# Understanding Attribute-based Access Control for Modelling and Analysing Healthcare Professionals' Security Practices

Livinus Obiora Nweke[1]
Information Security and Communication Technology
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway

Prosper Yeng[2]
Information Security and Communication Technology
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway

Stephen D. Wolthusen[3]
School of Mathematics and Information Security
Royal Holloway, University of London
Egham, United Kingdom
Information Security and Communication and Technology
Norwegain University of Science and Technology (NTNU)
Gjøvik, Norway

Bian Yang[4]
Information Security and Communication Technology
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway

***Abstract*—In recent years, there has been an increase in the application of attribute-based access control (ABAC) in electronic health (e-health) systems. E-health systems are used to store a patient's electronic version of medical records. These records are usually classified according to their usage i.e., electronic health record (EHR) and personal health record (PHR). EHRs are electronic medical records held by the healthcare providers, while PHRs are electronic medical records held by the patients themselves. Both EHRs and PHRs are critical assets that require access control mechanism to regulate the manner in which they are accessed. ABAC has demonstrated to be an efficient and effective approach for providing fine grained access control to these critical assets. In this paper, we conduct a survey of the existing literature on the application of ABAC in e-health systems to understand the suitability of ABAC for e-health systems and the possibility of using ABAC access logs for observing, modelling and analysing security practices of healthcare professionals. We categorize the existing works according to the application of ABAC in PHR and EHR. We then present a discussion on the lessons learned and outline future challenges. This can serve as a basis for selecting and further advancing the use of ABAC in e-health systems.**

***Keywords*—Attribute-Based Access Control (ABAC); e-health systems; Personal Health Record (PHR); Electronic Health Record (EHR)**

## I. Introduction

There has been a growing interest in the application of ABAC in e-health systems. This is evident by the increasing number of publications and on-going research activities in that direction. According to Gartner report [1] it is predicted that 70% of enterprises will adopt ABAC mechanism as the most dominant access control mechanism for the protection of critical assets. In the healthcare industry, e-health systems interact with critical assets like electronic medical records, and ABAC has been shown to offer a promising approach to securing these critical assets.

Traditionally, medical records are paper-based but tremendous progresses in information and communication technology have led to a shift from paper-based medical records to electronic version of the medical records. Like the traditional paper-based medical record, electronic version of the medical record is a collection of medical history of an individual. However, unlike the traditional paper-based medical records, the electronic version is stored in electronic format following the required standards.

The electronic version of medical records is usually classified according to their usage i.e., electronic health record (EHR) and personal health record (PHR). Whilst EHRs are electronic medical records of an individual held by the healthcare providers; PHRs are referred to as electronic medical records of an individual held by the individual themselves. Although EHRs can be shared across different healthcare providers, PHRs have shown to be an effective approach for individuals to share their electronic medical records with different healthcare providers, family and friends.

Sharing of electronic medical records raises security and privacy concerns for both EHR and PHR. For EHR, healthcare providers are required by regulatory bodies to ensure that the security and privacy of the electronic medical records are maintained. In the case of PHR, an individual would want to ensure that only authorized entities have access to their electronic medical records. Several approaches have been proposed to address the security and privacy concerns raised by EHR and PHR. The approach that have received wide-spread acceptance is ABAC.

ABAC aims to provide fine-grained access to a resource or an object based on the attributes of the subject and that of the object; in addition to the environmental conditions. A subject refers to an entity such as a person, process or device that wishes to access a resource or an object. A resource or an

object is a system-related entity containing information such as records, that a subject desires to access. The environmental conditions are the operational contexts such as the time and location of access. Hence, in ABAC, the attributes of the subject and the requested object as well as the environmental condition determines the set of operations that can be executed on the requested object.

A wide range of applications of ABAC in e-health systems have been proposed in the literature and examined in individual studies. However, a comprehensive survey of these techniques that can serve as a basis for selecting and further advancing the use of ABAC in e-health systems is still missing in the literature. Abbbas and Khan in [2] presented a review on the state of the art in privacy preserving techniques for e-health cloud based systems. The authors in [3], [4] provided a survey on the security and privacy issues in e-health cloud based systems. To the best of our knowledge, there is no survey on the application of ABAC in e-health systems.

In this paper, we present a survey on the application of ABAC in e-health systems. We categorize the different applications of ABAC in e-health systems according to those use in PHR and those apply in EHR. We present a comparison of the different approaches employ in the existing works. Then, using some of the key features of the existing approaches, we present a discussion on their differences. Also, we describe the lessons learned from the survey and outline future challenge. Lastly, the concept of modelling and analysing healthcare professionals' security practices is discussed.

The rest of this paper is organised as follows. Section II presents an overview of the security and privacy requirements for e-health systems. Also, the dominant access control mechanisms deploy in e-health systems are explored, and the justification for wide-spread acceptance of ABAC in e-health systems is described. Section III presents a literature survey of the existing works on the application of ABAC in e-health systems. Section IV discusses the lessons learned from the survey and outline future challenge. In addition a discussion on modelling and analysing healthcare professionals' security practices is presented. Section V concludes the paper.

