data for evaluation by the PDP. XACML policies are managed at the PAP. System administrators can perform actions such as creating, modifying, deleting, and searching policies through the PAP user interface. The design of all components associated with the decision making (via the PDP) should be located on a trusted server.

The policy structure of XACML consists of a policy set and a policy rule. Each policy can only match one Target. The Target is used to determine whether the policy is associated with the request statement. The target can be specified using the three following attribute categories: subject, resource, action. If the specified attribute category matches the attribute category of the request statement, the corresponding policy is considered to be associated with that request statement. For example, if the policy is for a document in the medical category, we can specify the target of the policy as follows:

(Policy 1) Any subject can take any action on a document
in the medical category. (1)

A policy can specify multiple rules. Rules consist of a Target, one or more Conditions, and an Effect. The target element used in the rule is used to evaluate whether or not the corresponding rule is related to the request as the target of the policy. It is used to evaluate if the rule is related to the request. If no target is specified, the rule is evaluated for all requests. Conditions specify authorization logic statements that contain Boolean expression values. The rule is used to determine if the condition is true or false (or Indeterminate). The effect value is an element that determines what value the rule will return when the Condition is true. For example, you can specify the following example rules for the Policy example above.

(Rule1) Subjects with the role of general practitioner can
read / print documents of their patient's medical category.
(Rule2) Subjects with the role of an emergency doctor can
read / print the medical category documents of their
patients in emergency situations. (2)

If the condition is true and the effect value is permit, then the return value is permit. An Obligation is an optional element that allows XACML to enable more fine-grained access control. Obligations specify the actions that the PEP should enforce while enforcing authorization decisions.

In XACML, each policy set has multiple policies, and each policy has multiple rules. A conflict can occur when different results are generated from each associated policy or rule. This problem can be solved by using a policy- or rule-combination algorithm. In the event of a conflict, the combination algorithm is used to rank the results of each policy or rule and derive the result. Table 1 presents the standard combination algorithms supported by XACML 3.0.

TABLE 1. The standard combination algorithms supported by XACML 3.0.

Algorithm	Definition	Coverage
permit-overrides	If there is any rule whose result is Permit, the final authorization decision is Permit.	R/P
deny-overrides	If any rule with a result of Deny exists, the final authorization decision is Deny.	R/P
first-applicable	The first result is the end result.	R/P
only-one-applicable	Evaluates the policy only if there is exactly one applicable policy and returns Indeterminate if more than one applicable policy exists.	P
ordered-permit-overrides	The same as permit-overrides, except that the order in which relevant rules are evaluated is the same as the order in which they are added to the policy.	R/P
ordered-deny-overrides	The same as deny-overrides, except that the order in which relevant rules are evaluated is the same as the order in which they are added to the policy.	R/P

* P and R denotes policy and rule respectively.

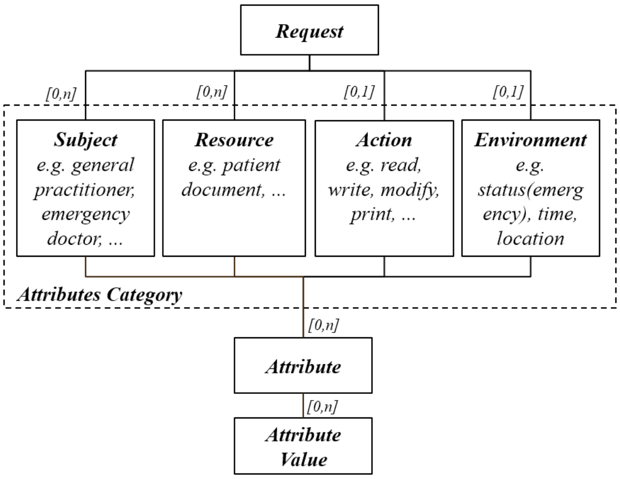
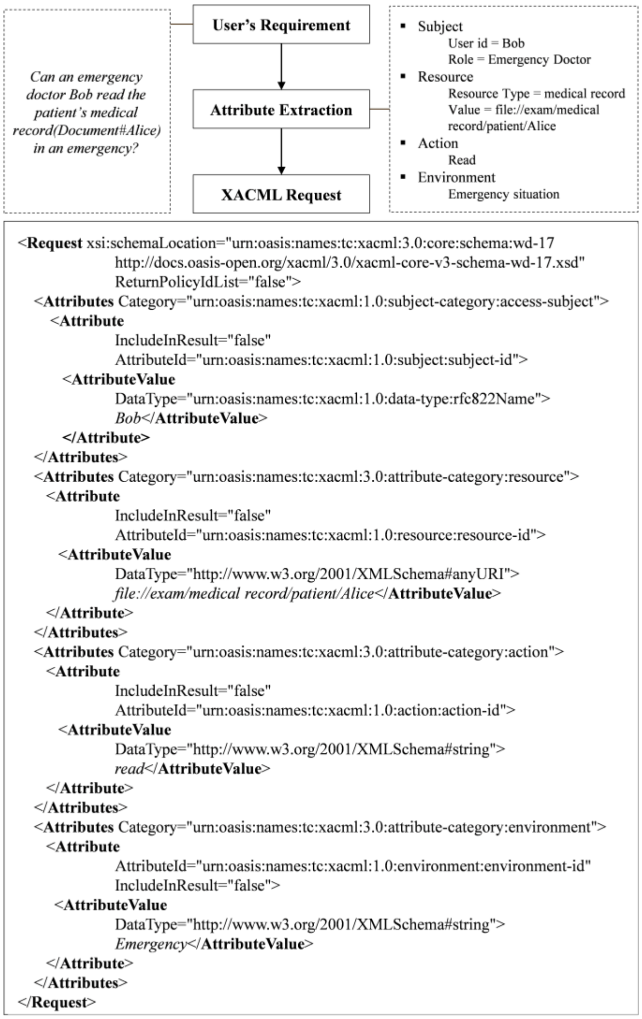

Request
[0,n]
[0,n]
[0,1]
[0,1]
Subject
e.g. general practitioner, emergency doctor, ...
Resource
e.g. patient document, ...
Action
e.g. read, write, modify, print, ...
Environment
e.g. status(emergency), time, location
Attributes Category
[0,n]
Attribute
[0,n]
Attribute Value

FIGURE 2. Structure of an XACML request.

In order to specify context, a request message in XACML uses a structure specifying attribute categories, attribute values, and metadata. Fig. 2 presents the structure of an XACML request. As depicted in the figure, one request message consists of several attributes, and attributes are comprised of four categories: subject, resource, action, and environment. The request message asks the PDP the following question: For a given subject, is it allowed to perform the specified action on the specified resource in the specified environment? If the request message satisfies the policy condition, it returns the Effect value.

Fig. 3 illustrates the process of generating an XACML request message based on user requirements. This process is performed in the PEP and the generated XACML request is sent to the PDP to evaluate whether or not it is authorized. In this example, as a requirement of the user, the emergency doctor, Bob, sends a request to read the medical documents of the patient, Alice, during an emergency. When such a requirement is created, an attribute extraction process is performed to extract and match the attributes from the requirement.


Can an emergency doctor Bob read the patient's medical record(Document#Alice) in an emergency?
User's Requirement
Attribute Extraction
XACML Request
▪ Subject
User id = Bob
Role = Emergency Doctor
▪ Resource
Resource Type = medical record
Value = file://exam/medical record/patient/Alice
▪ Action
Read
▪ Environment
Emergency situation

```
<Request xsi:schemaLocation="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17
                http://docs.oasis-open.org/xacml/3.0/xacml-core-v3-schema-wd-17.xsd"
                ReturnPolicyIdList="false">
  <Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
    <Attribute
                IncludeInResult="false"
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
      <AttributeValue
                DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">
                Bob</AttributeValue>
      </Attribute>
  </Attributes>
  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
    <Attribute
                IncludeInResult="false"
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
     <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                file://exam/medical record/patient/Alice</AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
    <Attribute
                IncludeInResult="false"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
     <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">
                read</AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
    <Attribute
                AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"
                IncludeInResult="false">
     <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">
                Emergency</AttributeValue>
    </Attribute>
  </Attributes>
</Request>
```

FIGURE 3. An example of the process of generating an XACML request message in a scenario where the emergency doctor Bob accesses patient Alice's data in an emergency.

