International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 05, 2020
ISSN: 1475-7192

A Model for Xml-based Electronic Health Record System

N. Gayathri, A. Priya, S. Sridhar and G. Charlyn Pushpa Latha

Abstract--- *Cloud-based electronic health record (EHR) frameworks change medicinal reports to be exchanged between medical institution; this can be relied upon to add to improvements in various therapeutic administrations; this can be expected to contribute enhancements in numerous medical services within the future. However, because the system design becomes more difficult, cloud-based EHR systems might introduce further security threats in comparison to existing singular systems. Thus, patients privacy in any health care system that's supported the quality of every patient within the health record system. so as to shield the privacy of patients, several approaches are planned to produce access management to patient documents once providing health services. However, most current systems don't support fine-grained access management or take into consideration further security factors like coding and digital signatures. In this paper, we've a bent to propose a cloud-based EHR model that performs attribute-based access management exploitation extensile access management language. Our EHR exhibit on security, performs fractional mystery composing and uses electronic marks once a patient record is circulated to a report requester. we have a tendency to use XML coding and XML digital signature technology. Our planned model works expeditiously and solely the mandatory data to requesters, who are for more efficiency and increased patients safety.*

Keywords--- *Cloud Storage, Access Control, Privacy Preserving, Cloud Security, XML (Extensible Markup Language), Attribute-based Encryption Scheme.*

I. INTRODUCTION

The technology has created nice strides within the field of medical information. so as to manage giant amounts of medical information transparently and cost-effectively, the necessity for processed medical information has inflated, and paper-based recording ways square measure bit by bit being replaced by digitized medical data systems [1]. EHRs square measure electronically hold on digital forms containingall of a patient's medical data [2]. EHRs follow international standards to confirm ability so patient information isn't created and managed by one health care organization, however by multiple medical establishment systems that permit sharing between numerous health care suppliers and organizations [3] (e.g., hospitals, laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and universities). The adaption of EHR will play a very important role in risingpatient safety and health care quality [4-6].

The existing EHR system was made in a very centralized information surroundings and medical data was hold

N. Gayathri, Assistant Professor, Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences. E-mail: gayathri005ece@gmail.com

A. Priya, Assistant Professor, Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences. E-mail: a.priya48@gmail.com

S. Sridhar, Assistant Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences. E-mail: 007sridol@gmail.com

G. Charlyn Pushpa Latha, Associate Professor, Department of Information Technology, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai. E-mail: charlyn.latha@gmail.com

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

on and managed within the context of hospital systems. However, thisapproach incurs high prices thanks to the initial construction of the system, maintenance, background, lack of practiced system engineers, and problems with patient medical data being incompatible with the systems in different hospitals. One potential resolution for the issues represented higher than has begun attracting vital attention [7]. That resolution is AN EHR system supported the cloud surroundings. Cloud computing is managed by a cloud supplier, that has benefits in terms of price and system enlargement in comparison to existing systems

Patient information may be shared and managed by numerous care suppliers. However, AN EHR system within the cloud surroundings comes with further security problems compared to a single-system surroundings as a result of patient information exchange happens between the cloud platform and numerous care establishments [9]. Patient personal data might cause security and privacy issues as a result of it contains sensitive and confidential information concerning the patient (e.g., hospitals, laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and universities) [10]. This data should be handled with care as a result of its exposure would represent a severe breach of the privacy of the individual. The EHR system should be designed to ensure security and privacy once sharing personal patient data [11].

Access management is incredibly necessary for shielding patient privacy once providing health services. Access management suggests that solely sending patient documents to approved doctors. However, most up-to-date access management systems for health services square measure inflexible thanks to exploitation role-based access management (RBAC) schemes [12]. What is more, further security problems might arise thanks to an absence of thought for numerous security factors. Therefore, so as to style a secure and versatile access system to shield patient privacy, we have a tendency to propose AN attribute-based access management model exploitation protractible access management language (XACML) [13].

The main contributions of this paper square measure as follows. 1) The attribute-based access management utilized in the planned model will give versatile and fine-grained access management in comparison to existing RBAC schemes. 2) By acting partial coding of patient privacy-related parts in patient documents via protractible language (XML) coding [14], the danger of further privacy exposure for the patient once a certified user views the patient documents are often prevented. 3) The digital signature method will prove that a document has not been falsified or altered, and may stop non-repudiation of the document. In addition, the planned model conforms to the technical safeguards of the yankee normal insurance movability and responsibleness act (HIPAA) [15].

II. RELATED WORK

Standards for EHR Systems

There square measure presently many standards in development for specifying EHRs, like HIPAA, OpenEHR [16], the health level seven (HL7) clinical document design (CDA) [17,18], and continuity of care document(CCD) [19]. HIPAA provides security measures and privacy protection mechanisms to shield health data. HIPAA has outlined personal recognizable data (e.g., Social Security variety, medical ID variety, mastercard variety, licence variety, home address, phone number, medical records, and different necessary data) as protected health information (PHI). HIPAA was created to shield the individual's letter. In 2009, HIPAA was redesigned into wellbeing

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

information innovation for financial and clinical wellbeing (HITECH) [20].HITECH provides further compliance standards for firms concerned in care. The technical safeguard portion of HIPAA specifies what needs should be met within the style of access management, transmission security, etc. once developing medical systems.

The HL7 CDA could be a markup normal that defines the structure and linguistics of CDA clinical documents for sharing functions. Clinical documentation could be a record of medical observations and services, and CDA records might embody text, images, sounds, and different multimedia system content. The CDA is encoded in XML, ANd associate degree execution system that exchanges CDA documents ought to meet all legal wants for authentication, confidentiality, and the technical portion are often designed by engineers, and therefore the clinical information portion are often designed by clinicians.

B. Privacy-preserving Methodologies for EHR Systems Several study papers have checked on security saving plans for EHR frameworks [12, 22-27]. Abbas ANd Khan [12] represented the wants that ought to be thought of for privacy in an E-health cloud. To preserve health information privacy in a very cloud surroundings, they represented however the e-Health system ought to take into account the subsequent requirements: integrity, confidentiality, legitimacy, responsibleness, audit, non-repudiation, anonymity, and unlinkability. They conjointly assessed however well studies on privacy preservation in EHR systems take into account these factors. They classify privacy-preserving approaches in e-Health Clouds as science approaches and non-cryptographic approaches. The science approaches use coding schemes like public key coding (PKE), bilateral key coding (SKE), and attribute-based coding (ABE) to shield health information in e-Health Cloud environments. Studies classified as non-cryptographic approaches in the main use techniques like policy-based access management. Pussewalage and Oleshchuk [22] request progresses for security preservation into science framework approaches (e.g., PKE, SKE, and ABE), get to the executives approaches (e.g., RBAC, ABAC), and biometric approaches. They characterize the wellbeing and protection request parts for e-wellbeing as a patient's understanding, a patient's administration, classification, data honesty, assent exemption, non-reputation, and auditing. Then, they assess whether or not papers proposing privacy-preserving schemes mirror these factors. Fernández-Alemán et al. [23] selected the highest papers within the field and analyzed the newest analysis trends. Their results show that over [*fr1] the EHR systems exploitation access management use RBAC, which twenty second use a public key infrastructure (PKI)-based digital signature mechanism.