## II. Background

In this section, we provide an overview of the security and privacy requirements for e-health systems. We also examine the commonly used access control measures for e-health systems and why ABAC mechanism is the most preferred access control mechanism for e-health systems.

### A. Requirements of E-Health Systems

Several standards and laws have been proposed to specify the security and privacy requirements for e-health systems. The most popular of these standards and laws is the American standard health insurance portability and accountability act (HIPAA) [5]. HIPAA is mainly concern about the privacy and security of patient health information (PHI). With the migration of PHI from paper-based to electronic format, HIPAA was upgraded to health information technology for economic and clinical health (HITECH) to address privacy and security concerns posed by such migration.

HIPAA is applicable to all types of Covered Entity or Business Associate that processes PHI. Covered Entity is a health care provider, a health plan or a health care clearing house who, in its normal activities, creates, maintains or transmits PHI [5]. Business Associate is a person or business that provide a service - or performs certain function or activity for - a covered entity when that service, function or activity involves the business associate having access to PHI maintained by the covered entity [5]. Usually, a business associate is required to sign business associate agreement with the Covered Entity stating what PHI they can access, how it would be used and that it will be returned or destroyed once the task it is needed for is completed [5]. Also, while the PHI is in the custody of the business associate, the business associate has the same HIPAA compliance obligations as a Covered Entity.

The two types of rules specified by HIPAA are the privacy rule and security rule. The privacy rule protects all PHI held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral [5]. Under the security rule, covered entities are required to evaluate risks and vulnerabilities in their environments and to implement security controls to address those risks and vulnerabilities [6]. There are three parts to the security rule: administrative safeguards, which is in the form of policies and procedures that brings the privacy rule and security rule together; technical safeguards refer to the technology that is used to protect PHI and provide access to the data; and physical safeguards, which has to do with physical access to PHI regardless of its location [6].

An international standard that defines the requirements for e-health systems is the ISO/IEC 27799 [7]. The ISO/IEC 27799 provides special recommendations on security needs in the healthcare sector, taking into account the unique nature of its operating environment. It applies ISO/IEC 27002 to the healthcare domain with appropriate security controls towards enhancing the protection of PHI. The development of ISO/IEC 27799 took into consideration, personal data protection legislations, privacy and security best practices, individual and organizational accountability, meeting the security needs identified in common healthcare situations, and operating electronic health information systems in an adequately secured healthcare environment. Also, ISO/IEC 27799 aims to protect information such as PHI, pseudonymized data derived from PHI, clinical or medical knowledge related or not related to any patient, data on health professionals, staff and volunteers, audit trail data produced by health information systems, including access control data and other security related system configuration data, for health information systems.

Other important standards for e-health systems include OpenEHR [8], the health level 7 clinical document architecture (CDA) [9], and the continuity of care document (CCD) [9]. The OpenEHR is an open standard that specifies the management and storage, retrieval and exchange of health data in EHRs. Also, openEHR defines specifications for clinical information models, EHR Extracts, demographics, data types and various kinds of service interfaces [8]. The HL7 CDA is a document markup standard that specifies the structure and semantics of clinical documents for the purpose of facilitating exchange between healthcare providers and patients [9]. A clinical document is defined by HL7 CDA as having the following features: persistence, stewardship, potential for

authentication, context, wholeness, and human readability [9]. And CCD is a joint effort of HL7 International and American society for testing and materials (ASTM) to enable interoperability of clinical data [9]. It allows physicians to send electronic medical information to other providers without loss of meaning and as such, improves the overall patient care.

In general, the requirements that are of interest to this survey are the recommended technical safeguards for e-health systems. These technical safeguards aim to provide secure, reliable, access to PHR or EHR; where and when it is requested. The requirements include the following [5]:

- Implement a means of access control
- Introduce a mechanism to authenticate PHR and EHR
- Implement tools for encryption and decryption
- Introduce activity logs and audit controls

### B. Access Control Mechanisms

One of the security controls necessary to meet the security and privacy requirements for e-health systems is the implementation of access control mechanisms. These are measures that can be used to regulate access to a given resource. Earlier implementation of access control mechanisms in e-health systems employ role-based access control (RBAC) [2]. RBAC restricts access to a resource based on the user's role. The use of a role based access control suffers some drawbacks as the definition of roles is static and it lacks flexibility and responsiveness. Every user needs to be enrolled in advance in the system. For example, in an emergency situation where the patient is outside the local domain where the patient health information held, a doctor not registered within the local domain of the patient will not be able to access the patient's health information. Therefore, the efficacy of role-based access control is limited because it cannot handle situations where unregistered personnel requires access to the system as in the case of emergency that we described.