First, the actor, Bob (more specifically Bob's id), wants to access the documents matching the Subject. The document that Bob wants to access is matched using the resource

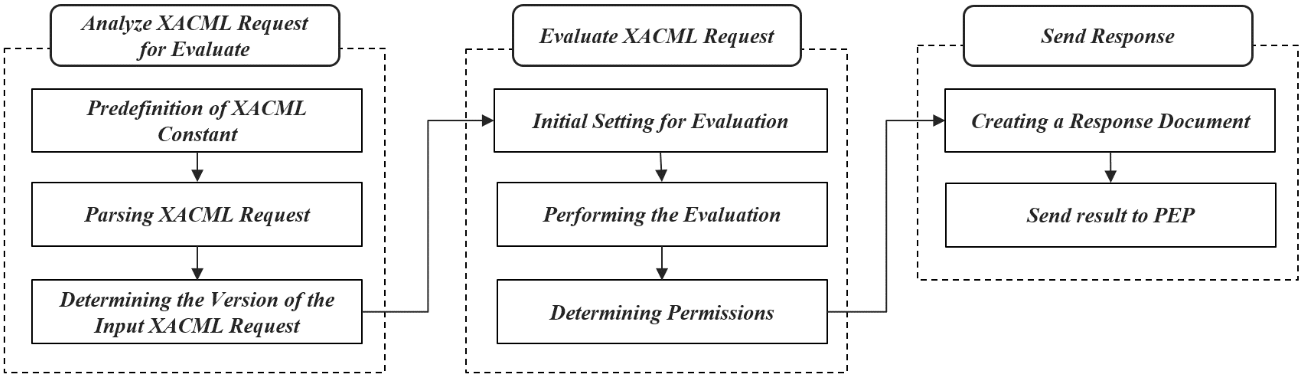

Analyze XACML Request for Evaluate
Predefinition of XACML Constant
Parsing XACML Request
Determining the Version of the Input XACML Request
Evaluate XACML Request
Initial Setting for Evaluation
Performing the Evaluation
Determining Permissions
Send Response
Creating a Response Document
Send result to PEP

FIGURE 4. The process of analyzing the request message and performing the evaluation process by the PDP to determine whether the user is a user who can access the patient's document.

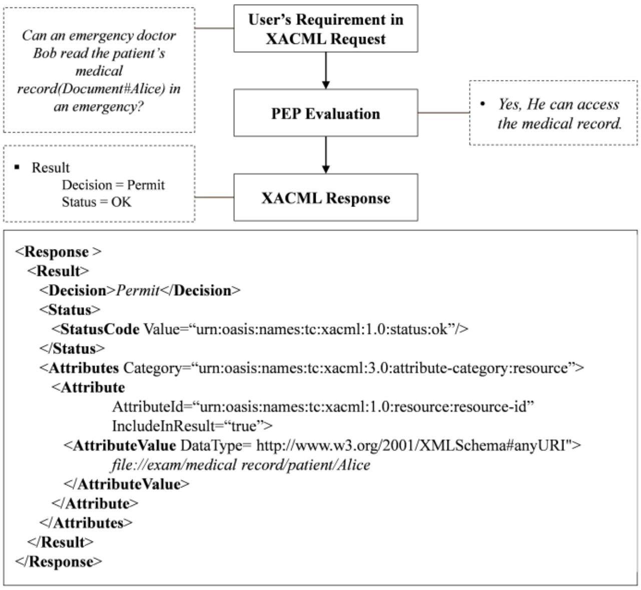
information. The resource type is a medical record, and the value is the path to the document. Actors can perform various actions on the document, such as read, write, and print. In this example, only read is allowed, so the read attribute is matched to the Action attribute. Finally, the Environment matches the emergency situation. At the end of the attribute extraction process, an XACML request message will be generated following the addition of a request header and attribute metadata information input.

The XACML request message generated by the PEP is passed to the PDP and evaluated for approval. Fig. 4 is a flow chart illustrating the process of receiving a request message from the PEP and performing evaluation. This process can be divided into three stages. The first stage is the process of determining compatibility settings and performing preprocessing prior to evaluating the request statement. For example, the process of defining XACML run constants is included this step. This allows the PDP to comprehend the meaning of the specified data values when analyzing the content of a request message. This process is performed before the request message is accepted, and is necessary for determining if the received request message is valid. When the validity of the request message is verified, the PDP parses the request statement to extract the desired information. Because syntax is slightly different depending on the version of XACML, one should check for compatibility via version checking and use an appropriate evaluation method based on the version.

In the second stage, evaluation is performed based on the parsed XACML request message data. The initial settings for evaluation are determined during system design. When the policy corresponding to the request is found, the final approval result is determined based on a calculation of the rule values for the relevant rules. Rule value estimation is performed as shown in Table 2. The PDP returns permit or deny values if the requested access is granted or rejected, respectively, and returns Indeterminate if the PDP cannot evaluate the request due to an error (e.g., missing attributes, network errors while retrieving policies, policy evaluation, syntax errors, etc.). If the PDP does not have a policy that applies to the request, it returns Not Applicable.

TABLE 2. Rule evaluation in XACML.

Target	Condition	Rule value
Match	True	Effect
Match	False	Not Applicable
Match	Indeterminate	Indeterminate
No-Match	Do not care	Not Applicable
Indeterminate	Do not care	Indeterminate


Can an emergency doctor Bob read the patient's medical record(Document#Alice) in an emergency?
User's Requirement in XACML Request
PEP Evaluation
• Yes, He can access the medical record.
▪ Result
Decision = Permit
Status = OK
XACML Response

```
<Response >
  <Result>
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
    <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
      <Attribute
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                IncludeInResult="true">
        <AttributeValue DataType= http://www.w3.org/2001/XMLSchema#anyURI">
                file://exam/medical record/patient/Alice
        </AttributeValue>
      </Attribute>
    </Attributes>
  </Result>
</Response>
```

FIGURE 5. An example of the process of generating an XACML response message after evaluation in the scenario of Fig. 3.

The final stage is to create a response Message based on the results of the evaluation stage and deliver it to the PEP. Fig. 5 presents the process of creating a response message after the PDP has finished evaluating the example scenario from Fig. 4. The response message is relatively simple compared to the request message. In a response message, decision results and a status can be specified. In this example, only a single approval result is displayed because it is a process for a single request statement. However, when a multi request

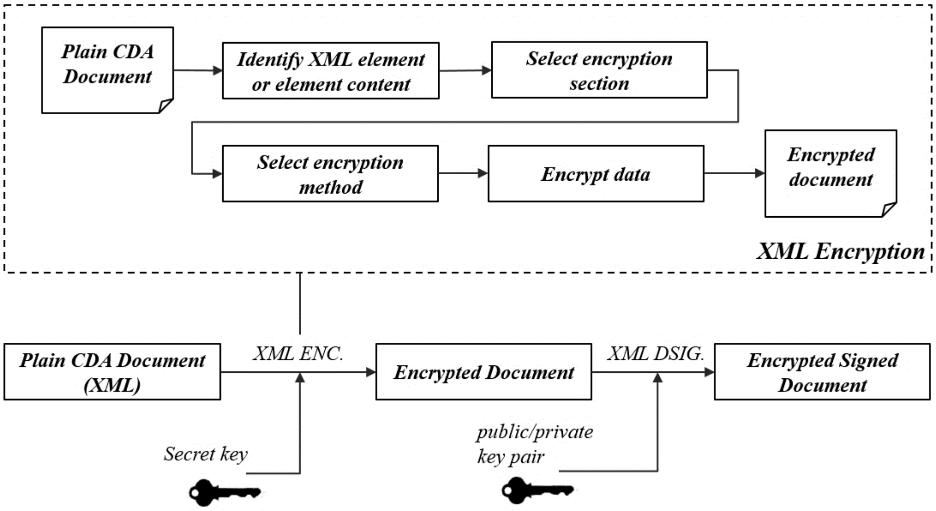


FIGURE 6. The process of encrypting medical documents using XML encryption in phase 2 of the proposed model.

is received, an approval result should be provided for each request.