There are many access management studies on EHR systems with the goal of protective the privacy of patients [28, 29, 31-47]. Bahga and Madisetti [28] received a two-level demonstrating approach for accomplishing phonetics capacity. It supports security measures and addresses the key needs of HIPAA and HITECH. Hsieh and Chen [29] planned a style for a secure practical cloud-based EHR service. It applies a broad spectrum of security mechanisms as well as XACML access management, XML coding, and XML digital signatures [30]. Rezaeibagha and alphabetic character [31] planned a secure EHR system design for secure information sharing. Their study divided the EHR system domain into direct and indirect access, and guarded patient privacy exploitation RBAC. Premarathne et al. introduced a science RBAC display for EHR frameworks. For user authentication, location and identity verification techniques were introduced, and steganography was applied to EKG (ECG) signal information. Peleg et al. [33] highlighted the issues with the RBAC model utilized in existing EHR system and planned a situation-based access

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

management model (SitBAC). SitBAC is intended to utilize understanding data get to ask for consequences in light of the fact that the reason for patient security. Gjanayake et al. [34] thought of versatile access management techniques for protecting patient privacy. Their planned access management model consists of 4 modules: RBAC, MAC, DAC, and PBAC. They conjointly developed a web-based image. Lunardelli et al. proposed AN analytic hierarchy method (AHP) model for determination policy conflict problems in EHR systems. They made a picture and broke down the framework execution was misuse XACML Access the board. Calvillo-Arbizu et al. [36] addressed the difficulty of most current clinical and EHR systems exploitation access management measures to support needs inside solely one organization. They planned AN access management mechanism supported XACML attribute-based access management (ABAC), that conforms to ISO 13606, that supports multi-domain sharing. The planned system applies AN metaphysics for automatic reasoning to a decision-making method. Kan principle et al. [39] planned a science approach for video information sharing in a very cloud-based multimedia surroundings. they propose a time-domain ABE theme that has time in ciphertext and key so solely users with sufficient attributes in a very specific time interval will rewrite the video content. Ming Li et al. [44] planned a patient-centric framework and incontestable mechanisms for acting access management in a very semi-trusted server surroundings. To perform fine-grained and scalable access management, they used ABE technology to write in code patient information. They applied their mechanisms and reduced the quality of key management in eventualities wherever multiple information homeowners and patients were distributed across numerous security domains. Mohamed Abomhara et al. [46] planned a work-based access management model that modifies the user-role assignment model through the conception of team role. They sculpturesque and verified the policies exploitation model checking techniques referred to as access management policy testing (ACPT) and showed their planned model is versatile and simple to manage. Mario Sicuranza and Angelo Esposito [47] showed a brand new approach combining many access management models. They thought of the wants of patients, care organizations, international norms and directives for model design ANd showed an algorithmic rule for access management. However, most of those studies don't take into account security factors, like confidentiality or integrity, in their styles, or use inflexible access management techniques, like RBAC.

III. THE PLANNED EHR SYSTEM MODEL FOR SHIELDING PATIENT PRIVACY

In the planned EHR model, ABAC exploitation XACML and XML security for coding and digital signatures is employed to shield patient privacy. this will shield patients from the danger of privacy infringement by providing solely the desired content from the requested patient medical documents to approved users.

A. Framework

We propose a brand new methodology for the event of AN EHR system that protects the privacy of patients in a very cloud surroundings. an outline of the planned model is conferred in Fig. 1. The planned model works in 2 main phases. The aim of the planned model is to produce medical documentation solely to approved users, while not infringing on the patient's privacy. First, access management supported XACML language is performed. It evaluates whether or not the user is allowed to receive the medical document. When access management is performed, if the user is allowed to access the documents for the patient, part a pair of is performed to shield the patient's privacy. In

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

Phase 2, partial coding and digital signatures square measure accustomed transmit the privacy-protected documents to the requesting user.

B. ABAC Exploitation XACML (Phase 1)

In part one of the planned model, ABAC exploitation XACML is performed. This part is comprised of 3 main components: the policy social control purpose (PEP), the policy call purpose (PDP), and therefore the policy administration purpose (PAP). By acting access management, the system will verify if missive of invitationshould be allowable or denied. The ginger is answerable for receiving user needs and imposing choices supported processed results. once a user sends AN access request through the ginger, the ginger generates missive of invitation message within the kind of XACML supported the user needs and passes it to the PDP. The PDP retrieves the XACML request, searches for and analyzes connected policies, makes a final authorization call, ANd generates an XACML response message. The generated response message is delivered back to the ginger, that enforces the received call. The PDP refers to data from the policy data purpose (PIP) and policy retrieval purpose (PRP) to judge user requests. The PIP stores the extra attributes needed to judge the policy (e.g., user role, clearance, and document classification). The PRP stores XACML policy information for analysis by the PDP. XACML policies square measure managed at the PAP. System directors will perform actions like making, modifying, deleting, and looking policies through the PAP computer program. the look of all parts related to the choice creating (via the PDP) ought to be situated on a sure server.

The policy structure of XACML consists of a policy set and a policy rule. Every policy will solely match one Target. The Target is employed to see whether or not the policy is related to the request statement. The target are often mere exploitation the 3 following attribute categories: subject, resource, action. If the required attribute class matches the attribute class of the request statement, the corresponding policy is taken into account to be related to that request statement. for instance, if the policy is for a document within the medical class, we are able to specify the target of the policy as follows:

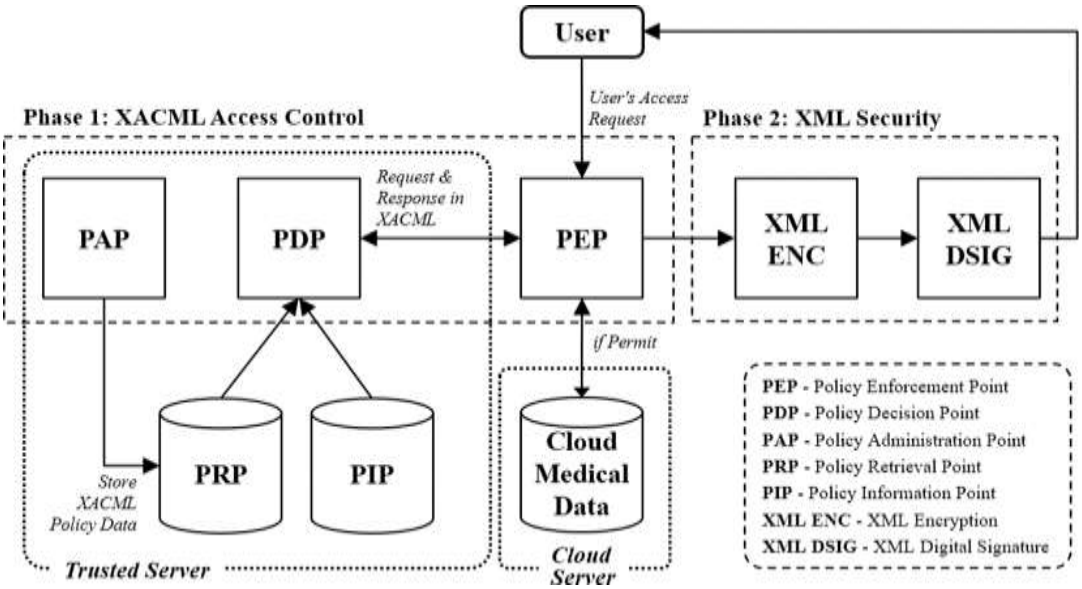


Fig. 1: Framework for our Planned Model

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

(Policy 1) Any subject will take any action on a (1) document within the medical class. A policy will specify multiple rules. Rules accommodates a Target, one or a lot of Conditions, and an impact. The target component utilized in the rule is employed to judge whether or not or not the corresponding rule is said to the request because the target of the policy. It's accustomed judge if the rule is said to the request. If no target is mere, the rule is evaluated for all requests.

Condition specify authorization logic statements that contain mathematician expression values. The rule is employed to see if the condition is true or false (or Indeterminate). The result worth is a part that determines what worth the rule can come back once the Condition is true. for instance, you'll specify the subsequent example rules for the Policy example higher than.