Emergency access such as self-authorization and break the glass (BTG) are basic requirements in healthcare systems. Self-authorization is a provision in the access control mechanism that allows healthcare professionals to access the minimum and necessary healthcare records for therapeutic purposes during emergency situations. Similarly, BTG mechanism is used when conventional access control mechanisms are inadequate to access minimum and necessary healthcare information for therapeutic measures [10], [11]. Considering that RBAC policies rely on permissions that does not often change [12], installing emergency access mechanisms on static roles may pose a high security threat. For instance, an adversary who might have unlawfully acquired health professionals' credentials under RBAC, could easily compromise healthcare records by using the emergency access control windows since there are no other control variables to authentic the accesses of the malicious user.

A flexible access control mechanism that provides fine grained access control to a resource is ABAC. Like RBAC, ABAC employs a policy driven approach. However, in ABAC, access to a resource is granted based on the attributes of the subjects and the objects together with the environmental attributes. This eliminates the need of having to register a user into the system before providing access; instead, access is granted based on the attributes of the user and that of the requested resource. Thus, ABAC mechanisms would provide appropriate level of access to healthcare records even for any extraordinary actions that need to be taken during emergency situations.

For emergency situations, ABAC ensures that the authentication mechanism of emergency accesses can be configured to include more control variables such as attributes of the user, environment and resources to reduce risk of privacy and security breaches. For instance, the resource and environmental attributes such as the patient status and location could indicate emergency care or intensive-care services. Hence, any accesses other than the specified attributes would be restricted, to reduce the risk of exploitation. Therefore, ABAC policies enables flexible configurations for users to override their conventional access restrictions in a controlled and justifiable manner in emergency access scenarios.

ABAC have shown to be an effective and efficient mechanism for providing fine-grained access to PHRs and EHRs given the dynamic nature of today's e-health environment. Also, it can be combined with different cryptographic schemes to provide secure and anonymous sharing of PHRs and EHRs among healthcare providers and patients. So many research efforts are on-going in developing appropriate ABAC model for e-health systems. The next section provides a survey of some of these efforts to further support the assertion that ABAC is a much better access control mechanism for e-health systems.

## III. Literature Survey

In this section, we present a survey of the existing literature on the application of ABAC in e-health systems. We categorize the existing work according to the type of patient's electronic version of medical records considered. Already we have observed that the electronic version of a patient health record is usually classified according to those held by the patient themselves (PHR) and those held by the healthcare providers (EHR). We use this understanding to present the different applications of ABAC in e-health systems.

### A. Application of ABAC in Personal Health Record (PHR)

PHR offers a flexible and convenient way for storing and sharing a patient's electronic version of medical records. It empowers the patients by giving them control over their medical record and deciding with whom to share those records. However, the current trend in the storage of PHR has shown that cloud platforms are very popular way of storing PHR. This raises questions of security and privacy of PHR as there have been wide spread concerns that PHR stored in the cloud may be exposed to unauthorized parties. Several approaches that use ABAC in PHR have been proposed in the literature to address these concerns.

A typical use case scenario of the application of ABAC in PHR is shown in Figure 1. Li et al [13] describe a unified fine-grained access control for PHR in cloud computing. In this system, the patient utilizes the cloud storage platform for storing the encrypted version their PHRs. The policy manager

facilitates the encryption of the patient's PHRs. Also, the medical staff is able to download the encrypted PHRs from the cloud and use their private keys to decrypt the PHRs. A trusted attribute authority is used for all patients and medical staff to authenticate and verify their attributes.

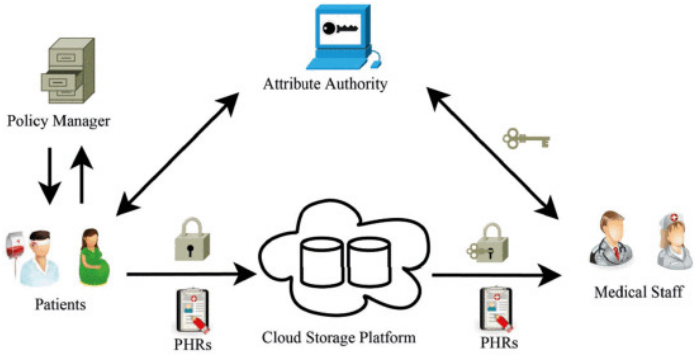


Fig. 1. Use Case Scenario of ABAC in PHR

[13]

One of the earliest approaches in the use of ABAC to provide security and privacy for PHR stored in the cloud is presented in [14]. The authors used a variant of attribute-based encryption (ABE) referred to as broadcast ciphertext policy ABE (bABE) which extends the functionality of ABE to include user revocation. An ABE uses a public key encryption system, where each user's key is labelled with a set of attributes, and the ciphertext is linked with an access policy. The private key of the user can decrypt the ciphertext only if the attribute set of the user's key matches the access policy associated with the ciphertext. Furthermore, the approach presented assumes trusted cloud provider and the use of a trusted authority to issue the relevant private keys.