C. XML SECURITY FOR MEDICAL DOCUMENT SECURITY (PHASE 2)

In the Access Control phase of the proposal model, when a user is authorized for a document, that document is then delivered to the user. The delivered document is vulnerable to security threats because it is a CDA/CCD original, which is not encrypted or signed. Therefore, even though the access control step has been performed, the patient still has the risk of their sensitive information being exposed. In order solve this problem, our proposed model uses XML security during Phase 2. During this process, partial encryption is performed using XML encryption and a digital signature is added using XML digital Signature. With XML encryption, partial encryption can be performed instead of total encryption, meaning it exposes only the necessary information to the user.

First, for the security of patient medical documents, we use XML encryption to perform partial encryption of contents that may infringe upon patient privacy with respect to the original CDA/CCD text following the access control process. XML encryption follows the process presented in Fig. 6.

First, the elements and element content of the CDA/CCD XML document are identified by parsing prior to encryption. We then classify the factors that may infringe upon patient privacy and select a portion of the document for encryption. If elements that may infringe upon an individual's privacy are selected, then encryption is performed on those elements. In the HIPAA standard, any information in medical records that is used to identify individuals is defined as PHI (e.g., medical records, billing information, health insurance information, and insurance information). PHI is created, used, and exposed during the provision of healthcare services and may be exploited to violate the privacy of individuals. Table 3 lists the 18 types of identifiers defined by HIPAA. Some of the data listed is closely related to data that may violate the patient's privacy. Additionally, there may be sensitive information that the patient does not wish to disclose. This information should also be partially encrypted and retrieved only with patient consent, if necessary. Once the encryption elements are selected, an encryption algorithm is selected and partial encryption is performed using the administrator's private key.

TABLE 3. Patient sensitive information for partial encryption.

Information that identifies an individual as defined by HIPAA (Safe Harbor). §164.514(b)(2)	Sensitive information that an individual does not want exposed.
Names, geographic data, all elements of dates, telephone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, including license plates, and device identifiers and serial numbers, web URLs, internet protocol addresses, biometric identifiers (e.g., retinal scan, fingerprints), full face photos and comparable images, any unique identifying number, characteristic, or code.	*Sexual diseases, psychosis, marital status, ethnicity, etc.*

When the XML partial encryption is completed, the XML digital signature is applied. An electronic signature proves that the person described as the author actually created the electronic document. It also proves that the contents were not falsified or altered during the sending and receiving process; this prevents the author from later denying the fact that the electronic document was created. The use of an XML digital signature is illustrated in Fig. 7.

The first step is to determine the type of digital signature to be used. There are three types of XML digital

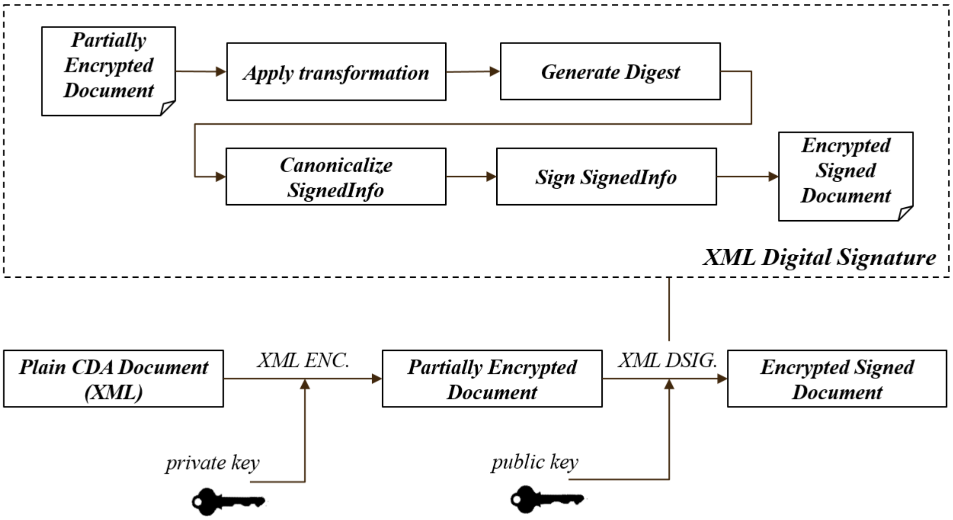


FIGURE 7. The process for performing an XML digital signature on a partially encrypted medical document in Fig. 6.

signatures: an enveloping signature, enveloped signature, and detached signature. For an enveloping signature, the subject data exists within the signature structure. This is advantageous for adding a digital signature to the packaged data in an XML payload. For an enveloped signature, the target data contains the signature structure. This can be used to digitally sign all or part of an XML document. A detached signature exists outside the data and does not have a signature structure. This is used to digitally sign data that exists at a location specified by a URI address. The second step is to create a digest. The data to be signed is given a new value of reduced size by using a hashing algorithm. This process is called creating a digest. The hash algorithm should be designed to produce the same digest for the same data and to generate a completely different digest value when a slight modification is made to the data. This prevents someone from performing reverse engineering on the data.

As a third step, XML canonicalization is performed. Within a serialized XML document, information can be represented in a variety of forms. The following example shows XML representations that have different octal string representations, but have the same meaning:

$$
\begin{aligned}
&< \text{name a} = \text{“1”b} = \text{“2”c} = \text{“3”}/ > \\
&< \text{name c} = \text{‘3’b} = \text{‘2’a} = \text{‘1’} >< /\text{name} > \qquad (3)
\end{aligned}
$$

In this case, the two statements are logically equivalent in an XML document, but do not guarantee equivalent hash values. Normalization is essential for logically identical XML documents to be transformed into a single piece of physical data. To make an XML document physically the same document, the W3C recommends an XML canonicalization algorithm, which can ensure interoperability with XML documents written in different structures. Although the initial 1.x version of the XML digital signature did not fully care for the canonicalization of issues such as whitespace or XML namespace notation, XML digital signature 2.0 follows canonicalization 2.0 to solve many of the problems in existing versions and improve robustness.

The final step is to calculate the signature value. In this process, the digest value is encrypted using the author's private key. The user later decrypts the signature value using the author's public key and compares it to the digest value to ensure that the signature is valid. If the two values are not the same, it means that the document is different from the one signed by the author. However, even if the values are different, it is not possible to know what caused the difference.

IV. IMPLEMENTATION

In this section, we discuss the implementation of the EHR prototype for evaluation of the proposed model. The implemented system is designed to demonstrate the applicability of the proposed model using actual medical data. We also analyze the flow of data by applying the proposed XACML access control and XML security process to this prototype.