(Rule1) Subjects with the role of doctor will browse / print documents of their patient's medical category.(2)

(Rule2) Subjects with the role of AN emergency doctor will browse / print the medical class documents of their patients in emergency things.

If the condition is true and therefore the result worth is allow, then the comeback worth is allow. AN Obligation is AN elective component {that allows |that permits |that changes} XACML to enable a lot of fine-grained access management. Obligations specify the actions that the ginger ought to enforce whereas imposing authorization choices.

In XACML, every policy set has multiple policies, and every policy has multiple rules. A conflict will occur once totally different results square measure generated from every associated policy or rule. This downside are often solved by employing a policy- or rule-combination algorithmic rule. within the event of a conflict, the mixture algorithmic rule is employed to rank the results of every policy or rule and derive the result. Table one presents the quality combination algorithms supported by XACML three.0.

In order to specify context, missive of invitation message in XACML uses a structure specifying attribute classes, attribute values, and information. Fig. a couple of presents the structure of A XACML request. As pictured within the figure, one request message consists of many attributes, and attributes square measure comprised of 4 categories: subject, resource, action, and surroundings.

The request message asks the PDP the subsequent question: For a given subject, is it allowed to perform {the mere| there quired| the desired} action on the required resource within the specified environment? If the request message satisfies the policy condition, it returns the result worth.

Fig. 3 illustrates the method of generating AN XACML request message supported user needs. This method is performed within the ginger and therefore the generated XACML request is distributed to the PDP to judge whether or not or not it's approved. During this example, as a demand of the user, the emergency doctor, Bob, sends missive of invitation to browse the medical documents of the patient, Alice, throughout AN emergency. Once such a demand is formed, AN attribute extraction method is performed to extract and match the attributes from the need.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

Table I: The Standard Combination Algorithms Supported by XACML 3.0

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.

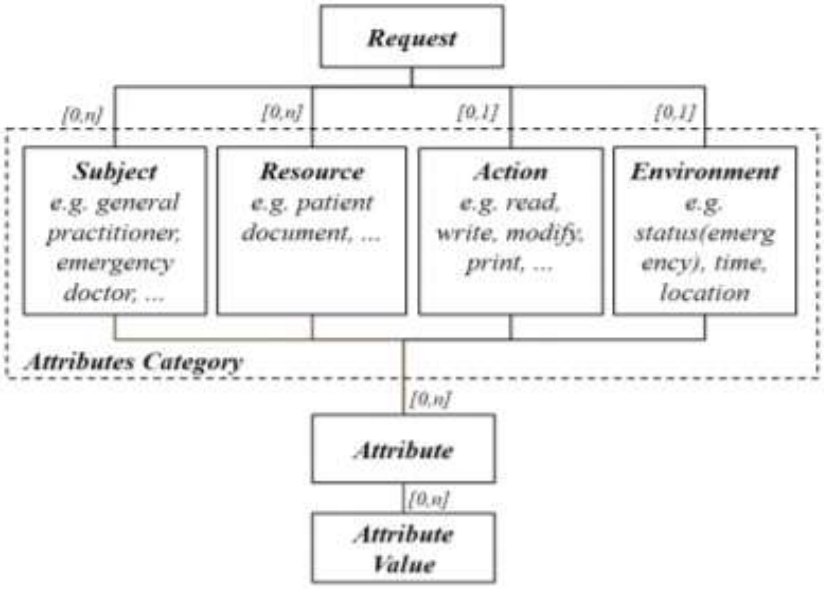
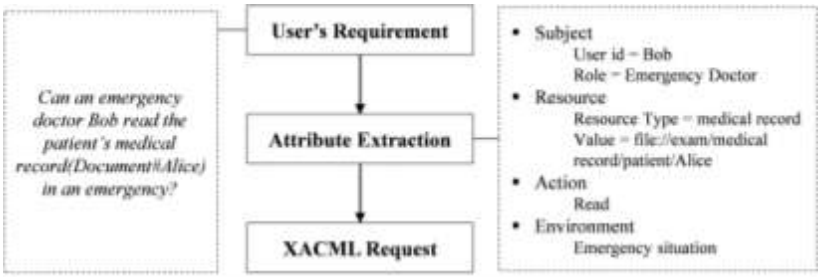


Fig. 2: Structure of an XACML Request

First, the actor, Bob (more specifically Bob's id), needs to access the documents matching the topic. The document that Bob needs to access is matched exploitation the resource data. The resource sort could be a case history, and therefore the worth is that the path to the document. Actors will perform numerous actions on the document, like browse, write, and print. During this example, solely browse is allowed, therefore the browse attribute is matched to the Action attribute. Finally, the surroundings matches the emergency state of affairs. At the top of the attribute extraction analysis. This method are often divided into 3 stages. The primary stage is that the method of determining compatibility settings and acting preprocessing before evaluating the request statement. for instance, the method of process XACML run constants is included this step. this permits the PDP to understand the

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

meaning of the mere information values once analyzing the content of missive of invitation message. This method 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 specified data. Because syntax is slightly totally different looking on the version of XACML, professionalcess, AN XACML request message are going to be generated following the addition of missive of invitation header and attribute information data input.




```
<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>
```

Fig. 3: An example of the method of generating AN XACML request message {in a |during a |in AN exceedingly| in a very} situation wherever the emergency doctor Bob accesses patient Alice's information in an emergency

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

The XACML request message generated by the ginger is passed to the PDP and evaluated for approval. Fig. four could be a flow chart illustrating the method of receiving missive of invitation message from the ginger and acting, one ought to check for compatibility via version checking ANd use an acceptable analysis methodology supported the version.

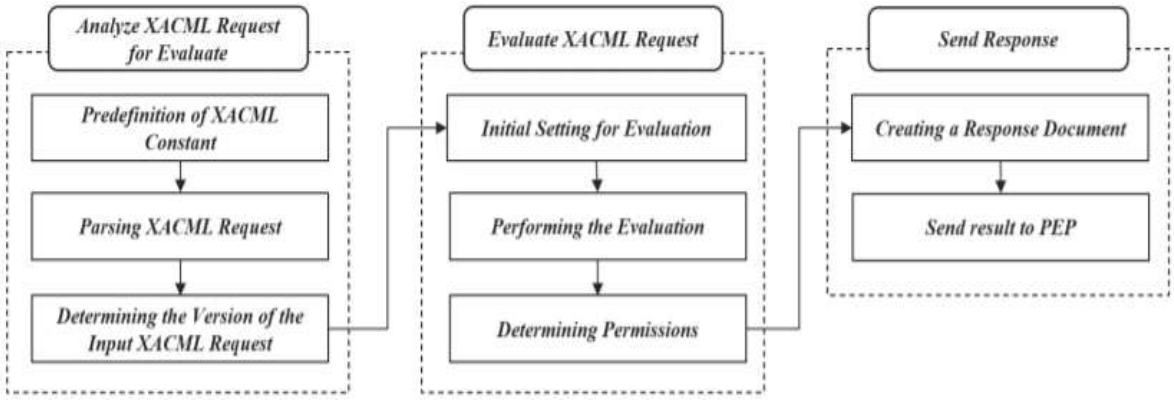


Fig. 4: The process of analyzing the request message and performing the evaluation process by the PDP to determine whether the user is a user who can access the patient's document

In the second stage, analysis is performed supported the parsed XACML request message information. The initial settings for analysis square measure determined throughout system style. once the policy love the request is found, the ultimate approval result's determined supported a calculation of the rule values for the relevant rules. Rule worth estimation is performed as shown in Table a pair of. The PDP returns allow or deny values if the requested access is granted or rejected, severally, and returns Indeterminate if the PDP cannot judge the request thanks to a slip (e.g., missing attributes, network errors whereas retrieving policies, policy analysis, syntax errors, etc.). If the PDP doesn't have a policy that applies to the request, it returns Not Applicable.