Li et al in [15] propose a patient-centric framework and approach which exploits ABE techniques to provide fine-grained access control to PHR in cloud environment. In the proposed model, the system is divided into several security domains according to the different users' data access requirements. ABE is deployed to cryptographically enforce patient centric PHR access. In additional, the PHR is assumed to be stored on a semi-trusted service provider and the proposed framework supports access revocation. Another patient-centric cloud-based secured PHR system is presented in [16]. The proposed system enables secure storage of PHR data on a semi-trusted cloud service provider and allows the patient to selectively share their PHR data with wide range of users. The authors reduced key management complexity for both owners and users by dividing the users into two security domains, namely: public domain and personal domain. Also, they show that PHR owners can encrypt PHR data for the public domain using ciphertext-policy ABE scheme, while the PHR data for the personal domain can be encrypted using anonymous multi-receiver identity encryption scheme.

A fine-grained access of interactive, PHR, that extends a secure composite document format i.e., Publicly Posted Composite Documents (PPCD) is described in [17]. PPCD is a SQLite-based serialization which is developed for business workflows and is able to contain multiple documents of different sensitivity and formatting. The method proposed in this work includes both the original PPCD-type and an additional new entry table to provide for password-based and private key access. The authors employ Password Key Derivation function as the privacy preserving technique and the method also supports access revocation. Ray et al in [18] apply attribute based access control for preserving the privacy of PHR. The authors show how the privacy of PHR can be expressed and enforced through the use of an attribute based access control supported by extensible access control markup language (XACML). In this paper, the XACML is used to model the different types of policies and expressing the patient's privacy preference for subsequent enforcement by the attribute based access policies.

There are constraints imposed on cloud based PHR schemes that use ABE. An approach to address these constraints is proposed in [19]. The method adopted in this work involves the use of multi-authority system architecture, unlike existing methods that utilize single trusted authority. In addition, a proxy re-encryption scheme is deployed to ensure that only authorized users are able to decrypt the required PHR files. A more recent work by Li et al [13] present a unified fine-grained access control for PHR in cloud environment. The proposed approach is able to store PHR for multiple patients. It consists of ABE layer and symmetric layer. Whilst the ABE layer facilitates a multi-privilege access control for PHR from multiple patients; in the symmetric layer, symmetric keys that match medical workers' access privileges and the keys with higher privilege can override keys with lower privilege but not the other way around. Also, the authors use ciphertext policy ABE as the privacy preserving technique for the proposed method.

### *B. Application of ABAC in Electronic Health Record (EHR)*

EHR is handled by healthcare providers and also, it provides them with the opportunity of sharing those records among different healthcare providers. EHR is usually stored on-premise under the administrative control of the healthcare provider but recent trends have shown a gradual shift from on-premise storage of EHR to cloud. This further increases the risk of exposing EHR to unauthorized parties. However, ABAC has demonstrated to be a promising approach to mitigating the risk of exposing EHR to unauthorized parties. Different methods that employ ABAC in EHR have been discussed in existing works.

The system architecture as shown in Figure 2, depicts a use case scenario of the application of ABAC in EHR. Joshi et al [20] in this work provide users access to the system using Access Broker Unit. The Access Broker Unit consists of the organizational Knowledge Base, the Rule Based Engine and the Policy Unit. The Organization Knowledge Base stores all the details of the users in the form of an ontology - the EHR Ontology. The Policy Unit stores all the access policies. And the Rule Based Engine uses the user and document attributes from the ontology for implementing the access control policies. The authors use ABE for encryption, and the Key Generation Unit generates the private keys required for the ABE. Then, the encrypted data are stored in the cloud, which hosts, the EHR Ontology.

Pussewalage and Oleshchuk in [21] propose an ABAC scheme for secure sharing of EHR. The scheme uses selective

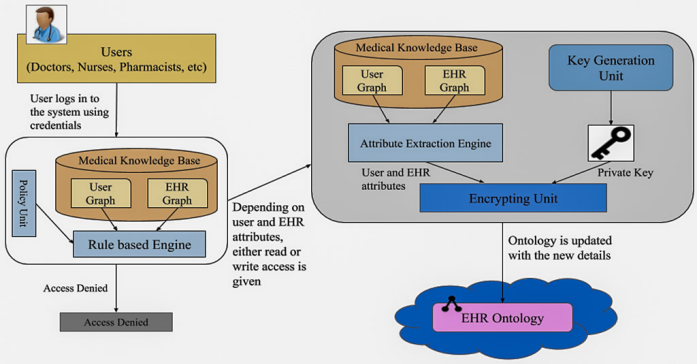


Fig. 2. Use Case Scenario of ABAC in EHR

[20]

disclosure that meets the security requirement of EHR. An access requester supplies a valid set of attributes that satisfies the underlying policy of the requested object using attribute and private key commitments. The proposed approach is said to be collision resistant; such that it is impossible to collude attributes of more than one user to gain access to EHR. This is achieved by giving a unique identifier to every user and including it to every attribute key owned by the respective users. In addition, the proposed method supports on demand user revocation and it is applicable to on-premise storage platform.