A. DEVELOPMENT ENVIRONMENT

The system is implemented in the Java web server (JDK8) environment [48]. Balana (version 1.0.0) was used for the implementation of XACML access control [49]. It is managed by WSO2 and builds upon the Sun XACML 2.0 implementation. It is open source and licensed under an Apache license. We leveraged the source code of the XML security library (version 1.2.24) in order to implement XML encryption and digital signatures. The library is licensed by Aleksey Sanin (MIT License) [50]. We also used cryptographic libraries, including the libxml library for XML parsing [51] and OpenSSL for encryption [52].

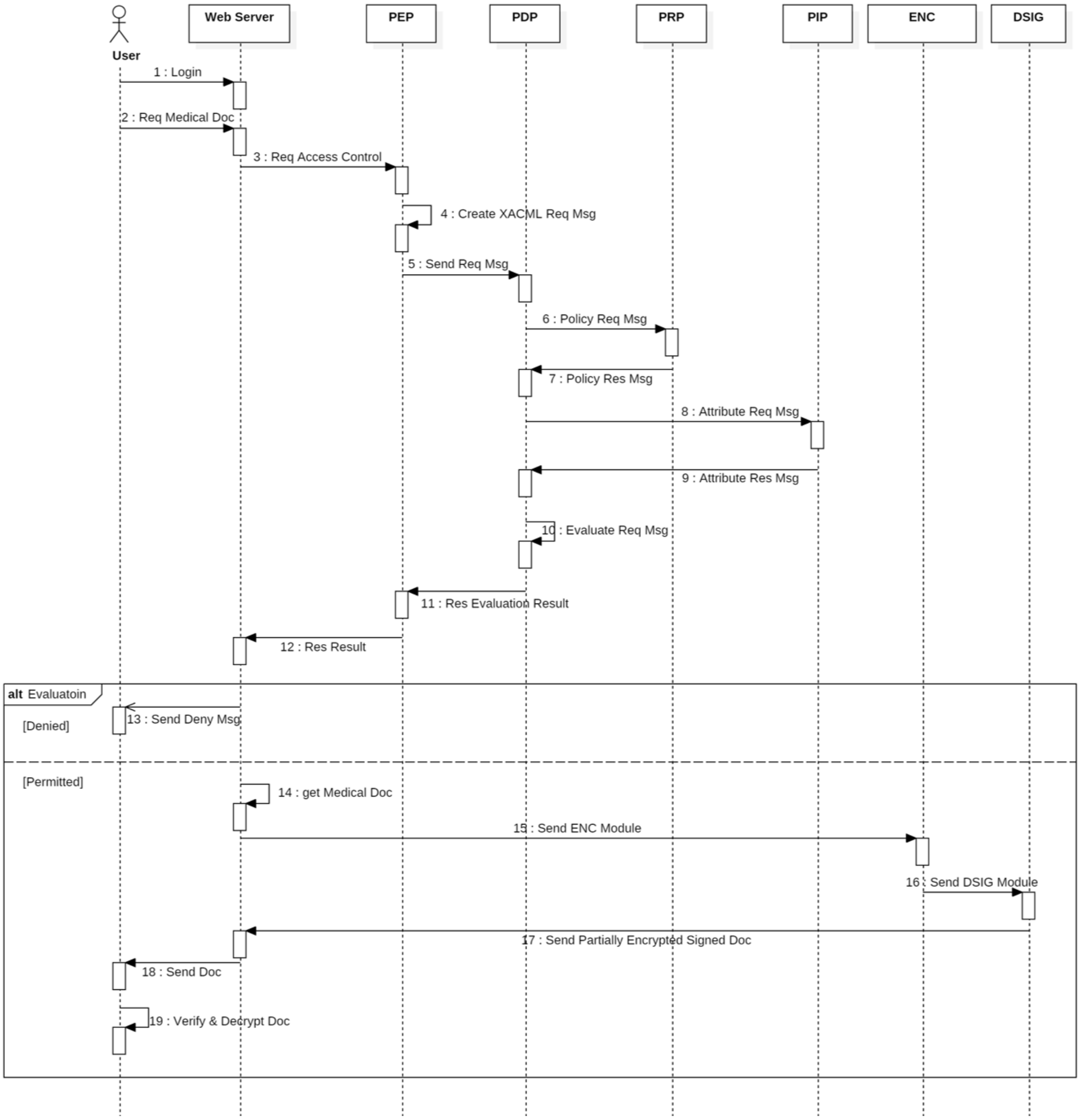


FIGURE 8. **The UML Sequence Diagram of the Implementation System.**

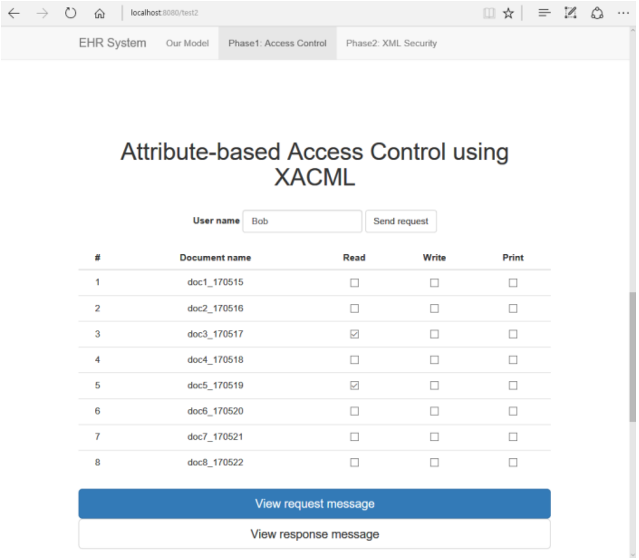
B. MEDICAL DATA (MIMIC III)

We used sample data created by referring to the schema and values of the medical information mart for intensive care III (MIMIC-III) in order to replicate the data format used in hospitals for our implementation [53]. MIMIC-III is a free critical care database. MIMIC-III includes health-related data for more than 40,000 patients who stayed in the intensive care unit between 2001 and 2012 at the Beth Israel Deaconess Medical Center. The database includes demographics information, patient vital sign measurements, laboratory test results, procedures, medications, caregiver notes, imaging reports, and mortality information.

C. SYSTEM DESIGN

Because the real EHR system is very large, there is a limit to the implementation of the system in this study. Thus, we limit the input of user requirements in order to simplify implementation complexity. For example, a user may select only a limited set of documents or actions. This also simplifies the task of complex policy design. The key management required for encryption and signing also uses a local key store in order to reduce implementation complexity. Fig. 8 presents the UML sequence diagram of the implemented system.

First, the user must log in to the server to confirm their identity. The HIPAA standard specifies unique user identification as a requirement when performing access control. The user then requests a medical document from the web server. Fig. 9 presents the user request portion of the implemented system. When a user selects the desired document and action, and sends an access control request through the web server, the PEP generates a corresponding XACML request



Attribute-based Access Control using XACML

User name: Bob

#	Document name	Read	Write	Print
1	doc1_170515	☐	☐	☐
2	doc2_170516	☐	☐	☐
3	doc3_170517	☑	☐	☐
4	doc4_170518	☐	☐	☐
5	doc5_170519	☑	☐	☐
6	doc6_170520	☐	☐	☐
7	doc7_170521	☐	☐	☐
8	doc8_170522	☐	☐	☐

FIGURE 9. Screenshot of Prototype Application showing access control part.

TABLE 4. Elements to be considered for partial encryption.

Elements to Consider Encryption	Related Elements
Patient's Personal Information	-Date of Birth(DOB). Date of Death(DOD) -Insurance -Language -Religion -Marital Status -Ethnicity
Disease-Related Information	-Disease Name -Drug Information
Hospital Use Information	- Hospital Admission/Discharge Date

message. The request message is sent to the PDP, which evaluates the user request using the stored policy.