Table II: 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

The final stage is to make a response Message supported the results of the analysis stage and deliver it to the ginger. Fig. five presents the method of making a response message when the PDP has finished evaluating the instance situation from Fig. 4. The response message is comparatively straightforward compared to the request message. in a very response message, call results and a standing are often mere. during this example, solely one approval result's displayed as a result of it's a method for one request statement. However, once a multi request is received, AN approval result ought to be provided for every request.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

C. XML Security for Medical Document Security (Phase 2)

In the Access management part of the proposal model, once a user is allowed for a document, that document is then delivered to the user. The delivered document is prone to security threats as a result of it's a CDA/CCD original, that isn't encrypted or signed. Therefore, albeit the access management step has been performed, the patient still has the danger of their sensitive data being exposed. so as solve this downside, our planned model uses XML security throughout part

During this method, partial coding is performed exploitation XML coding and a digital signature is additional exploitation XML digital Signature. With XML coding, partial coding are often performed rather than total coding, which means it exposes solely the mandatory data to the user.

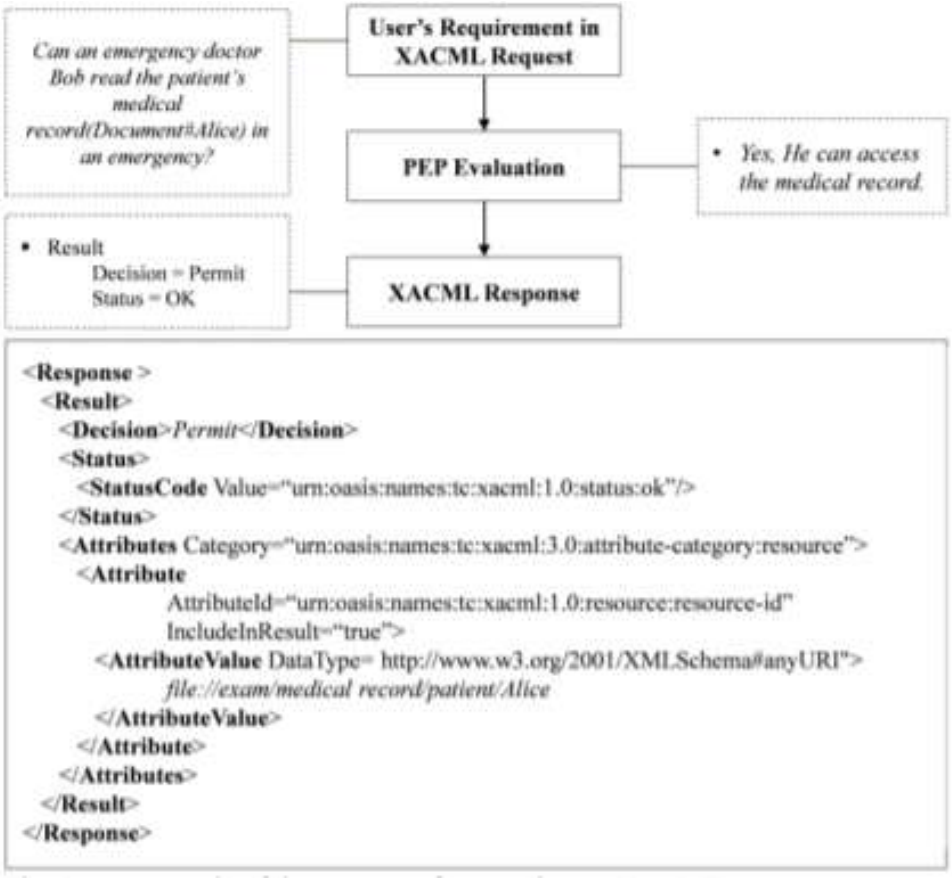


Fig. 5: An example of the method of generating AN XACML response message when analysis within the situation of Fig. 3.

First, for the safety of patient medical documents, we have a tendency to use XML coding to perform partial coding of contents that will infringe upon patient privacy with reference to the initial CDA/CCD text following the access management method. XML coding follows the method conferred in Fig. 6.

First, {the components| the weather} and element content of the CDA/CCD XML document square measure known by parsing before coding. We have a tendency to then classify the factors that will infringe upon patient

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

privacy and choose some of the document for coding. If elements that will infringe upon a personality's privacy square measure selected, then coding is performed on those parts. Within the HIPAA normal, any data in medical records that's accustomed establish people is outlined as letter (e.g., medical records, charge data, insurance data, and insurance information). Letter is formed, used, and exposed throughout the availability of care services and will be exploited to violate the privacy of people. Table three lists the eighteen kinds of identifiers outlined by HIPAA. a number of {the information| the info| the information} listed is closely associated with data that will violate the patient's privacy. In addition, there is also sensitive data that the patient doesn't want to disclose. This data ought to even be partly encrypted and retrieved solely with patient consent, if necessary. Once the coding parts square measure selected, AN coding algorithmic rule is chosen and partial coding is performed exploitation the administrator's personal key.

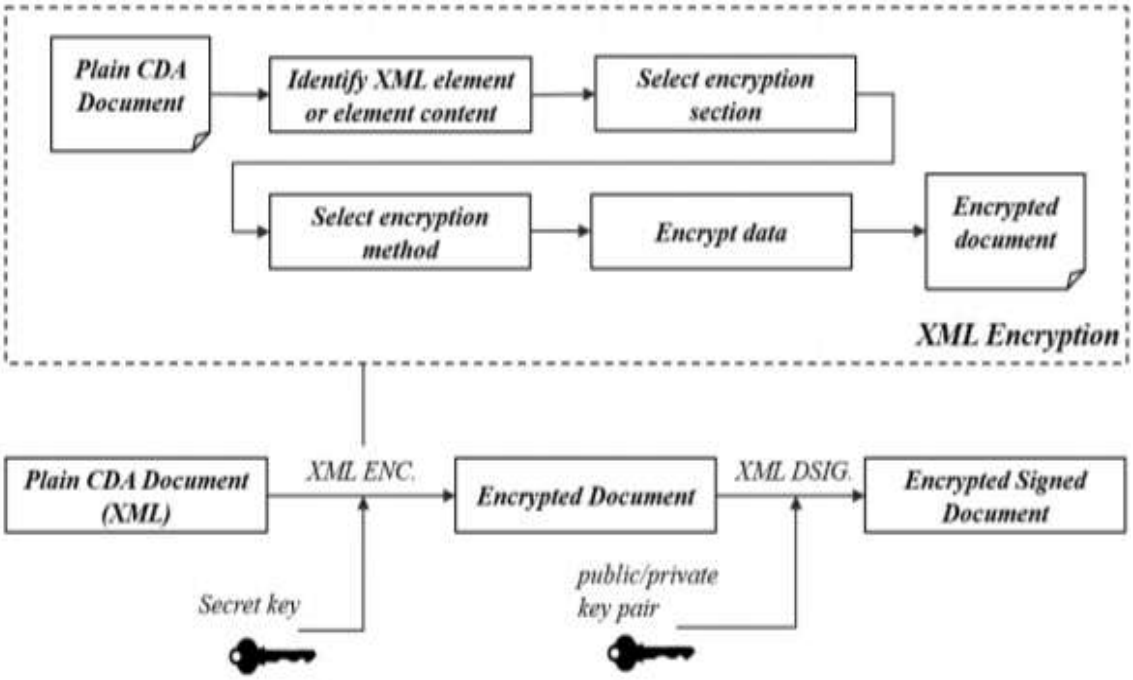


Fig. 6: The process of encrypting medical documents using XML encryption in phase 2 of the proposed model

When the XML partial coding is completed, the XML digital signature is applied. AN electronic signature proves that the person represented because the author truly created the electronic document. It conjointly proves that the contents weren't falsified or altered throughout the causation and receiving process; this prevents the author from later denying the very fact that the electronic document was created. The utilization of AN XML digital signature is illustrated in Fig. 7.