Several standards have been developed to facilitate interoperability of EHR. The most recent effort in that direction is the Fast Health Interoperability Resources (FHIR) [22], which specifies requirements for fast and efficient storage/retrieval of EHR. The authors in [23] exploit ABAC to create owner-centric methodology for granting access to EHR. They focussed on FHIR and suggested ways to allow incremental and batch release of EHR stored using FHIR to any requesting party, based on access policies defined by the resource-owners.

Cloud based storage are currently being adopted by healthcare providers for storing EHR. Joshi et al. in [20] develop an ABAC mechanism for cloud-based EHR that uses ABE to securely store EHR at field level. The developed system extracts the user and EHR filed attribute from a HIPAA complaint knowledge graph which facilitates easy querying and faster data access operation. Also, in [24] the authors propose ABAC which uses Hidden Vector Encryption system to encrypt EHR in cloud environment. The approach presented is able to protect EHR from insider attacks as EHR can only be view by those that are able to supply the appropriate attributes. Seol et al in [25] present a cloud-based EHR model that performs ABAC using XACML. The combination of XML encryption and XML digital signatures are used as security and privacy preserving technique.

There are situations where EHR is shared among different providers. It is possible for an adversary to infer the health condition of a patient by observing the frequency in which the EHR is accessed by a particular healthcare provider. This type of situation violates the privacy of the patient. The authors in [26] propose an efficient multi-show unlinkable access for collaborative e-health environment that exploits attribute-based credential scheme. They utilize anonymous attribute credentials which ensure that users can anonymously prove the ownership of a set of attributes to a verifier and by so doing, obtain access to the protected resources. The method involves randomization of the users credential along with its signature before being disclosed to a verifier. Similarly, Michalas and Weingarten in [27] describe the use of HealthShare, a secure approach for sharing EHR between multiple organizations hosting patient's data in different cloud environments. In the proposed method, a revocable key-policy ABE is used to ensure that access by a malicious or compromised user/organization can easily be revoked without generating new encryption keys.

## IV. Discussion

In this section, we present a comparison of the different approaches used in the existing works. We then use some of the key features of the existing approaches to present a discussion on their differences. Also, we describe the lessons learned from the survey and outline future challenge. Lastly, the concept of modelling and analysing healthcare professionals' security practices is discussed.

### A. Comparison of the Different Approaches

A detailed summary of the existing works on the application of ABAC in e-health systems that we have presented in this work is shown in Table I. Some of the key features of the existing approaches are employed to discuss the differences in the approaches. Also, we describe the lessons learned from the survey and outline future challenge.

*1) Privacy Preserving Techniques:* refer to approaches that may be exploited to provide confidentiality of PHR and EHR. It involves the encryption of the health data to be stored using cryptographic methodologies such that only an individual that possess the decryption key can have access to the health data. It can be observed from Table I that whilst the existing works employ different privacy preserving techniques, ABE and its variants appears to be the most popular approach.

ABE is a type of public key encryption where the private key and the ciphertext are related with a set of attributes or an access policy over the attributes of the users. There are two main variants of ABE, and they are: ciphertext-policy ABE [28] and key-policy ABE [29]. A combination of ciphertext with access policy specifying the attributes of legitimate users is employ in ciphertext-policy ABE, while key-policy ABE uses a set of attributes and private keys associated with the access policy to specify which ciphertexts the key holder can access. Li et al. in [13] argue that ciphertext-policy ABE is more flexible and appropriate for PHR than key-policy ABE in practice. This is evident from the summary in Table I as most application of ABAC in PHR use ciphertext-policy ABE for privacy protection.

Another privacy preserving technique that is used in the existing works is XACL. XAMCL defines a declarative fine-grained, ABAC control policy language which describes how to evaluate access requests according to rules stated in access policies [30]. The authors in [18] use XAMCL to show how a patient's privacy preferences could be expressed and enforced in PHR. XAMCL is deploy in [23] as the privacy preserving technique for EHR. The authors utilize XAMCL for providing

TABLE I. SUMMARY OF EXISTING WORKS ON APPLICATION OF ABAC IN E-HEALTH SYSTEMS

| Work | Type of Health Record Considered | Privacy Preserving Technique | Access Revocation | Storage Platform Used | Adversarial Model Assumption |
|---|---|---|---|---|---|
| [15] | PHR | ABE | Supported | Cloud | Semi-trusted Service Provider |
| [16] | PHR | Ciphertext-Policy ABE | Not Specified | Not Specified | Semi-trusted Service Provider |
| [18] | PHR | XACML | Not Specified | Not Specified | Not Specified |
| [20] | EHR | Ciphertext-Policy ABE | Not Specified | Cloud | Not Specified |
| [27] | EHR | Key-Policy ABE | Supported | Cloud | Trusted Service Provider |
| [25] | EHR | XACML with XML Encryption and XML Digital Signatures | Not Specified | Cloud | Not Specified |
| [13] | PHR | Ciphertext-Policy ABE | Not Specified | Cloud | Semi-trusted Service Provider |
| [17] | PHR | Password Key Derivation Function | Supported | Cloud | Not Specified |
| [26] | EHR | U-Prove | Not Specified | On-Premise | Trusted Service Provider |
| [21] | EHR | Not Specified | Supported | On-Premise | Trusted Service Provider |
| [24] | EHR | Hidden Vector Encryption | Not Specified | Cloud | Not Specified |
| [19] | PHR | Proxy Re-encryption | Supported | Cloud | Semi-trusted Service Provider |
| [14] | PHR | Ciphertext-Policy ABE | Supported | Cloud | Trusted Service Provider |
| [23] | EHR | XACML | Not Specified | On-Premise | Trusted Service Provider |