If the evaluation returns denied, the Web server sends a message to the user that their request is denied and the process is terminated. If the evaluation returns permit, the web server fetches the requested medical information. If there are multiple requested documents, the XML security process is performed only for documents that are permitted. The model proposed in this paper uses a cloud repository to fetch medical data, but the implemented system is designed to fetch medical information from a local store in order to reduce complexity.

In the Select Encryption Section of the XML encryption process, data elements that can infringe upon the privacy of a patient are classified. Table 4 lists the sections that should be considered for partial encryption in the MIMIC-III data schema. These include patient personal information, disease related information, and hospital use information.

After the partial encryption zone is determined, XML encryption is performed on the corresponding sections. Finally, a digital signature is added to ensure the validity of the document. Fig. 10 presents the process of encrypting and signing medical documents in the implemented system. The digital signature and encrypted document are then validated and decrypted by the user.

V. DISCUSSION

We proposed an EHR system model that operates in a cloud-based environment to protect patient privacy. The proposed model differs from existing approaches mainly in terms of security. Table 5 compares the approaches used existing models with the proposed model discussed in section 3. We selected recent access control studies related to patient privacy protection for comparison.

The following five security evaluation factors were used for comparisons with existing studies:

1) Authorization: A process of granting or denying a user access to a system. This grants the user permission to access appropriate health data only.

2) Confidentiality: Ensures that health data remain confidential and inaccessible to unauthorized users.

3) Integrity: Ensures that health data are not modified when delivered to another party. Only authorized users can change health data.

4) Accountability: Monitors access to medical data. This allows the system to identify the user who performed a particular action and what actions occurred during a specific period.

5) Non-Repudiation: Ensures that the abuse of medical data cannot be denied by proving the fact after sending or receiving a message.

As shown in Table 5, most of the security EHR modeling Approaches have problems with fully supporting various security activities because they are too focused on a specific activity. Most studies proposed a method for access control that does not address the problems of confidentiality and integrity of internal data. Because patient data can be attacked in a variety of manners, multiple security systems are required to protect privacy. In this paper, we satisfy these requirements through a two-phase model.

According to Abbas and Kahn [12], privacy-preserving techniques in e-health fall into two categories: cryptographic approaches and non-cryptographic approaches (e.g., access control). The model proposed in this study falls within the group of cryptographic approaches because it contains an encryption technique. However, the encryption technique we use is not used directly to protect a patient's health data privacy, but is an additional technique used for secondary protection after access control. Therefore, the proposed model is closer to being a hybrid approach.

As shown in Table 5, many existing approaches use RBAC. However, as the numbers of resources and users increase, the RBAC model increases the number of roles and policies, resulting in a scalability issue [59]. This problem is caused by the static characteristics of RBAC. The ABAC model has been developed to resolve this issue. The ABAC used in the

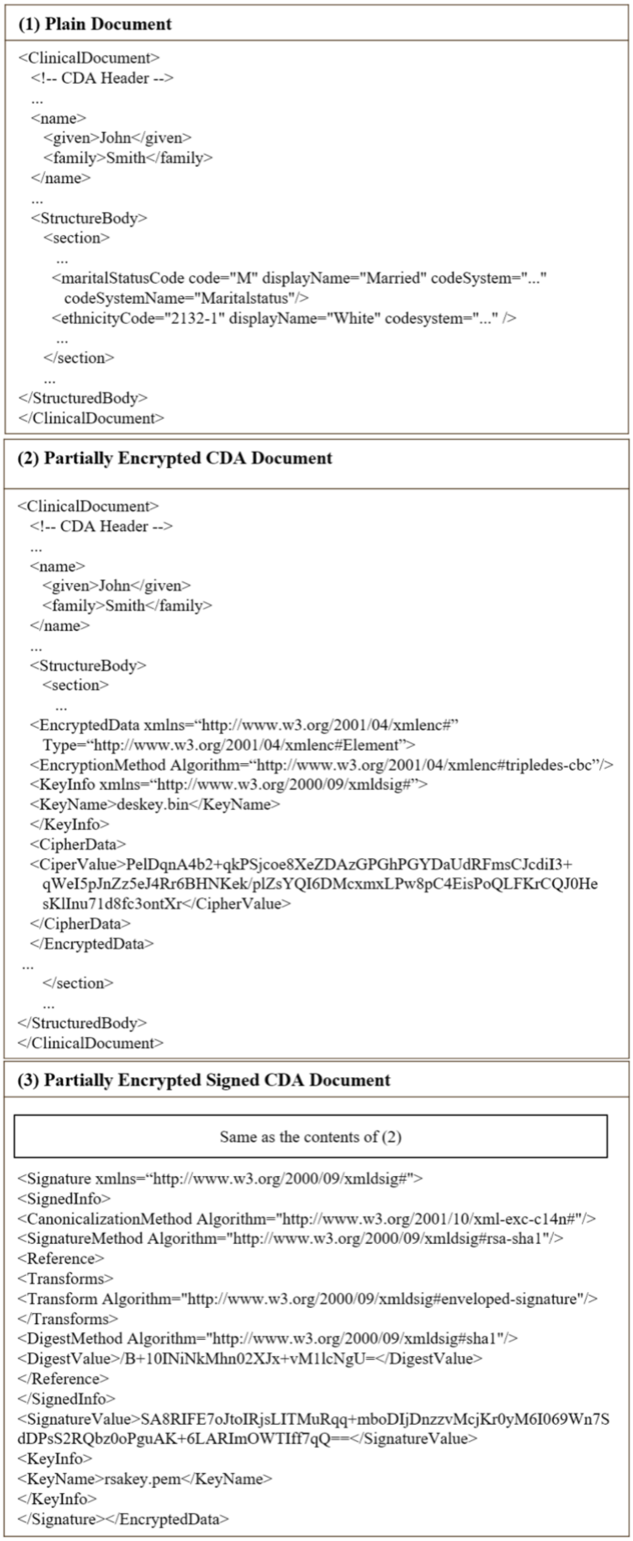
TABLE 5. Comparison with existing privacy preservation studies in e-health.