The first step is to see the kind of digital signature to be used. There square measure 3 kinds of XML digital signatures: AN close signature, enclosed signature, and detached signature. For AN close signature, the topic information exists inside the signature structure. This can be advantageous for adding a digital signature to the prepacked information in AN XML payload. For AN enclosed signature, the target information contains the signature structure. This will be accustomed digitally sign all or a part of AN XML document. A detached signature

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

exists outside the information and doesn't have a signature structure. this can be accustomed digitally sign information that exists at a location mere by a URI address. The second step is to make a digest. the information to be signed is given a brand new worth of reduced size by employing a hashing algorithmic rule. This method is termed making a digest. The hash algorithmic rule ought to be designed to provide a similar digest for a similar information and to come up with a very totally different digest worth once a small modification is created to the information. This prevents somebody from acting reverse engineering on the information.

Table III: Patient Sensitive Information for Partial Encrytion

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.*

As a 3rd step, XML canonicalization is performed. Inside a serialized XML document, data are often delineated in a very sort of forms. the subsequent example shows XML representations that have totally different positional representation system string representations, however have a similar meaning:

<name a="1" b="2" c= "3"/>
<name c='3' b='2' a= '1'></name>

during this case, the 2 statements square measure logically equivalent in AN XML document, however don't guarantee equivalent hash values. Standardization is important for logically identical XML documents to be reworked into one piece of physical information. To create AN XML document physically a similar document, the W3C recommends AN XML canonicalization algorithmic rule, which may guarantee ability with XML documents written in several structures. Though the initial one.x version of the XML digital signature failed to totally look after the canonicalization of problems like whitespace or XML namespace notation, XML digital signature a pair of.0 follows canonicalization a pair of.0 to resolve several of the issues in existing versions and improve hardiness.

The final step is to calculate the signature worth. In this process, the digest worth is encrypted exploitation the author's personal key. The user later decrypts the signature worth exploitation the author's public key and compares it to the digest worth to confirm that the signature is valid. If the 2 values don't seem to be a similar, it implies that the document is totally different from the one signed by the author. However, albeit the values square measure totally different, it's inconceivable to grasp what caused the distinction.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

IV. IMPLEMENTATION

In this section, we have a tendency to discuss the implementation of the EHR image for analysis of the planned model. The enforced system is meant to demonstrate the pertinence of the planned model exploitation actual medical information. We have a tendency to conjointly analyze the flow of information by applying the planned XACML access management and XML security method to the present image.

A. Development Surroundings

The system is enforced within the Java net server (JDK8) surroundings [48]. Balana (version one.0.0) was used for the implementation of XACML access management [49]. It's managed by WSO2 and builds upon the Sun XACML a pair of.0 implementation. It's open supply and licenced beneath an Apache license. We have a tendency to leveraged the ASCII text file of the XML security library (version one.2.24) so as to implement XML coding and digital signatures. The library is licenced by Aleksey Sanin (MIT License) [50]. We have a tendency to conjointly used science libraries, as well as the libxml library for XML parsing [51] and OpenSSL for coding [52].

B. Medical Information (MIMIC III)

We used sample information created by touching on the schema and values of the medical data marketplace for medical care III (MIMIC-III) so as to duplicate the information format utilized in hospitals for our implementation [53]. MIMIC-III could be a free crucial care information. MIMIC-III includes health-related information for over forty,000 patients World Health Organization stayed within the medical care unit between 2001 and 2012 at the alphabetic character Israel Protestant deacon eye. The information includes demographics data, patient sign measurements, laboratory check request exploitation the hold on policy.

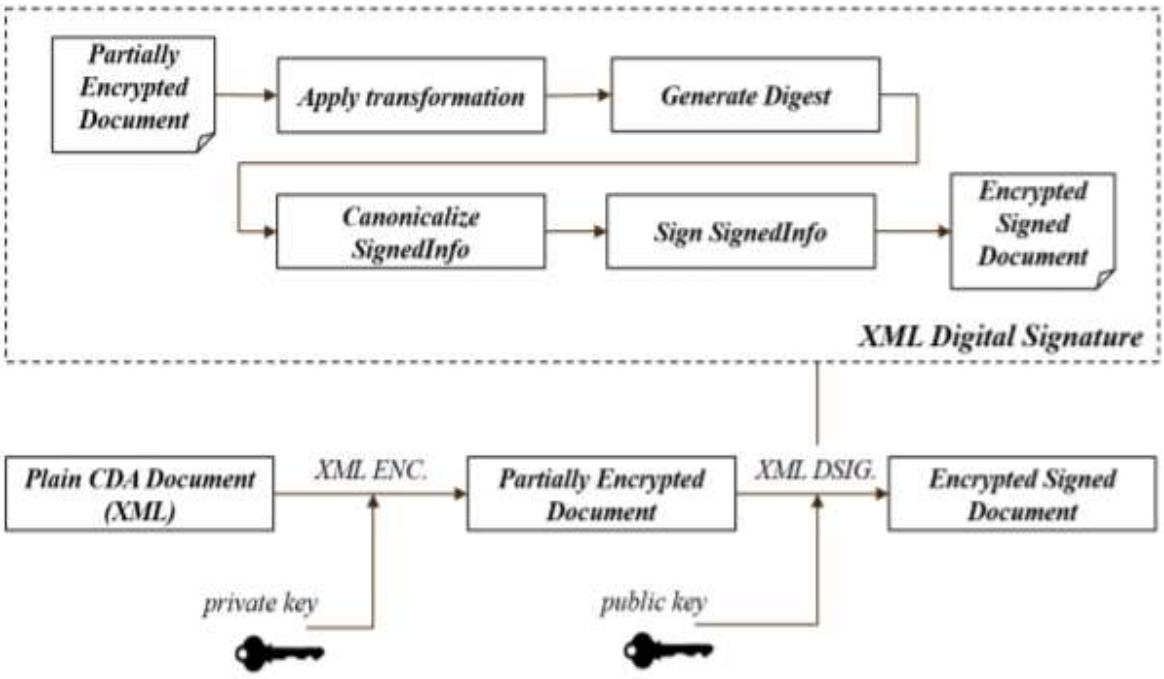


Fig. 7: The Method for Acting AN XML Digital Signature on a Partly Encrypted Medical Document in Fig. 6.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