fine-grained authorization and access to FHIR resources. Seol et al in [25] employ XACML with XML encryption and XML digital signatures as additional measure for ensuring that the privacy and security of EHR are preserved.

Other privacy preserving techniques used in the existing works surveyed include: the use of password key derivation function, U-Prove, hidden vector encryption and proxy re-encryption. Balinsky and Mohammad [17] use password key function to provide end-to-end encryption and show that it ensures no central authority is needed when accessing plaintext data or decryption keys. Authors in [26] argue that enforcing anonymously as well as multi-session unlinkable access for users in e-health is very pertinent. They use the standard U-prove credential scheme and formally prove its multi-show unlinkability property. The paper in [24] use hidden vector encryption to encrypt and embed access control policies within the encrypted data. This approach completely removes the need for two separate security controls. Also Pussewalage and Oleshchuk [19] apply a proxy re-encryption scheme to ensure that only authorized users are able to decrypt PHR files.

*2) Access Revocation:* is another important feature of the existing works surveyed. Although not all the works specified the presence of access revocation, it is an essential characteristic of ABAC in e-health as it enables the disabling of a user's access to PHR or EHR. Several methods have been adopted in order to provide efficient access revocation. The authors in [15] implement access revocation by re-encrypting the ciphertexts and updating the users' private keys. For the papers in [19], [21], the attribute authority is responsible for the access revocation process.

The remaining papers surveyed in this work adopted direct access revocation. The authors in [17] present direct access revocation where the owner of PHR can revoke access by re-encrypting and signing the PHR with a set of newly generated keys. For the paper in [14], each user has a user-index which facilitates direct revocation of user access to an encrypted data. This eliminates the need for re-encrypting the data or refreshing the system parameters to implement access revocation. Also, Michalas and Weingarten [27] present an algorithm that EHR owner can use to revoke access for the unique key that is generated for a particular user. Like the approach in [14], the EHR owner does not have to decrypt and then re-encrypt file with a fresh key.

*3) Storage Platform Used:* refers to method used in storing the PHRs or EHRs. The traditional approach for EHRs has been on-premise, but recent trends have shown a gradual shift to cloud environment. This is due to flexibility and cost-effectiveness that cloud storage environment offers. In the case of PHRs, cloud storage has been the prevalent methodology for storage because it is infeasible for a single individual to bear the cost of setting up storage resources for storing PHRs. Hence, patients that would like to be responsible for their medical health records rely of cloud storage platforms for storing their health information.

*4) Adversarial Model Assumption:* has to do with the assumptions made by the different models about the nature of the storage platform used in storing PHRs and EHRs. These assumptions are necessary when developing formal proof that the proposed approach is feasible and meets all the legal and ethical requirements for storing PHRs and EHRs. The adversarial model assumption considered in most of the existing papers surveyed either assumes trusted service provider or semi-trusted provider. Although these are reasonable assumptions, it would also be insightful to consider untrusted service providers. This would guarantee that the stringent privacy and security requirements for PHR and EHR are met.

*5) Lessons Learned and Future Challenge:* Indeed, e-health systems require a flexible and fine-grained access control mechanism for secured access to PHRs and EHRs. ABAC has shown to be an efficient and effective approach to meeting the security and privacy requirements of e-health systems. We have presented a survey of the different applications of ABAC in e-health systems. By classifying the existing works according to the types of health records considered, we are able to investigate what have been done so far in the literature.

We observe that there has been an increasing adoption of PHR for storing patient health records. This gives the patient greater control of their health record, allowing them to share it with different healthcare providers, family and friends. Also, we notice that ciphertext-policy ABE is the predominant privacy preserving technique used for PHR as it enables the patient to revoke access easily to any user they no longer want to have access to their PHR. In addition, cloud storage platform is used in all the surveyed works for storing PHR.

The storing of EHR as observed in this survey is shifting from the traditional on-premise to cloud environment. This can be attributed to the flexibility and cost-effectiveness of the cloud storage platform. Further, there is an increasing collaboration between different healthcare providers which have led to different approaches proposed for facilitating such collaborations without compromising the privacy of the patient.