	Strength(s)	Weakness(es)	Privacy-preserving mechanism	Operation Environment	AU	CO	IN	AC	NR	ST	IM
CHISTAR [28]	Interoperability, scalability, maintainability	Inflexible access control	RBAC, AES-256, SSO, SSL, MAC	Cloud-based	✓	✓	✓	✓	✗	✓	✓
Vista [54]	-	client-server architecture,	RBAC	Non-cloud-based	✓	✗	✗	✓	✗	✓	✓
Hsieh and Chen [29]	Flexible access control, confidentiality and integrity control	Lack of prototype implementation	ABAC(XACML), XML Security (on Policy)	Cloud-based	✓	✓	✓	✓	✓	✗	✗
Rezaeibagha and Mu [31]	Scalability, confidentiality, and secure data outsourcing.	Data sharing problems can be caused by increasing the complexity of EHR data policies and users	RBAC, CP-ABE	Cloud-based	✓	✓	✗	✓	✗	✗	✗
Premarathne et al. [32]	Performs access control through context and location awareness	Key exchange problem between various parties	RBAC, PKI	Cloud-based	✓	✗	✓	✓	✗	✗	✗
Peleg et al. [33]	Structured specification of patient data access scenarios via situation models,	Scalability issues	Situation-based Access Control	Not indicated	✓	✗	✗	✓	✗	✓	✗
Gajanayake et al. [34]	Combine three existing access control models	-	MAC, DAC, RBAC, PBAC	Not indicated	✓	✗	✗	✓	✗	✗	✓
Lunardelli et al. [35]	Provides a solution to the situation of policy conflict	Lack of security aspect issue	ABAC (XACML)	Not indicated	✓	✗	✗	✓	✗	✗	✓
Calvillo-Arbizu et al. [36]	Flexible access control	No consideration of confidentiality or integrity issues	ABAC (XACML)	Not indicated	✓	✗	✗	✓	✗	✓	✗
Gope and Amin [37]	Practicality, robustness	Inflexible access control	RBAC, MAC	Cloud-based	✓	✓	✗	✓	✓	✗	✗
Alshehri et al. [38]	High performance over time overhead and storage overhead	Lack of non-repudiation	ABAC, ECC, CP-ABE	Cloud-based	✓	✓	✓	✓	✗	✓	✗
Yang et al. [39]	Flexible access control, dynamically changing user's attributes	Lack of implementation system	ABAC, time-domain ABE	Cloud-based	✓	✓	✗	✓	✗	✗	✗
Mohandas [41]	Fine grained access control, anonymization	-	ABAC, CP-ABE, k-anonymization	Cloud-based	✓	✓	✗	✓	✓	✗	✓
Neubauer and Heurix [55]	Provides a methodology for the pseudonymization of medical data	No cover for digital signature	Pseudonymization, encryption	Not indicated	✓	✓	✓	✗	✗	✓	✓
Sandıkkaya et al. [56]	Performed the pseudonymization and can break-the glass procedures.	Inflexible access control	Encryption, signature, RBAC and pseudonymization	Not indicated	✓	✓	✓	✓	✓	✗	✓
Sharma and Balasubramanian [57]	self-protect the data in case of breached access using biometrics.	-	Biometric encryption	Cloud-based	✓	✓	✗	✗	✗	✗	✓
Au and Croll [58]	Consider various factors for privacy protection	Inflexible access control	Pseudonymization, PKE, RBAC, digital signature	Not indicated	✓	✓	✓	✓	✓	✓	✗
Proposed Approach	Fully support all evaluation requirements	-	ABAC(XACML), XML Security	Cloud-based	✓	✓	✓	✓	✓	✓	✓

* AU: Authorization, CO: Confidentiality, IN: Integrity, AC: Accountability, NR: Non-repudiation, ST: Standard, IM: Implementation

proposed model is a more flexible approach than RBAC, thus enabling more fine-grained access control.

Many existing studies related to the ABAC mechanism use ABE [60]. Typically, these schemes use attribute values as parameters to generate cipher text and secret keys. In ABE, a user with a secret key for that attribute can decrypt the encrypted data [61]. Compared with the existing PKE approach, ABE allows flexible one-to-many encryption, rather than one-to-one encryption. Moreover, data access without a trusted mediator is possible when using cryptography [58]. ABE also has a low cost in the decryption phase owing to the bilinear pairing computation [62].



(1) Plain Document

```
<ClinicalDocument>
  <!-- CDA Header -->
  ...
  <name>
    <given>John</given>
    <family>Smith</family>
  </name>
  ...
  <StructureBody>
    <section>
      ...
     <maritalStatusCode code="M" displayName="Married" codeSystem="..."
       codeSystemName="Maritalstatus"/>
     <ethnicityCode="2132-1" displayName="White" codesystem="..." />
      ...
    </section>
    ...
</StructuredBody>
</ClinicalDocument>
```

(2) Partially Encrypted CDA Document

```
<ClinicalDocument>
  <!-- CDA Header -->
  ...
  <name>
    <given>John</given>
    <family>Smith</family>
  </name>
  ...
  <StructureBody>
    <section>
      ...
  <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
    Type="http://www.w3.org/2001/04/xmlenc#Element">
  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <KeyName>deskey.bin</KeyName>
  </KeyInfo>
  <CipherData>
  <CiperValue>PelDqnA4b2+qkPSjcoe8XeZDAzGPGhPGYDaUdRFmsCJcdiI3+
    qWeI5pJnZz5eJ4Rr6BHNKek/plZsYQI6DMcxmxLPw8pC4EisPoQLFKrCQJ0He
    sKlInu71d8fc3ontXr</CipherValue>
  </CipherData>
  </EncryptedData>
 ...
    </section>
    ...
</StructuredBody>
</ClinicalDocument>
```

(3) Partially Encrypted Signed CDA Document

Same as the contents of (2)