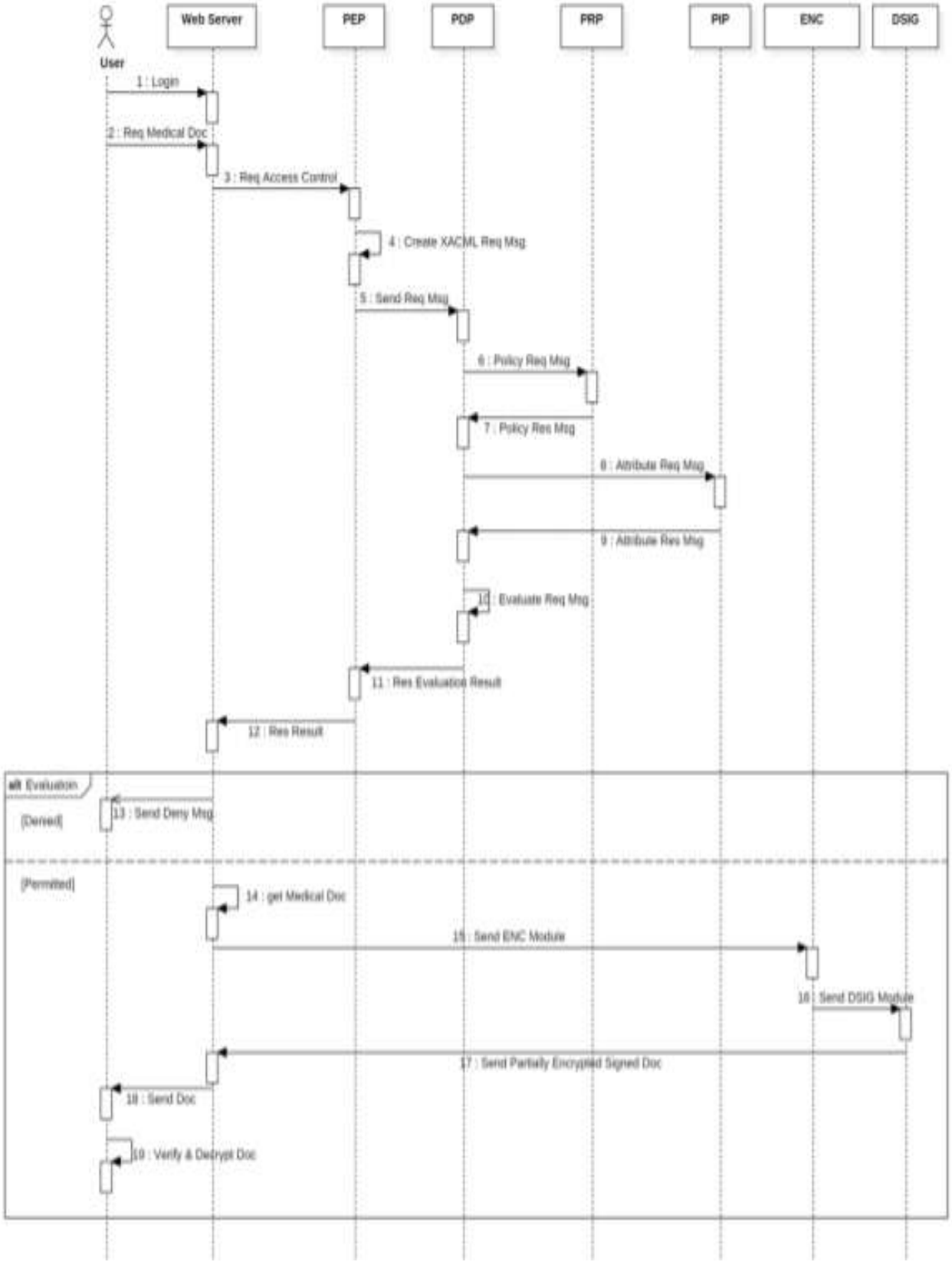


Fig. 8: The UML Sequence Diagram of the Implementation System.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

If the analysis returns denied, the net server sends a message to the user that their request is denied and therefore the method is terminated. If the analysis returns allow, the net server fetches the requested medical data. If there square measure multiple results, procedures, medications, caregiver notes, imaging reports, and mortality data.

Fig. 9: Screenshot of Prototype Application Showing Access Control Part

C. System Style

Because the $64000 EHR system is incredibly giant, there's a limit to the implementation of the system during this study. Thus, we have a tendency to limit the input of user needs so as to alter implementation quality. for instance, a user might choose solely a restricted set of documents or actions. This conjointly simplifies the task of complicated policy style. The key management needed for coding and sign language conjointly uses an area key store so as to scale back implementation quality. Fig. eight presents the UML sequence diagram of the enforced system.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

First, the user should log in to the server to verify their identity. The HIPAA normal specifies distinctive user identification as a demand once acting access management. The user then requests a medical document from the net server. Fig. nine presents the user request portion of the enforced system. once a user selects the specified document and action, ANd sends an access management request through the net server, the ginger generates a corresponding XACML request message.

The request message is distributed to the PDP, that evaluates the user requested documents, the XML security method is performed just for documents that square measure allowable. The model planned during this paper uses a cloud repository to fetch medical information, however the enforced system is meant to fetch medical data from an area store so as to scale back quality.

Table IV: Elements to be Considered for Partial Encrytion

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

In the choose coding Section of the XML coding method, information parts that may infringe upon the privacy of a patient square measure classified. Table four lists the sections that ought to be thought of for partial coding within the MIMIC-III information schema. These embody patient personal data, sickness connected data, and hospital use data.

After the partial coding zone is set, XML coding is performed on the corresponding sections. Finally, a digital signature is additional to confirm the validity of the document. Fig. ten presents the method of encrypting and sign language medical documents within the enforced system. The digital signature and encrypted document square measure then valid and decrypted by the user.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

Fig. 10: The Process of Encrypting and Digitally Signing Medical Documents

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

V. DISCUSSION

We planned AN EHR system model that operates in a very cloud-based surroundings to shield patient privacy. The planned model differs from existing approaches in the main in terms of security. Table five compares the approaches used existing models with the planned model mentioned in section three. We have a tendency to selected recent access management studies associated with patient privacy protection for comparison.

The following 5 security analysis factors were used for comparisons with existing studies:

Authorization: A method of granting or denying a user access to a system. This grants the user permission to access acceptable health information solely.

Confidentiality: Ensures that health information stay confidential and inaccessible to unauthorized users.

Integrity: Ensures that health information don't seem to be changed once delivered to a different party. solely approved users will modification health information.

Accountability: Monitors access to medical information. This permits the system to spot the user World Health Organization performed a selected action and what actions occurred throughout a particular amount.

Non-repudiation: Ensures that the abuse of medical information cannot be denied by proving the very fact when causation or receiving a message.

As shown in Table five, most of the safety EHR modeling

Approaches have issues with totally supporting numerous security activities as a result of they're too centered on a particular activity. Most studies planned a technique for access management that doesn't address the issues of confidentiality and integrity of internal information. as a result of patient information are often attacked in a very sort of manners, multiple security systems square measure needed to shield privacy. during this paper, we have a tendency to satisfy these needs through a two-phase model.

According to Abbas and designer [12], privacy-preserving techniques in e-health comprise 2 categories: science approaches and non-cryptographic approaches (e.g., access control). The model planned during this study falls inside the cluster of science approaches as a result of it contains AN encryption technique. However, the coding technique we have a tendency to use isn't used on to shield a patient's health information privacy, however is a further technique used for secondary protection when access management. Therefore, the planned model is nearer to being a hybrid approach.

As shown in Table five, several existing approaches use RBAC. However, because the numbers of resources and users increase, the RBAC model will increase the amount of roles and policies, leading to a measurability issue [59]. This downside is caused by the static characteristics of RBAC. The ABAC model has been developed to resolve this issue. The ABAC utilized in the planned model could be a a lot of versatile approach than RBAC, therefore enabling a lot of fine-grained access management.

The planned model uses XML digital signatures to confirm information integrity and non-repudiation. Digital signatures give a helpful thanks to prove authentication (for the sender) repudiation [64]. Digital signatures are often

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

accustomed show that a digitally signed document is strictly what the signer meant, which no change of state has occurred within the method of generating, distributing, or storing AN electronic document. it's conjointly doable to perform a non-repudiation perform by checking the content of a message employing a digital signature. in addition, the planned model follows the technical safeguard standards planned by HIPAA and its pertinence was incontestable through image implementation.