All the survey works either assumes that the service provider is trusted or semi-trusted. In the future, approaches that consider untrusted service provides needs to be examined. Recent data breaches involving cloud providers and insider threats further buttress the need to investigate ABAC mechanism for e-health systems that assumes untrusted service providers. Such stringent assumption would ensure that in the case that the third party providers are compromised, the privacy of the patient is still preserved.

### *B. Towards Modelling and Analysing Healthcare Professionals' Security Practices*

Logging of healthcare professionals' accesses is required in the code of conduct for healthcare and care service of Norway [31] and in most international standards for healthcare service. The purpose of logging and protecting the logs includes non-repudiation and investigations [32], [33]. Access logs can be analysed to improve data quality and integrity by detecting healthcare information errors and inconsistencies [32], [33]. For this reason, the Healthcare Security Practice Analysis, Modelling and Incentivization (HSPAMI) project was initiated to determine the metrics of healthcare professional's security practices towards improving upon their conscious care behaviour [34]. One of the major tasks of HSPAMI is to analyse healthcare professionals' access logs towards improving their security behaviour [34].

Analysing RBAC logs may require a lot effort and resources to design the algorithm, for such analysis to be efficient and effective. This is because RBAC mechanisms emphasize only on the role attribute as a control variable for implementing the required protection mechanisms. Without considerable efforts and resources, a higher rate of outliers, false positives and false negative rates are likely to be recorded during the analysis. It is desirable to design the algorithm for the log analysis taking into consideration the environment attributes, the resource attributes and the attributes of the objects in emergency access scenarios. For instance, the log analysis algorithm should be able to determine if the patient status was classified under emergency within the given period. Also, the location of the patient such as the type of hospital ward could support in decision making. Thus, if the patient was admitted in the intensive-care unit (ICU) or emergency ward, the environmental attributes could provide such knowledge. Since RBAC does not include these control variables, more resources may have to be invested in designing such algorithms for efficient log analysis.

In the case of ABAC logs, analysing the logs would likely require less resource to design the algorithm for such analysis to be efficient and effective. ABAC mechanism as we already observed, contain more control variables and as such the logs of ABAC would also contain those variables. These control variables in ABAC logs are desirable variables for the design of an efficient algorithm for log analysis, unlike RBAC that uses the role attribute as the main control variable. Therefore, given that ABAC logs include the control variables needed for the design of an efficient algorithm for the analysis of access logs, fewer resources are likely to be deployed in the design such algorithms.

## V. Conclusion

In summary, we have presented a survey of the existing works on the application of ABAC in e-health systems. We classified the existing works according to the application of ABAC in PHR and EHR. Our survey showed that cloud based storage of PHR and EHR is very popular and that ciphertext-policy ABE is the commonly used for providing security and privacy guarantees in the storage of PHR in the cloud environment. Moreover, we presented a comparison of the different approaches employed in the existing works and used some key characteristics of the existing approaches to present a discussion on their differences. The lessons learned from the survey are described and future challenge that needs to be investigated is outlined. Lastly, a discussion on modelling and analysing healthcare professionals' security practices is presented.

## References

[1] Gartner, "Market trends: Cloud-based security services market, worldwide, 2014," 2014. [Online]. Available: https://www.gartner.com/doc/2607617

[2] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds," vol. 18, pp. 1431–1441, 2014.

[3] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "ehealth cloud security challenges: A survey," *Journal of Healthcare Engineering*, vol. 2019, pp. 1–15, 2019.

[4] N. A. Azeez and C. V. der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Informatics Journal*, vol. 20, pp. 97–108, 2019.

[5] HIPAA-Journal, "Hipaa explained." [Online]. Available: https://www.hipaajournal.com/hipaa-explained/

[6] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg, "Nist special publication 800-66 revision 1: An introductory resource guide for implementing the health insurance portability and accountability act (hipaa) security rule," 2008.

[7] ISO, "Iso/iec 27799:2016 health informatics - information security management in health using iso/iec 27002," 2016. [Online]. Available: https://www.iso.org/standard/62777.html

[8] openEHR, "openehr – a semantically -enabled health computing platform," 2016.

[9] HL7-International, "Clinical document architcture (cda)."

[10] A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zao, R. Chilro, and L. Antunes, "How to securely break into rbac: The btg-rbac model," in *Proc. Annual Computer Security Applications Conf*, Dec. 2009, pp. 23–31.

[11] HIPAA, "Break glass procedure: Granting emergency access to critical ephi systems," 2004.

[12] A. D. Brucker and H. Petritsch, "Extending access control models with break-glass," in *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '09. New York, NY, USA: ACM, 2009, pp. 197–206. [Online]. Available: http://doi.acm.org/10.1145/1542207.1542239

[13] W. Li, B. M. Liu, D. Liu, R. P. Liu, P. Wang, S. Luo, and W. Ni, "Unified fine-grained access control for personal health records in cloud computing," *IEEE Journal of Biomedical and Health Informatics*, vol. 23, no. 3, pp. 1278–1289, May 2019.