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference>
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>/B+10INiNkMhn02XJx+vM1lcNgU=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>SA8RIFE7oJtoIRjsLITMuRqq+mboDIjDnzzvMcjKr0yM6I069Wn7S
dDPsS2RQbz0oPguAK+6LARImOWTIff7qQ==</SignatureValue>
<KeyInfo>
<KeyName>rsakey.pem</KeyName>
</KeyInfo>
</Signature></EncryptedData>
```

FIGURE 10. The process of encrypting and digitally signing medical documents.

However, the ABE method has a disadvantage in that the owner of the data must encrypt the data using the public key of the user who has full authority. There are limits to applying these schemes in real-world environments because they allow users access to the system using monolithic attribute access [63]. Although further studies are attempting to fix this problem in the classical ABE model (e.g., KP-ABE, CP-ABE, NON-MONOTONIC, HABE, and MABE), these studies also have complicated or unsuitable problems in terms of implementation. The XML encryption technology applied to our model is simple and provides flexibility in terms of encryption. One of the benefits of XML encryption is the ability to selectively encrypt portions of a message and, thus, to protect integrity. This ensures confidentiality, and a patient's medical documentation may only be partially encrypted for elements that require encryption. XML encryption is compatible with a variety of encryption algorithms (e.g., AES-256, TRIPLEDES, etc.).

There were also some other mechanisms for protecting medical information privacy. For example, many studies have used anonymization and pseudonymization mechanisms to protect privacy. Encryption and this de-identification mechanism are different concepts because of the following characteristics: this de-identification mechanism is to make sure that the information is public and not know who it is, and encryption does not allow information to be identified before disclosure. Thus, rather than how a mechanism is more effective at protecting privacy, each can be used as an underlying technology for privacy protection, depending on factors or situations to protect. Our paper does not address this mechanism at present, but we will address this issue in future studies.

The proposed model uses XML digital signatures to ensure data integrity and non-repudiation. Digital signatures provide a useful way to prove authentication (for the sender of a signed message), integrity (for signed documents), and non-repudiation [64]. Digital signatures can be used to show that a digitally signed document is exactly what the signer intended, and that no tampering has occurred in the process of generating, distributing, or storing an electronic document. It is also possible to perform a non-repudiation function by checking the content of a message using a digital signature. Additionally, the proposed model follows the technical safeguard standards proposed by HIPAA and its applicability was demonstrated through prototype implementation.

VI. CONCLUSION

Recently, EHR systems in the cloud environment have shown the potential to improve the quality of medical service by sharing and utilizing patient data across various medical institutions. However, this environment creates additional security risks and patient privacy can be violated by various malicious attacks. Despite the importance of data security, many systems do not consider security factors during their modeling process or regard them as minor factors.

We proposed a cloud-based EHR model that guarantees patient privacy. The proposed model is divided into two stages: access control, and the application of encryption and digital signatures. The proposed model uses an ABAC method built upon XACML. After performing access control on patient documents, encryption is performed and digital signatures are added using XML encryption and XML digital signatures as an added security measure. The proposed model provides more flexible and fine-grained control than existing RBAC systems and alleviates the risk of exposing patient privacy information by using partial encryption and electronic signatures. The implementation of a prototype demonstrated the feasibility of the proposed model. We compared the implemented security factors with those used in other related studies and determined that the proposed method is superior to previous methods in terms of security.

In the future, we will further refine the processes used in the proposed model and implement additional security features. We will also expand the implementation of the prototype to implement a more refined system and perform quantitative performance evaluation.

REFERENCES

[1] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, "Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption," *J. Amer. Med. Informat. Assoc.*, vol. 13, no. 2, pp. 121–126, 2006. [Online]. Available: https://academic.oup.com/jamia/article/13/2/121/729326/Personal-Health-Records-Definitions-Benefits-and

[2] C. P. Waegemann. (2003). *Ehr vs. CPR vs. EMR. Healthcare Informatics Online*. [Online]. Available: https://pdfs.semanticscholar.org/ce2f/cf783c1fa2afdaa81c5a46c317e7edff04bc.pdf

[3] H. van der Linden, D. Kalra, A. Hasman, and J. Talmon, "Inter-organizational future proof EHR systems: A review of the security and privacy related issues," *Int. J. Med. Inf.*, vol. 78, no. 3, pp. 141–160, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1386505608001081

[4] P. C. Tang, "*Key Capabilities of an Electronic Health Record System*," Washington, DC, USA: Institute Medicine National Academies, 2003. [Online]. Available: http://www.nationalacademies.org/hmd/Reports/2003/Key-Capabilities-of-an-Electronic-Health-Record-System.aspx

[5] R. H. Miller, C. West, T. M. Brown, I. Sim, and C. Ganchoff, "The value of electronic health records in solo or small group practices," *Health Affairs*, vol. 24, no. 5, pp. 1127–1137, 2005. [Online]. Available: http://content.healthaffairs.org/content/24/5/1127.short

[6] B. Middleton *et al.*, "Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA," *J. Amer. Med. Inf. Assoc.*, vol. 20, no. e1, pp. e2–e8, 2013. [Online]. Available: https://academic.oup.com/jamia/article/20/e1/e2/692244/Enhancing-patient-safety-and-quality-of-care-by

[7] S. R. Simon *et al.*, "Correlates of electronic health record adoption in office practices: a statewide survey," *J. Amer. Med. Inform. Assoc.*, vol. 14, no. 1, pp. 110–117, 2007. [Online]. Available: https://academic.oup.com/jamia/article/14/1/110/746202/Correlates-of-Electronic-Health-Record-Adoption-in

[8] K. A. Ratnam and P. D. D. Dominic, "Cloud services—Enhancing the Malaysian healthcare sector," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, Jun. 2012, pp. 604–608. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6297101/

[9] R. Zhang and L. Liu (2010 July "Security models and requirements for healthcare application clouds," in *Proc. IEEE 3rd Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2010, pp. 268–275. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/5557983/

[10] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in *Proc. ACM Workshop Cloud Comput. Security*, 2009, pp. 103–114. [Online]. Available: http://dl.acm.org/citation.cfm?id=1655024

[11] P. Ray and J. Wimalasiri, "The need for technical solutions for maintaining the privacy of EHR," in *Proc. 28th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBS)*, Sep. 2006, pp. 4686–4689. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/4462848/

[12] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 4, pp. 1431–1441, Apr. 2014. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6714376/

[13] *Extensible Access Control Markup Language (XACML) Version 3.0*, OASIS Standard 22, Jan. 2013. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[14] (Dec. 10, 2002). *XML Encryption Syntax and Processing, W3C Recommendation*. [Online]. Available: http://www.w3.org/TR/xmlenc-core/

[15] *Standards for Privacy of Individually Identifiable Health Information: Final Rule*, Standard 45 CFR Parts 160 and 164, Dec. 2000.

[16] (2016). *openEHR—A Semantically-Enabled, Vendor-Independent Health Computing Platform*. [Online]. Availabile: http://www.openehr.org/resources/white_paper_docs/openEHR_vendor_independent_platform.pdf

[17] (2017). *HL7: Health Level 7 (HL7)*. [Online]. Available: http://www.hl7.org

[18] R. H. Dolin, L. Alschuler, S. Boyer, C. Beebe, F. M. Behlen, and P. V. Biron, *Hl7 Clinical Document Architecture, Release 2.0*, ANSI Standard ISO/HL7 27932:2009, 2004.

[19] (2009). *HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component*. [Online]. Available: http://www.hitsp.org/ConstructSet_Details.aspx?&PrexAlpha=4&PrexNumeric=32

[20] *HITECH Act Enforcement Interim Final Rule*, US Health & Human Services, Washington, DC, USA, 2013.

[21] *Standard Specification for Continuity of Care Record (CCR)*, Standard ASTM E2369, 2005. [Online]. Available: https://www.astm.org/Standards/E2369.htm

[22] H. S. G. Pussewalage and V. A. Oleshchuk "Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions," *Int. J. Inf. Manage.*, vol. 36, no. 6, pp. 1161–1173, Dec. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0268401216300706

[23] J. L. Fernández-Alemán, I. C. Señor, P. A. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1532046412001864

[24] M. Anwar, J. Joshi, and J. Tan, "Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges," *Health Policy Technol.*, vol. 4, no. 4, pp. 299–311, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2211883715000659

[25] S. S. Bhuyan *et al.*, "Privacy and security issues in mobile health: Current research and future directions," *Health Policy Technol.*, vol. 6, no. 2, pp. 188–191, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2211883717300047

[26] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Inform.*, vol. 55, pp. 272–289, Jun. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S153204641500074X

[27] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Inform. J.*, vol. 18, no. 2, pp. 113–122, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1110866516300482

[28] A. Bahga and V. K. Madisetti, "A cloud-based approach for interoperable electronic health records (EHRs)," *IEEE J. Biomed. Health Informat.*, vol. 17, no. 5, pp. 894–906, Sep. 2013. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6497443/