VI. CONCLUSION

Recently, EHR systems within the cloud surroundings have shown the potential to enhance the standard of medical service by sharing and utilizing patient information across numerous medical establishments. However, this surroundings creates further security risks and patient privacy are often desecrated by numerous malicious attacks. Despite the importance of information security, several systems don't take into account security factors throughout their modeling method or regard them as minor factors.

We planned a cloud-based EHR model that guarantees patient privacy. The planned model is split into 2 stages: access management, and therefore the application of coding and digital signatures. The planned model uses AN ABAC methodology engineered upon XACML. When acting access management on patient documents, coding is performed and digital signatures ar} additional exploitation XML coding and XML digital signatures as an extra security measure. The planned model provides a lot of versatile and fine-grained management than existing RBAC systems and alleviates the danger of exposing patient privacy data by exploitation partial coding and electronic signatures. The implementation of a image incontestable the practicability of the planned model. we have a tendency to compared the enforced security factors with those utilized in different connected studies and determined that the planned methodology is superior to previous ways in terms of security.

In the future, we'll any refine the processes utilized in the planned model and implement further security measures. we'll conjointly expand the implementation of the image to implement a a lot of refined system and perform quantitative performance analysis.

ACKNOWLEDGEMENT

This work was supported by Institute for data Promotion (IITP) grant funded by the Korean Peninsula government (MSIT) (No.2017-0-00756, Development of ability and management technology of IoT system with heterogeneous ID mechanism). The co-corresponding authors square measure Doo-Kwon Baik and Young-Gab Kim.

REFERENCES

[1] Tang, P.C., Ash, J.S., Bates, D.W., Overhage, J.M., & Sands, D.Z. (2006). Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association,* [Online]. 13(2), 121-126.

[2] Waegemann, C.P. (2003). Ehr vs. cpr vs. emr. Healthcare Informatics Online, [Online]. 1, 1-4. Available: https://pdfs.semanticscholar.org/ce2f/cf783c1fa2afdaa81c5a46c317e7ed ff04bc.pdf

[3] van der Linden, H., Kalra, D., Hasman, A., &Talmon, J. (2009). Interorganizational future proof EHR systems: a review of the security and privacy related issues. International journal of medical informatics, [Online]. 78(3), 141-160. Available: http://www.sciencedirect.com/science/article/pii/S1386505608001081

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

[4] Tang, P. C. (2003). Key capabilities of an electronic health record system. Washington, DC, Institute of Medicine of the National Academies. [Online]. Available: http://www.nationalacademies.org/hmd/Reports/2003/Key-Capabilitiesof-an-Electronic-Health-Record-System.aspx

[5] Miller, R.H., West, C., Brown, T.M., Sim, I., & Ganchoff, C. (2005). The value of electronic health records in solo or small group practices. *Health Affairs,* [Online]. 24(5), 1127-1137.

[6] Middleton, B., Bloomrosen, M., Dente, M.A., Hashmat, B., Koppel, R., Overhage, J.M., & Zhang, J. (2013). Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA. *Journal of the American Medical Informatics Association,* [Online]. 20(e1), e2-e8.

[7] Simon, S.R., Kaushal, R., Cleary, P.D., Jenter, C.A., Volk, L.A., Poon, E.G., & Bates, D.W. (2007). Correlates of electronic health record adoption in office practices: a statewide survey. *Journal of the American Medical Informatics Association,* [Online]. 14(1), 110-117.

[8] Ratnam, K.A., & Dominic, P.D.D. (2012, June). Cloud servicesEnhancing the Malaysian healthcare sector. In Computer & Information Science (ICCIS), 2012 International Conference on. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6297101/

[9] Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/5557983/

[10] Benaloh, J., Chase, M., Horvitz, E., &Lauter, K. (2009, Nov.). Patient controlled encryption: ensuring privacy of electronic medical records. In Proceedings of the 2009 ACM workshop on Cloud computing security. [Online]. Available: http://dl.acm.org/citation.cfm?id=1655024

[11] Ray, P., &Wimalasiri, J. (2006, Aug.). The need for technical solutions for maintaining the privacy of EHR. In Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/4462848/

[12] Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacypreserving approaches in the e-health clouds. IEEE Journal of Biomedical and Health Informatics, [Online]. 18(4), 1431-1441.

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

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

[15] Standards for Privacy of Individually Identifiable Health Information: Final Rule. Dec. 28, 2000.

[16] openEHR Community: openEHR, Available: http://www.openehr.org

[17] HL7: Health level 7 (HL7), Available: http://www.hl7.org

[18] Dolin, R.H., Alschuler, L., Boyer, S., Beebe, C., Behlen, F.M., Biron, P.V.: Hl7 clinical document architecture, release 2.0. ANSI Standard (2004)

[19] C 32 - HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component. Available: http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&Prefi xNumeric=32

[20] HITECH Act enforcement interim final rule. US Department of Health and Human Services. 2013

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

[22] Pussewalage, H.S.G., & Oleshchuk, V.A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management,* [Online]. 36(6), 1161-1173.

[23] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P.Á.O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics,* [Online]. 46(3), 541- 562.

[24] Anwar, M., Joshi, J., & Tan, J. (2015). Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges. Health Policy and Technology, [Online]. 4(4), 299-311.

[25] Bhuyan, S., Kim, H., Isehunwa, O.O., Kumar, N., Bhatt, J., Wyant, D. K., Dasgupta, D. (2017). Privacy and security issues in mobile health: current research and future directions. Health Policy and Technology. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2211883717300047

[26] Camara, C., Peris-Lopez, P., &Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of biomedical informatics, [Online]. 55, 272-289.

[27] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., &Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal, [Online]. 18(2), 113-122.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

[28] Bahga, A., & Madisetti, V.K. (2013). A cloud-based approach for interoperable electronic health records (EHRs). *IEEE Journal of Biomedical and Health Informatics.* [Online]. 17(5), 894-906.

[29] Hsieh, G., & Chen, R. J. (2012, Dec.). Design for a secure interoperable cloud-based Personal Health Record service. In Cloud Computing Technology and Science (CloudCom), 2012 *IEEE 4th International Conference on*. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6427582/

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

[31] Rezaeibagha, F., & Mu, Y. (2016). Distributed clinical data sharing via dynamic access-control policy transformation. *International journal of medical informatics.* [Online]. 89, 25-31.

[32] Premarathne, U., Abuadbba, A., Alabdulatif, A., Khalil, I., Tari, Z., Zomaya, A., &Buyya, R. (2016). Hybrid cryptographic access control for cloud-based EHR systems. *IEEE Cloud Computing.* [Online]. 3(4), 58-64.

[33] Peleg, M., Beimel, D., Dori, D., & Denekamp, Y. (2008). Situation-based access control: Privacy management via modeling of patient data access scenarios. Journal of biomedical informatics. [Online]. 41(6), 1028-1040.

[34] Gajanayake, R., Iannella, R., & Sahama, T. (2014). Privacy oriented access control for electronic health records. *Electronic Journal of Health Informatics.* [Online]. 8(2), 15.

[35] Lunardelli, A., Matteucci, I., Mori, P., & Petrocchi, M. (2013, June). A prototype for solving conflicts in XACML-based e-Health policies. *In Computer-Based Medical Systems (CBMS),* 2013 IEEE 26th *International Symposium on*. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6627838/

[36] Calvillo-Arbizu, J., Roman-Martinez, I., &Roa-Romero, L. M. (2014, June). Standardized access control mechanisms for protecting ISO 13606- based electronic health record systems. *In Biomedical and Health Informatics (BHI), 2014 IEEE-EMBS International Conference on*. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6864421/

[37] Gope, P., & Amin, R. (2016). A novel reference security model with the situation based access policy for accessing ephr data. *Journal of medical systems,* [Online]. 40(11), 242.