[14] S. Narayan, M. Gagné, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," in *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop*, ser. CCSW '10. New York, NY, USA: ACM, 2010, pp. 47–52. [Online]. Available: http://doi.acm.org/10.1145/1866835.1866845

[15] 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 Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[16] C. Wang, X. Xu, D. Shi, and W. Lin, "An efficient cloud-based personal health records system using attribute-based encryption and anonymous multi-receiver identity-based encryption," in *Proc. Cloud and Internet Computing 2014 Ninth Int. Conf. P2P, Parallel, Grid*, Nov. 2014, pp. 74–81.

[17] H. Y. Balinsky and N. Mohammad, "Fine grained access of interactive personal health records," in *Proceedings of the 2015 ACM Symposium on Document Engineering*, ser. DocEng '15. New York, NY, USA: ACM, 2015, pp. 207–210. [Online]. Available: http://doi.acm.org/10.1145/2682571.2797098

[18] I. Ray, T. C. Ong, I. Ray, and M. G. Kahn, "Applying attribute based access control for privacy preserving health data disclosure," in *Proc. IEEE-EMBS Int. Conf. Biomedical and Health Informatics (BHI)*, Feb. 2016, pp. 1–4.

[19] H. S. G. Pussewalage and V. Oleshchuk, "A patient-centric attribute based access control scheme for secure sharing of personal health records using cloud computing," in *Proc. IEEE 2nd Int. Conf. Collaboration and Internet Computing (CIC)*, Nov. 2016, pp. 46–53.

[20] M. Joshi, K. Joshi, and T. Finin, "Attribute based encryption for secure access to cloud based ehr systems," in *Proc. IEEE 11th Int. Conf. Cloud Computing (CLOUD)*, Jul. 2018, pp. 932–935.

[21] H. S. G. Pussewalage and V. A. Oleshchuk, "An attribute based access control scheme for secure sharing of electronic health records," in *Proc. Applications and Services (Healthcom) 2016 IEEE 18th Int. Conf. e-Health Networking*, Sep. 2016, pp. 1–6.

[22] HL7-International, "Fhir overview," 2019. [Online]. Available: https://www.hl7.org/fhir/overview.html

[23] S. Mukherjee, I. Ray, I. Ray, H. Shirazi, T. Ong, and M. G. Kahn, "Attribute based access control for healthcare resources," in *Proceedings of the 2Nd ACM Workshop on Attribute-Based Access Control*, ser. ABAC '17. New York, NY, USA: ACM, 2017, pp. 29–40. [Online]. Available: http://doi.acm.org/10.1145/3041048.3041055

[24] E. Mrema and V. Kumar, "Fine grained attribute based access control of healthcare data," 2018.

[25] K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik, "Privacy-preserving attribute-based access control model for XML-based electronic health record system," *IEEE Access*, vol. 6, pp. 9114–9128, 2018.

[26] H. S. G. Pussewalage and V. A. Oleshchuk, "An efficient multi-show unlinkable attribute based credential scheme for a collaborative e-health environment," in *Proc. IEEE 3rd Int. Conf. Collaboration and Internet Computing (CIC)*, Oct. 2017, pp. 421–428.

[27] A. Michalas and N. Weingarten, "Healthshare: Using attribute-based encryption for secure data sharing between multiple clouds," in *Proc. IEEE 30th Int. Symp. Computer-Based Medical Systems (CBMS)*, Jun. 2017, pp. 811–815.

[28] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security and Privacy (SP '07)*, May 2007, pp. 321–334.

[29] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, ser. CCS '06. New York, NY, USA: ACM, 2006, pp. 89–98. [Online]. Available: http://doi.acm.org/10.1145/1180405.1180418

[30] O. Standard, "extensible access control markup language (xacml) version 3.0," Jan. 2013. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[31] D. ehelse, "Code of conduct for information security and data protection in the healthcare and care services sector," 2018. [Online]. Available: https://ehelse.no/normen/documents-in-english

[32] A. Ferreira, R. Cruz-Correia, and L. Antunes, "Usability of authentication and access control: A case study in healthcare," in *Proc. Carnahan Conf. Security Technology*, Oct. 2011, pp. 1–7.

[33] A. Ferreira, P. Farinha, C. Santos-Pereira, R. J. C. Correia, P. P. Rodrigues, A. da Costa Pereira, and V. Orvalho, "Log analysis of human computer interactions regarding break the glass accesses to genetic reports," in *ICEIS 2013 - Proceedings of the 15th International Conference on Enterprise Information Systems, Volume 3, Angers, France, 4-7 July, 2013*, S. Hammoudi, L. A. Maciaszek, J. Cordeiro, and J. L. G. Dietz, Eds. SciTePress, 2013, pp. 46–53.

[34] P. Yeng, B. Yang, and E. Snekkenes, "Observational measures for effective profiling of healthcare staffs' security practices," in *Proc. IEEE 43rd Annual Computer Software and Applications Conf. (COMPSAC)*, vol. 2, Jul. 2019, pp. 397–404.