[29] G. Hsieh and R.-J. Chen, "Design for a secure interoperable cloud-based Personal Health Record service," in *Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2012, 472–479. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6427582/

[30] (Jun. 10, 2008). *XML Signature Syntax and Processing (Second Edition), W3C Recommendation*. [Online]. Available: http://www.w3.org/TR/xmldsig-core/

[31] F. Rezaeibagha and Y. Mi, "Distributed clinical data sharing via dynamic access-control policy transformation," *Int. J. Med. Inform.*, vol. 89, pp. 25–31, May 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1386505616300223

[32] U. Premarathne *et al.*, "Hybrid cryptographic access control for cloud-based EHR systems," *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 58–64, Aug. 2016. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/7571083/

[33] M. Peleg, D. Beimel, D. Dori, and Y. Denekamp, "Situation-based access control: Privacy management via modeling of patient data access scenarios," *J. Biomed. Inform.*, vol. 41, no. 6, pp. 1028–1040, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1532046408000506

[34] R. Gajanayake, R. Iannella, and T. Sahama, "Privacy oriented access control for electronic health records," *Electron. J. Health Inform.*, vol. 8, no. 2, p. 15, 2014. [Online]. Available: http://www.ejhi.net/ojs/index.php/ejhi/article/view/265

[35] A. Lunardelli, I. Matteucci, P. Mori, and M. Petrocchi, "A prototype for solving conflicts in XACML-based e-Health policies," in *Proc. IEEE 26th Int. Symp. Comput.-Based Med. Syst. (CBMS)*, Jun. 2013, pp. 449–452. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6627838/

[36] J. Calvillo-Arbizu, I. Roman-Martinez, and L. M. Roa-Romero, "Standardized access control mechanisms for protecting ISO 13606-based electronic health record systems," in *Proc. IEEE-EMBS Int. Conf. Biomed. Health Inform. (BHI)*, Jun. 2014, pp. 539–542. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6864421/

[37] P. Gope and R. Amin, "A novel reference security model with the situation based access policy for accessing ephr data," *J. Med. Syst.*, vol. 40, p. 242, Nov. 2016. [Online]. Available: https://link.springer.com/article/10.1007/s10916-016-0620-4

[38] S. Alshehri, S. P. Radziszowski, and R. K. Raj, "Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption," in *Proc. IEEE 28th Int. Conf. Data Eng. Workshops (ICDEW)*, Apr. 2012, pp. 143–146. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6313671/

[39] K. Yang, Z. Liu, X. Jia, and X. S. Shen, "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach," *IEEE Trans. Multimedia*, vol. 18, no. 5, pp. 940–950, May 2016. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/7422115/

[40] Y. Y. Chen, J. C. Lu, and J. K. Jan, "A secure EHR system based on hybrid clouds," *J. Med. Syst.*, vol. 36, no. 5, pp. 3375–3384, 2012. [Online]. Available: https://link.springer.com/article/10.1007/s10916-012-9830-6

[41] A. Mohandas and S. S, "Privacy preserving content disclosure for enabling sharing of electronic health records in cloud computing," in *Proc. 7th ACM India Comput. Conf.*, 2014, Art. no. 7. [Online]. Available: https://dl.acm.org/citation.cfm?id=2675753

[42] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller, "Aspects of privacy for electronic health records," *Int. J. Med. Inform.*, vol. 80, no. 2, pp. e26–e31, 2011. [Online]. Available: https://dl.acm.org/citation.cfm?id=1943539

[43] P. W. Fong, "Relationship-based access control: Protection model and policy language," in *Proc. 1st ACM Conf. Data Appl. Security Privacy*, Feb. 2011, pp. 191–202. [Online]. Available: https://dl.acm.org/citation.cfm?id=1943539

[44] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[45] Y. Y. Chen, J. C. Lu, and J. K. Jan, "A secure EHR system based on hybrid clouds," *J. Med. Syst.*, vol. 36, no. 5, pp. 3375–3384, 2012. [Online]. Available: https://link.springer.com/article/10.1007/s10916-012-9830-6

[46] M. Abomhara, H. Yang, and G. M. Køien, "Access control model for cooperative healthcare environments: Modeling and verification," in *Proc. IEEE Int. Conf. Healthcare Inform. (ICHI)*, Oct. 2016, pp. 46–54. [Online]. Available: http://ieeexplore.ieee.org/document/7776326/#full-text-section

[47] M. Sicuranza and A. Esposito, "An access control model for easy management of patient privacy in EHR systems," in *Proc. 8th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2013, pp. 463–470. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6750243/

[48] (2015). *Oracle's Java SE Development Kit 8*. [Online]. Available: http://docs.oracle.com/javase/8/docs/

[49] (Jan. 30, 2015). *WSO2 Balana 1.0.0*. [Online]. Available: http://xacmlinfo.org/category/balana/

[50] (Apr. 20, 2017). *XML Security Library 1.2.24*. [Online]. Available: https://www.aleksey.com/xmlsec/

[51] (2004). *Libxml2 Library*. [Online]. Available: http://xmlsoft.org/downloads.html

[52] OpenSSL Software Foundation. (Feb. 16, 2017). *OpenSSL 1.1.0e Library*. [Online]. Available: https://www.openssl.org

[53] A. E. Johnson. (Mar. 2016). *MIMIC-III, A Freely Accessible Critical Care Database*. Scientific Data. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4878278/

[54] (2012). *VistA Monograph*. [Online]. Available: www.va.gov/vista monograph

[55] T. Neubauer and J. Heurix, "A methodology for the pseudonymization of medical data," *Int. J. Med. Inform.*, vol. 80, no. 3, pp. 190–204, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1386505610002042

[56] M. T. Sandıkkaya, D. B. De, and V. Naessens, "Privacy in commercial medical storage systems," in *Proc. Int. Conf. Electron. Healthcare*, Dec. 2010, pp. 247–258. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-23635-8_32

[57] S. Sharma and V. Balasubramanian, "A biometric based authentication and encryption framework for sensor health data in cloud," in *Proc. Int. Conf. Inf. Technol. Multimedia (ICIMU)*, Nov. 2014, pp. 49–54. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/7066602/

[58] R. Au and P. Croll, "Consumer-centric and privacy-preserving identity management for distributed e-health systems," in *Proc. 41st Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2008, p. 234. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/4438938/

[59] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The NIST model for role-based access control: Towards a unified standard," in *Proc. ACM Workshop Role-Based Access Control*, Jul. 2000, pp. 1–11. [Online]. Available: http://csrc.nist.gov/staff/Kuhn/towards-std.pdf

[60] S. Zeadally and M. Badra, Eds., *Privacy in a Digital, Networked World: Technologies, Implications and Solutions*. London, U.K.: Springer, Oct. 2015. [Online]. Available: https://link.springer.com/content/pdf/10.1007/978-3-319-08470-1.pdf

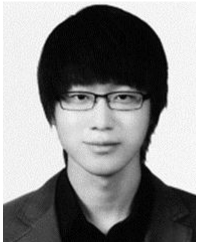
[61] A. Sahai and B. Waters. "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, May 2005, pp. 457–473. [Online]. Available: https://link.springer.com/content/pdf/10.1007/b136415.pdf#page=470

[62] C. Wang, X. Liu, and W. Li, "Design and implementation of a secure cloud-based personal health record system using ciphertext-policy attribute-based encryption," *Int. J. Intell. Inf. Database Syst.*, vol. 7, no. 5, pp. 389–399, 2013. [Online]. Available: http://www.inderscienceonline.com/doi/abs/10.1504/IJIIDS.2013.056381

[63] H. Lin, J. Shao, C. Zhang, and Y. Fang, "CAM: Cloud-assisted privacy preserving mobile health monitoring," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 985–997, Jun. 2013. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6490390/

[64] R. N. Lakshmi, R. Laavanya, M. Meenakshi, and C. S. G. Dhas, "Analysis of attribute based encryption schemes," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 3, pp. 1076–1081, 2015. [Online]. Available: http://oaji.net/articles/2015/2028-1433398925.pdf

[65] R. Kaur and A. Kaur, "Digital signature," in *Proc. Int. Conf. Comput. Sci. (ICCS)*, Sep. 2012, pp. 295–301. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6391693/



KWANGSOO SEOL is currently pursuing the Ph.D. degree in computer engineering with the Department of Computer Science and Engineering, Korea University. His current research interests include medical security, self-adaptive software, big data, and machine learning. He is a member of the Center for Autonomous and Adaptive Software with Korea University.

YOUNG-GAB KIM received the B.S. degree in biotechnology and genetic engineering and minored in computer science and engineering and the M.S. and Ph.D. degrees in computer science and engineering from Korea University, Seoul, South Korea, in 2001, 2003, and 2006 respectively. He was an Assistant Professor with the School of Information Technology, Catholic University of Daegu. He is currently an Associate Professor with the Department of Computer and Information Security, Sejong University. He has published over 130 research papers in the field of computer science and information security. His current research interests include big data security, network security, home network, security risk analysis, and security engineering. As a Korean ISO/IEC JTC1 member, he is contributing in developing data exchange standards.

EUIJONG LEE is currently pursuing the Ph.D. degree in computer engineering with the Department of Computer Science and Engineering, Korea University. His current research interests include self-adaptive software, software verification, model-checking, and machine learning. He is a member of the Center for Autonomous and Adaptive Software with Korea University.

YOUNG-DUK SEO is currently pursuing the Ph.D. degree in computer engineering with the Department of Computer Science and Engineering, Korea University. His current research interests include self-adaptive software, big data, and social network services. He is a member of the Center for Autonomous and Adaptive Software with Korea University.

DOO-KWON BAIK received the B.S. degree in mathematics from Korea University, Seoul, Korea, in 1974, and the M.S. and Ph.D. degrees in computer science from Wayne State University, Detroit, MI, USA, in 1983 and 1986, respectively. He was the Founder and the Director of Information and Communication Research Institute, Korea University. He is currently the Director of Software System Laboratory and a Professor of Computer Science Department, Korea University. His current research interests include modeling, simulation, and software engineering. He has been a Committee Member of ISO/IEC JTC1/SC32 for 20 years.