[38] Alshehri, S., Radziszowski, S. P., & Raj, R. K. (2012, April). Secure access for healthcare data in the cloud using ciphertext-policy attributebased encryption. In Data Engineering Workshops (ICDEW), 2012 *IEEE 28th International Conference on* (pp. 143-146). IEEE. [Online].

[39] Yang, K., Liu, Z., Jia, X., & Shen, X. S. (2016). Time-domain attributebased access control for cloud-based video content sharing: A cryptographic approach. *IEEE Transactions on Multimedia,* [Online] 18(5), 940-950.

[40] Chen, Y.Y., Lu, J.C., & Jan, J. K. (2012). A secure EHR system based on hybrid clouds. *Journal of medical systems,* [Online]. 36(5), 3375-3384.

[41] Mohandas, A. (2014, October). Privacy preserving content disclosure for enabling sharing of electronic health records in cloud computing. In Proceedings of the 7th ACM India Computing Conference (p. 7). ACM. [Online]. Available: https://dl.acm.org/citation.cfm?id=2675753

[42] Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects of privacy for electronic health records. *International journal of medical informatics,* [Online]. 80(2), e26-e31.

[43] Fong, P.W. (2011, February). Relationship-based access control: protection model and policy language. In Proceedings of the first ACM conference on Data and application security and privacy (pp. 191-202). ACM. [Online]. Available: https://dl.acm.org/citation.cfm?id=1943539

[44] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attributebased encryption. *IEEE transactions on parallel and distributed systems,* [Online]. 24(1), 131-143.

[45] Chen, Y.Y., Lu, J.C., & Jan, J.K. (2012). A secure EHR system based on hybrid clouds. Journal of medical systems, [Online]. 36(5), 3375-3384.

[46] Abomhara, M., Yang, H., &Køien, G. M. (2016, October). Access control model for cooperative healthcare environments: Modeling and verification. *In Healthcare Informatics (ICHI),* 2016 *IEEE International Conference on* (pp. 46-54). IEEE. [Online].

[47] Sicuranza, M., & Esposito, A. (2013, December). An access control model for easy management of patient privacy in EHR systems. *In Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for* (pp. 463-470). IEEE. [Online].

[48] Oracle's Java SE Development Kit 8, Available: http://docs.oracle.com/javase/8/docs/

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

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

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

[51] Libxml2 Library, Available: http://xmlsoft.org/downloads.html
[52] OpenSSL 1.1.0e Library, OpenSSL Software Foundation,16 Feb 2017, https://www.openssl.org
[53] Johnson, A. E., Pollard, T. J., Shen, L., Lehman, L. W. H., Feng, M., Ghassemi, M., & Mark, R. G. (2016). MIMIC-III, a freely accessible critical care database. Scientific data, 3. Available: https://www.ncbi.nlm. nih.gov/pmc/articles/PMC4878278/
[54] VistA Monograph (2012) [Online]. Available: www.va.gov/vista monograph
[55] Neubauer, T., &Heurix, J. (2011). A methodology for the pseudonymization of medical data. *International journal of medical informatics*, [Online]. 80(3), 190-204.
[56] Sandıkkaya, M.T., De Decker, B., & Naessens, V. (2010, December). Privacy in commercial medical storage systems. In International Conference on Electronic Healthcare (pp. 247-258). Springer, Berlin, Heidelberg. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-23635-8_32
[57] Sharma, S., & Balasubramanian, V. (2014, November). A biometric based authentication and encryption Framework for Sensor Health Data in Cloud. In Information Technology and Multimedia (ICIMU), 2014 Internatio nal Conference on (pp. 49-54). IEEE. [Online].
[58] Au, R., &Croll, P. (2008, January). Consumer-centric and privacy preserving identity management for distributed e-health systems. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual (pp. 234-234). IEEE. [Online].
[59] Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000, July). The NIST model for role-based access control: towards a unified standard. In ACM workshop on Role-based access control. [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] Sahai, A., & Waters, B. (2005, May). Fuzzy identity-based encryption. *In Eurocrypt.* [Online]. 3494, 457-473.
[62] Wang, C., Liu, X., & Li, W. (2013). Design and implementation of a secure cloud-based personal health record system using ciphertext-policy attribute-based encryption. *International Journal of Intelligent Information and Database Systems*, [Online]. 7(5), 389-399.
[63] Lin, H., Shao, J., Zhang, C., & Fang, Y. (2013). CAM: cloud-assisted privacy preserving mobile health monitoring. *IEEE Transactions on Information Forensics and Security*, [Online]. 8(6), 985-997.
[64] Lakshmi, R.N., Laavanya, R., Meenakshi, M., & Dhas, C.S.G. (2015). Analysis of Attribute Based Encryption Schemes. *International Journal of Computer Science and Engineering*, [Online]. 3(3), 1076-1081.
[65] Kaur, R., & Kaur, A. (2012, September). Digital signature. *In Computing Sciences (ICCS)*, 2012 International Conference on (pp. 295-301). IEEE. [Online]. A
[66] Rajendran T et al. "Recent Innovations in Soft Computing Applications", *Current Signal Transduction Therapy.* Vol. 14, No. 2, pp. 129 – 130, 2019.
[67] Emayavaramban G et al. "Indentifying User Suitability in sEMG based Hand Prosthesis for using Neural Networks", Current Signal Transduction Therapy. Vol. 14, No. 2, pp. 158 – 164, 2019.
[68] Rajendran T & Sridhar KP. "Epileptic seizure classification using feed forward neural network based on parametric features". *International Journal of Pharmaceutical Research.* 10(4): 189-196, 2018.
[69] Hariraj V et al. "Fuzzy multi-layer SVM classification of breast cancer mammogram images", *International Journal of Mechanical Engineering and Technology*, Vol. 9, No.8, pp. 1281-1299, 2018.
[70] Muthu F et al. "Design of CMOS 8-bit parallel adder energy efficient structure using SR-CPL logic style". *Pakistan Journal of Biotechnology.* Vol. 14, No. Special Issue II, pp. 257-260, 2017.
[71] Keerthivasan S et al. "Design of low intricate 10-bit current steering digital to analog converter circuitry using full swing GDI". *Pakistan Journal of Biotechnology.* Vol. 14, No. Special Issue II, pp. 204-208, 2017.
[72] Vijayakumar P et al. "Efficient implementation of decoder using modified soft decoding algorithm in Golay (24, 12) code". *Pakistan Journal of Biotechnology.* Vol. 14, No. Special Issue II, pp. 200-203, 2017.
[73] Rajendran T et al. "Performance analysis of fuzzy multilayer support vector machine for epileptic seizure disorder classification using auto regression features". *Open Biomedical Engineering Journal.* Vol. 13, pp. 103-113, 2019.
[74] Rajendran T et al. "Advanced algorithms for medical image processing". *Open Biomedical Engineering Journal*, Vol. 13, 102, 2019.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020

[75] Anitha T et al. "Brain-computer interface for persons with motor disabilities - A review". *Open Biomedical Engineering Journal*, Vol. 13, pp. 127-133, 2019.

[76] Yuvaraj P et al. "Design of 4-bit multiplexer using sub-threshold adiabatic logic (stal)". *Pakistan Journal of Biotechnology*. Vol. 14, No. Special Issue II, pp. 261-264, 2017.

DOI: 10.37200/IJPR/V24I5/PR2020286
Received: 18 Mar 2020 | Revised: 30 Mar 2020 | Accepted: 08 Apr 2020